De Jacobson-commutativiteitsstelling

Pos, Lars

L.A.A. Pos

De Jacobson-commutativiteitsstelling

Bachelorscriptie

19 december 2024

Scriptiebegeleider: M. A. Daas

Universiteit Leiden
Mathematisch Instituut

Inhoudsopgave

1 Introductie

In 1945 publiceerde Nathan Jacobson een artikel **[6]** waarin hij onder andere de volgende stelling bewees.

Stelling 1.0.1. (Jacobson). *Zij R een ring. Als voor alle $x \in R$ geldt dat er een $n \geq 2$ bestaat zodanig dat $x^n = x$, dan is R commutatief.*

De stelling is een terloops gevolg van een aantal algemene stellingen die hij bewijst in het artikel. In een reeks artikelen **[3]**, **[4]**, **[5]** keek Israel Herstein specifiek naar deze stelling en wist hem te generaliseren.

Stelling 1.0.2. (Jacobson-Herstein). *Zij R een ring. Er geldt dat R commutatief is dan en slechts dan als voor alle $x, y \in R$ geldt dat er een $n \geq 2$ bestaat zodat $(xy - yx)^n = xy - yx$.*

De implicatie naar links volgt direct: in een commutatieve ring geldt dat $xy - yx = 0$ en $0^n = 0$. De kracht van deze stelling zit hem dus in de implicatie naar rechts. We noemen $xy - yx$ ook wel de commutator van x en y, dus de voorwaarde van Stelling 1.0.1 hoeft enkel te gelden voor commutatoren om te kunnen concluderen dat de ring commutatief is.

Definitie 1.0.3. *Een ring die voldoet aan de voorwaarde van Stelling 1.0.2 noemen we een JH-ring.*

In deze scriptie zal ik een bewijs geven voor de stelling van Jacobson-Herstein gebaseerd op het bewijs uit het boek *A first course in noncommutative rings* **[7]**. Dit bewijs is op zijn beurt weer gebaseerd op de artikelen van Herstein. Mijn intentie is geweest het bewijs zo elementair mogelijk op te bouwen. Waar mogelijk heb ik geprobeerd het bewijs te versimpelen. Verder kijken we in deze scriptie ook naar bewijzen van een gevolg van de stelling van Jacobson. Om die te formuleren hebben we de volgende definitie nodig.

Definitie 1.0.4. *Voor een geheel getal $n > 1$ noemen we een ring R een n-ring als voor alle $x \in R$ geldt dat $x^n = x$.*

Uit de stelling van Jacobson volgt dat voor $n \geq 2$ alle n-ringen commutatief zijn. Voor kleine n zijn er elementaire bewijzen van deze stelling op te schrijven. We zullen algemene technieken ontwikkelen om de commutativiteit van sommige n-ringen aan te tonen. In tegenstelling tot het bewijs van de stelling van Jacobson-Herstein hebben we hier niet het keuzeaxioma nodig en de bewijzen die we zullen geven zijn zelfs geheel intuïtionistisch. Het zal blijken dat deze technieken niet voldoende zijn om de commutativiteit van alle n-ringen aan te tonen, dus we zullen ook kijken naar de limitaties van diezelfde technieken (in sectie 4.5 wordt dat precies gemaakt).

2 Voorkennis

Qua voorkennis wordt enige kennis van groepen, ringen en Galoistheorie verwacht. De meest belangrijke resultaten worden in dit hoofdstuk nogmaals toegelicht.

2.1 Algemene voorkennis

Definitie 2.1.1. *Een* ring *is additieve abelse groep R samen met een binaire operatie $\cdot$ zodanig dat aan de volgende drie voorwaardes voldaan wordt:*

*(*eenheidselement*). Er is een element $1 \in R$ zodat voor alle $r \in R$ geldt dat $1 \cdot r = r \cdot 1 = r$.*
*(*associativiteit*). Voor alle $x, y, z \in R$ geldt dat $(xy)z = x(yz)$.*
*(*distributiviteit*). Voor alle $x, y, z \in R$ geldt dat $x(y+z) = xy + xz$ en $(x+y)z = xz + yz$.*

In het vervolg is R telkens een ring.

Definitie 2.1.2. *We noemen een ring R* commutatief *als voor alle $x, y \in R$ geldt dat $xy = yx$.*

Definitie 2.1.3. *Als voor twee elementen $x, y \in R$ geldt dat $xy = 1$ dan noemen we x een* linksinverse *van y en y een* rechtsinverse *van x.*

Lemma 2.1.4. *Als een element $x \in R$ zowel een linksinverse y en een rechtsinverse z heeft dan geldt $y = z$.*

Bewijs. Er geldt dat $yx = 1 = xz$, dus $y = y(xz) = (yx)z = z$. □

Definitie 2.1.5. *Een element $r \in R$ noemen we een* eenheid *als het zowel een links als een rechtsinverse heeft. Wegens Lemma 2.1.4 is dit equivalent aan het hebben van een unieke tweezijdige inverse. De tweezijdige inverse van een eenheid r noteren we als r^{-1}.*

Lemma 2.1.6. *De verzameling eenheden $R^\times$ van een ring R vormt een groep onder vermenigvuldiging.*

Bewijs. We beginnen met het verifiëren dat vermenigvuldiging goedgedefineerd is op $R^\times$. Voor $u, v \in R^\times$ geldt dat $v^{-1}u^{-1}(uv) = 1 = (uv)v^{-1}u^{-1}$, dus $uv \in R^\times$. Vervolgens gaan we de drie groepsaxioma's bij langs:
(*eenheidselement*). Aangezien $1 \cdot 1 = 1$ geldt dat $1 \in R^\times$ en voor alle $u \in R^\times$ geldt dat $1 \cdot u = u \cdot 1 = u$, dus $R^\times$ heeft een eenheidselement.
(*associativiteit*). Als deelverzameling van R erft $R^\times$ de associatieve eigenschap.
(*tweezijdige inverses*). Aangezien $uu^{-1} = u^{-1}u = 1$ geldt dat u de inverse is van u^{-1}, dus $u^{-1} \in R^\times$. □

Lemma 2.1.7. *Als $uv, vu \in R^\times$ dan $u, v \in R^\times$.*

Bewijs. Aangezien $uv \in R^\times$ bestaat er een $s \in R^\times$ zodanig dat $suv = 1 = uvs$. Hieruit volgt dat v een linksinverse heeft en u een rechtsinverse. Aangezien $vu \in R^\times$ bestaat er een $t \in R^\times$ zodanig dat $tvu = 1 = vut$. Hieruit volgt dat u een linksinverse heeft en v een rechtsinverse. We concluderen dat $u, v \in R^\times$. □

Definitie 2.1.8. *Een* linksideaal *I van een ring R is een deelverzameling $I \subset R$ zodanig dat $(I, +)$ een ondergroep is van $(R, +)$ en voor alle $r \in R$, $i \in I$ geldt dat $ri \in I$. Als verder ook voor alle $i \in I$ en $r \in R$ geldt dat $ir \in I$ dan noemen we I een* ideaal *of ook wel een* tweezijdig ideaal.

Definitie 2.1.9. *Een (links)ideaal I van een ring R noemen we* maximaal *als $I \neq R$ en voor ieder (links)ideaal J met $I \subset J$ geldt dat $J = I$ of $J = R$.*

Opmerking 2.1.10. *Wegens Zorn's lemma heeft iedere ring ongelijk aan de nulring een maximaal ideaal.*

Definitie 2.1.11. *Een* R-linksmoduul *is een additieve abelse groep* M*, samen met een multiplicatief genoteerde bewerking* $R \times M \to M$*, die voldoet aan de volgende voorwaardes:*

$$\begin{aligned}(r+s)\cdot m &= rm + sm\\ r(m+n) &= rm + rn\\ r(sm) &= (rs)m.\end{aligned}$$

Een R-rechtsmoduul *is een additieve abelse groep* M *samen met een multiplicatief genoteerde bewerking* $M \times R \to M$ *die voldoet aan dezelfde voorwaardes:*

$$\begin{aligned}m\cdot(s+r) &= ms + mr\\ (n+m)r &= nr + mr\\ (ms)r &= m(sr).\end{aligned}$$

In tegenstelling tot de conventie voor idealen wordt met moduul een linksmoduul bedoeld. Een (R,S)-bimoduul M *is een* R*-linksmoduul en een* S*-rechtsmoduul met* $(rm)s = r(ms)$ *voor alle* $r \in R$*,* $m \in M$ *en* $s \in S$*.*

Definitie 2.1.12. *Een deelmoduul* N *van een moduul* M *van de ring* R *is een ondergroep van* M *zodanig dat voor alle* $r \in R$ *en* $n \in N$ *geldt dat* $rn \in N$*.*

Voorbeeld 2.1.13. Een ring R is altijd een linksmoduul over zichzelf en de deelmodulen van R zijn precies de linksidealen van R.

Definitie 2.1.14. *Een* delingsring *is een ring* R *waarvoor geldt dat* $R^\times = R \setminus \{0\}$*.*

Opmerking 2.1.15. Merk op dat een delingsring niet per se commutatief is. Zo is $\mathbb{H}$ (de quaternionen) een delingsring, maar $ij = k \neq -k = ji$.

Definitie 2.1.16. *Een commutatieve delingsring noemen we een* lichaam*.*

Definitie 2.1.17. *Het* centrum $Z(R)$ *van een ring* R *bestaat uit alle elementen* $x \in R$ *zodanig dat voor alle* $y \in R$ *geldt dat* $xy = yx$*.*

Lemma 2.1.18. *Het centrum* $Z(R)$ *is gesloten onder optelling, aftrekken en vermenigvuldiging.*

Bewijs. Stel $x, y \in Z(R)$, dan geldt voor alle $z \in R$ dat

$$(x+y)z = xz + yz = zx + zy = z(x+y).$$

Dus geldt dat $x + y \in Z(R)$. Ook hebben we $xyz = xzy = zxy$, dus $xy \in Z(R)$. Voor alle $x \in R$ geldt dat $-1 \cdot x + x = (-1+1)x = 0 = x(-1+1) = x \cdot -1 + x$, dus $-1 \cdot x = x \cdot -1$, waardoor $-1 \in Z(R)$. Voor alle $x, y \in Z(R)$ hebben we nu dat $x - y = x + (-1 \cdot y)$, dus ook $x - y \in Z(R)$. □

Definitie 2.1.19. *Een* ringhomomorfisme *van de ring* R *naar de ring* S *is een groepshomomorfisme* $f : R \to S$ *zodanig dat voor alle* $x, y \in R$ *geldt dat* $f(xy) = f(x)f(y)$ *en verder* $f(1_R) = 1_S$*.*

Lemma 2.1.20. *De verzameling bijectieve ringhomomorfismen van R naar R vormt een groep onder samenstelling.*

Bewijs. Allereerst controleren we dat deze bewerking goedgedefinieerd is. We weten dat de samenstelling van bijectieve groepshomomorfismen weer een bijectief groepshomomorfisme is. Verder geldt voor $x, y \in R$ en ringhomomorfismen f en g dat

$$(f \circ g)(xy) = f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y)) = (f \circ g)(x)(f \circ g)(y)$$

en

$$(f \circ g)(1) = f(g(1)) = f(1) = 1.$$

Dus de bewerking is goedgedefineerd. We gaan de drie groepsaxioma's bij langs.
(*eenheidselement*). De identiteitsafbeelding id_R is een bijectief ringhomomorfisme. Zij f een bijectief ringhomomorfisme. Voor $x \in R$ geldt dat $(\mathrm{id}_R \circ f)(x) = \mathrm{id}_R(f(x)) = f(x)$ en $(f \circ \mathrm{id}_R)(x) = f(\mathrm{id}_R(x)) = f(x)$, dus id_R is inderdaad het eenheidselement.
(*associativiteit*). Voor alle $x \in R$ en bijectieve ringhomomorfismen f, g en h geldt dat

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x).$$

(*inverse*). De inverse van een bijectief groepshomomorfisme is een bijectief groepshomomorfisme en voor $x, y \in R$ geldt dat $f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(x))f(f^{-1}(y)) = xy$, dus als we f^{-1} aan beide kanten toepassen krijgen we $f^{-1}(x)f^{-1}(y) = f^{-1}(xy)$. Verder geldt dat $f(1) = 1$, dus ook $f^{-1}(1) = 1$. We concluderen dat f^{-1} ook een bijectief ringhomomorfisme is. □

Definitie 2.1.21. *De* automorfismengroep $\mathrm{Aut}(R)$ *van een ring R is de verzameling bijectieve ringhomomorfismen van R naar R. Wegens Lemma 2.1.20 is de automorfismengroep van R ook daadwerkelijk een groep.*

Definitie 2.1.22. *Een* moduulhomomorfisme *van een R-moduul M naar een R-moduul N is een groepshomomorfisme $f : M \to N$ zodat voor $r \in R$ en $m \in M$ geldt dat $f(rm) = rf(m)$.*

Lemma 2.1.23. *Voor een moduul M over een ring R geldt dat de verzameling moduulhomomorfismen van M naar M een ring vormt onder puntsgewijs optellen en samenstelling.*

Bewijs. Allereerst controleren we dat deze bewerkingen goedgedefinieerd zijn. We weten dat de puntsgewijze som en samenstelling van groepshomomorfismen weer een groepshomomorfisme is. Verder geldt voor $m \in M$ en moduulhomomorfismen f en g dat

$$(f + g)(rm) = f(rm) + g(rm) = rf(m) + rg(m) = r(f(m) + g(m)) = r(f + g)(m)$$

en

$$(f \circ g)(rm) = f(g(rm)) = f(rg(m)) = rf(g(m)) = r(f \circ g).$$

Dus deze bewerkingen zijn goedgedefinieerd. We gaan de drie ringaxioma's bij langs.
(*eenheidselement*). De identiteitsafbeelding id_M is een moduulhomomorfisme. Voor alle moduulhomomorfismen f en $m \in M$ geldt dat $(\mathrm{id}_M \circ f)(m) = \mathrm{id}_M(f(m)) = f(m)$ en

$(f \circ \mathrm{id}_M)(m) = f(\mathrm{id}_M(m)) = f(m)$.
(*associativiteit*). Voor alle $m \in M$ en moduulhomomorfismen f, g en h geldt dat

$$((f \circ g) \circ h)(m) = (f \circ g)(h(m)) = f(g(h(m))) = f(g \circ h)(m) = (f \circ (g \circ h))(m).$$

(*distributiviteit*). Voor alle $m \in M$ en moduulhomomorfismen f, g en h geldt dat

$$((f + g) \circ h)(m) = (f + g)(h(m)) = f(h(m)) + g(h(m)) =$$

$$(f \circ h)(m) + (g \circ h)(m) = ((f \circ h) + (g \circ h))(m)$$

en

$$(f \circ (g + h))(m) = f((g + h)(m)) = f(g(m) + h(m)) =$$

$$f(g(m)) + f(h(m)) = (f \circ g)(m) + (f \circ h)(m) = ((f \circ g) + (f \circ h))(m).$$

Dus aan alle axioma's wordt voldaan. □

Definitie 2.1.24. *Voor een ring R en een moduul M noemen we de verzameling moduulhomomorfismen van M naar M de* endomorfismering $\mathrm{End}_R(M)$. *Wegens Lemma 2.1.23 is de endomorfismering van R ook daadwerkelijk een ring.*

2.2 Voorkennis paragraaf 3.2

Definitie 2.2.1. *Een lichaamsuitbreiding $K \subset L$ noemen we* Galois *als er een eindige ondergroep G van* $\mathrm{Aut}(L)$ *bestaat zodanig dat $K = L^G := \{x \in L : \sigma(x) = x \text{ voor alle } \sigma \in G\}$. In dat geval noemen we G de* Galoisgroep *van de uitbreiding $K \subset L$. Indien G eindig is spreken we van een eindige Galoisuitbreiding. In dat geval noemen we $|G|$ de graad van de lichaamsuitbreiding $K \subset L$.*

Lemma 2.2.2. *Zijn L en M lichamen zodat L een eindige Galoisuitbreiding is van M met Galoisgroep G. Dan geldt voor $\alpha \in L$ dat $\prod_{\sigma \in G} \sigma(\alpha) \in M$.*

Bewijs. Voor $\mu \in G$ geldt dat $\mu(\prod_{\sigma \in G} \sigma(\alpha)) = \prod_{\sigma \in G} (\mu\sigma)(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$, waardoor $\prod_{\sigma \in G} \sigma(\alpha) \in L^G = M$. □

Definitie 2.2.3. *Zijn L en M lichamen zodat L een eindige Galoisuitbreiding van M is met Galoisgroep G. Voor een element $\alpha \in L$ definiëren we de* normafbeelding $N : L \to M$ *als*

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Lemma 2.2.4. *Zij M een eindig lichaam van karakteristiek p en kardinaliteit p^n. Zij verder L een lichaamsuitbreiding van graad m met Galoisgroep G. Dan geldt dat de normafbeelding $N : L \to M$ surjectief is.*

Bewijs. Voor $q = p^n$ geldt dat het automorfisme σ met $\sigma(x) = x^q$ een automorfisme is van L dat precies M invariant laat, dus G wordt voortgebracht door σ. Er moet gelden dat de orde van σ gelijk is aan m want de lichaamsuitbreiding heeft graad m, dus voor alle $x \in L$ hebben we dat $x = \sigma^m(x) = x^{q^m}$. Zij k het getal zodat L precies q^k elementen heeft. Als $k < m$ dan geldt voor alle $x \in L$ dat $x = x^{q^k} = \sigma^k(x)$, maar σ had orde m,

tegenspraak. Nu moet er gelden dat $k = m$, want alle $x \in L$ zijn een oplossing van $x^{q^m} = x$ en dit polynoom heeft maximaal q^m oplossingen. Zij nu $\alpha \in L$ een voortbrenger van de cyclische groep $L^\times$. Dan geldt dat

$$N(\alpha) = \prod_{0 \leq i \leq m-1} \sigma^i(\alpha) = \prod_{0 \leq i \leq m-1} \alpha^{q^i} = \alpha^{1+q+\ldots+q^{m-1}}.$$

Omdat α een voortbrenger is van $L^\times$ geldt dat α orde $q^m - 1$ heeft. Aangezien er geldt dat $(q-1)(1+q+\ldots+q^{m-1}) = q^m - 1$ is de orde van $N(\alpha)$ gelijk aan $q-1$. Dus $N(\alpha)$ is een voortbrenger van K en aangezien de normafbeelding multiplicatief is volgt hieruit dat hij ook surjectief is. □

Lemma 2.2.5. *Zij L een lichaam en zij G een ondergroep van $\mathrm{Aut}(L)$ voortgebracht door een automorfisme σ van orde groter of gelijk aan $m \in \mathbb{Z}_{\geq 0}$. Zij verder K een ring zodanig dat $L \subset K$ en zij $\sum_{i=0}^{m-1} a_i \sigma^i(x) = 0$ met $a_i \in K$ een relatie die geldt voor alle $x \in L$. Dan geldt voor alle $0 \leq i \leq m-1$ dat $a_i = 0$.*

Bewijs. We gaan met inductie naar n bewijzen dat iedere relatie $\sum_{i=0}^{n} a_i \sigma^i(x) = 0$ voor $n \leq m-1$ triviaal moet zijn. De inductiebasis is duidelijk, als $a_0 = 0$ dan geldt $a_0 = 0$. Neem nu aan dat we de bewering bewezen hebben voor alle $n < k$ en kijk naar het geval $n = k$. Vervang in de relatie x door xy voor een variabele $y \in L$. We krijgen $\sum_{i=0}^{k} a_i \sigma^i(x)\sigma^i(y) = 0$. We kunnen de oorspronkelijke relatie ook vermenigvuldigen met $\sigma^k(y)$, dan krijgen we dat $\sum_{i=0}^{k} a_i \sigma^i(x)\sigma^k(y) = 0$. Neem nu het verschil van deze twee vergelijkingen. Er volgt dat $\sum_{i=0}^{k-1} a_i(\sigma^i(y) - \sigma^k(y))\sigma^i(x) = 0$. Wegens de inductiehypothese moet gelden dat $a_i(\sigma^i(y) - \sigma^k(y)) = 0$, maar aangezien $\sigma^k \neq \sigma^i$ voor alle $0 \leq i < k$ kunnen we een $\alpha \in L$ vinden met $\sigma^i(\alpha) \neq \sigma^k(\alpha)$. Als we $y = \alpha$ invullen krijgen we dat $a_i(\sigma^i(\alpha) - \sigma^k(\alpha)) = 0$ met $\sigma^i(\alpha) - \sigma^k(\alpha) \neq 0$. Aangezien $\sigma^i(\alpha) - \sigma^k(\alpha) \in L$ kunnen we met zijn inverse vermenigvuldigen en krijgen we dat $a_i = 0$, waarmee de inductie is voltooid. □

2.3 Voorkennis paragraaf 3.3

Definitie 2.3.1. *Een ring R noemen we* simpel *als R precies twee tweezijdige idealen heeft, namelijk (0) en R.*

Definitie 2.3.2. *Een moduul M over een ring R noemen we* simpel *als het precies twee deelmodulen heeft, namelijk $\{0\}$ en M.*

Lemma 2.3.3. (Schur). *De endomorfismering van een simpel moduul M over de ring R is een delingsring.*

Bewijs. Zij $f \in \mathrm{End}_R(M)$ en neem aan dat $f \neq 0$. Om te laten zien dat f een eenheid gaan we eerst aantonen dat f bijectief is. Er geldt dat $\mathrm{im}(f)$ en $\ker(f)$ deelmodulen van M zijn, want voor $m = f(n) \in \mathrm{im}(f)$ en $r \in R$ geldt dat $rm = rf(n) = f(rn) \in \mathrm{im}(f)$ en voor $m \in \ker(f)$ geldt dat $f(rm) = rf(m) = 0$. Omdat $f \neq 0$ geldt dat $\mathrm{im}(f)$ niet het nulmoduul is, en $\ker(f)$ niet heel M. Aangezien M simpel is moet dus gelden dat $\mathrm{im}(f) = M$ en $\ker(f) = 0$, dus f is bijectief. Dat betekent dat f^{-1} als functie bestaat. De

inverse van een bijectief groepshomomorfisme is altijd weer een groepshomomorfisme en voor $r \in R$, $m \in M$ geldt dat $f(rf^{-1}(m)) = rf(f^{-1}(m)) = rm$. Door f^{-1} aan beide kanten toe te passen krijgen we $rf^{-1}(m) = f^{-1}(rm)$. Er geldt dus $f^{-1} \in \mathrm{End}_R(V)$. □

Definitie 2.3.4. *De* annihilator $\mathrm{Ann}_R(M)$ *van een moduul M over een ring R is de verzameling van alle $r \in R$ waarvoor voor alle $m \in M$ geldt dat $r \cdot m = 0$.*

Lemma 2.3.5. *De annihilator $\mathrm{Ann}_R(M)$ van een moduul M over een ring R is een tweezijdig ideaal.*

Bewijs. De annihilator $\mathrm{Ann}_R(M)$ is de kern van het ringhomomorfisme $R \to \mathrm{End}_{\mathbb{Z}} M$ wat $r \in R$ stuurt naar de afbeelding die $m \in M$ stuurt naar rm. Aangezien kernen altijd tweezijdige idealen zijn is $\mathrm{Ann}_R(M)$ een tweezijdig ideaal. □

Definitie 2.3.6. *Een moduul M over een ring R noemen we* trouw *als $\mathrm{Ann}_R(M) = (0)$.*

Definitie 2.3.7. *Een ring R noemen we linksprimitief als er een trouw simpel R-moduul M bestaat.*

Definitie 2.3.8. *Een ideaal I van een ring R noemen we linksprimitief als R/I een linksprimitieve ring is.*

Definitie 2.3.9. *Een moduul M over een ring R noemen we* semisimpel *als er een verzameling I bestaat en voor elke $i \in I$ er een simpel moduul M_i is zodanig dat $M = \bigoplus_{i \in I} M_i$.*

Lemma 2.3.10. *Zij M een semisimpel moduul over een ring R waarvoor de verzameling I eindig is. Voor ieder deelmoduul N van M kunnen we een deelmoduul P vinden zodat $N \oplus P = M$.*

Bewijs. Schrijf M als $\bigoplus_{i=1}^{n} M_i$ met M_i simpel. Zij J een maximale deelverzameling van $\{1, 2, \ldots, n\}$ zodanig dat $(\bigoplus_{j \in J} M_j) \cap N = 0$. We gaan uit het ongerijmde bewijzen dat $(\bigoplus_{j \in J} M_j) \oplus N = M$, dus stel dat $(\bigoplus_{j \in J} M_j) \oplus N \neq M$. Dan is er een k zodanig dat $M_k \not\subset (\bigoplus_{j \in J} M_j) \oplus N$. Er geldt dus dat $k \notin J$. Aangezien M_k simpel is moet gelden dat $M_k \cap ((\bigoplus_{j \in J} M_j) \oplus N) = 0$. Omdat J maximaal is geldt dat $(\bigoplus_{j \in J \cup \{k\}} M_j) \cap N \neq 0$, dus er zijn $m \in M_k$, $l \in \bigoplus_{j \in J} M_j$ en $n \in N$ zodat $m + l = n \neq 0$. Maar dan geldt dat $m = n - l \in (\bigoplus_{j \in J} M_i) \oplus N$, dus $m = 0$. Dat betekent dat $l = n \neq 0$, maar dat is in tegenspraak met $(\bigoplus_{j \in J}) \cap N = 0$. We concluderen dat $(\bigoplus_{j \in J} M_j) \oplus N = M$. □

2.4 Voorkennis Hoofstuk 4

Definitie 2.4.1. *Een ring R noemen we* gereduceerd *als voor alle $x \in R$ uit $x^2 = 0$ volgt dat $x = 0$.*

Stelling 2.4.2. (Bezout). *Voor iedere eindige verzameling $\{x_1, x_2, \ldots, x_n\} \in \mathbb{Z}$ bestaan er $a_1, a_2, \ldots a_n \in \mathbb{Z}$ zodanig dat $a_1x_1 + a_2x_2 + \ldots a_nx_n = \mathrm{ggd}(x_1, x_2, \ldots x_n)$.*

Bewijs. De verzameling $S = \{b_1x_1 + b_2x_2 + \ldots b_nx_n | b_1, b_2, \ldots b_n \in \mathbb{Z}\}$ is een ideaal van $\mathbb{Z}$, want S is gesloten onder optellen en vermenigvuldiging met een element uit de ring. We weten dat $\mathbb{Z}$ een hoofdideaaldomein is, dus er geldt $S = (g)$ voor een $g \geq 0$. Voor alle $b_1, b_2, \ldots b_n \in \mathbb{Z}$ geldt dat $\mathrm{ggd}(x_1, x_2, \ldots x_n) | b_1x_1 + b_2x_2 + \ldots b_nx_n$, dus

$\text{ggd}(x_1, x_2, \ldots x_n) | g$. Ook geldt dat $x_1, x_2, \ldots, x_n \in S$, dus $g|x_1$, $g|x_2$, ..., $g|x_n$. Daaruit volgt dat $g|\,\text{ggd}(x_1, x_2, \ldots x_n)$, dus er moet gelden dat $g = \text{ggd}(x_1, x_2, \ldots x_n)$. Dat betekent dat $\text{ggd}(x_1, x_2, \ldots x_n) \in S$ dus er bestaan inderdaad a_1, a_2, ..., a_n zodanig dat $a_1x_1 + a_2x_2 + \ldots a_nx_n = \text{ggd}(x_1, x_2, \ldots x_n)$. □

Stelling 2.4.3. (Fermat). *Zij p een priemgetal. Voor alle $x \in \mathbb{Z}$ geldt dat $x^p \equiv x \mod p$.*

Bewijs. Merk op dat aangezien we modulo p werken het volstaat de stelling te bewijzen voor alle niet-negatieve gehele getallen. Dit gaan we doen met inductie. Het basisgeval $x = 0$ volgt triviaal, aangezien $0^p \equiv 0 \mod p$. Stel nu dat we de stelling bewezen hebben voor zekere $x = k$, dan geldt dat $(k+1)^p = \sum_{i=0}^{p} k^i \binom{p}{i}$ en aangezien $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ voor $0 < i < p$ deelbaar is door p (de teller is deelbaar door p, maar de noemer niet), geldt dat $(k+1)^p \equiv k^p + 1^p \equiv k+1 \mod p$. Dus geldt de stelling ook voor $x = k+1$, wat de inductie voltooid. □

Stelling 2.4.4. (Wilson). *Zij p een priemgetal. Er geldt dat $(p-1)! \equiv -1 \mod p$.*

Bewijs. Wegens de kleine stelling van Fermat geldt dat alle elementen van $\mathbb{F}_p$ nulpunt zijn van het polynoom $x^p - x$. Aangezien we p nulpunten hebben gevonden van een monisch polynoom van graad p moet er gelden dat

$$x^p - x \equiv x(x-1)(x-2)\ldots(x-(p-1)) \mod p.$$

Dat betekent dat ook de coëfficiënt van x aan beide kanten gelijk moet zijn, dus geldt er dat $-1 \equiv (-1)^{p-1}(p-1)! \equiv (p-1)! \mod p$. □

Lemma 2.4.5. *Er geldt voor $1 \leq n \leq p-2$ dat*

$$1^n + 2^n + \ldots + (p-1)^n \equiv 0 \mod p.$$

Bewijs. Zij a een primitieve eenheidswortel modulo p. Aangezien a een eenheid is geldt dat vermenigvuldiging met a bijectief is, dus $\{1, 2, \ldots, p-1\} = \{a, 2a, \ldots, (p-1)a\}$. Hierdoor geldt er dat

$$1^n + \ldots + (p-1)^n \equiv a^n + (2a)^n + \ldots + ((p-1)a)^n \equiv a^n(1^n + 2^n + \ldots + (p-1)^n) \mod p.$$

Omdat $1 \leq n \leq p-2$ geldt dat $a^n \neq 1$, want de orde van a is $p-1$. Daaruit volgt dat $1^n + 2^n + \ldots + (p-1)^n \equiv 0 \mod p$. □

3 De stelling van Jacobson-Herstein

In de volgende paragrafen bewijzen we de stelling van Jacobson-Herstein. Dit doen we in vier stappen. We bewijzen de stelling achtereenvolgens voor delingsringen, links-primitieve ringen, semiprimitieve ringen en als laatste voor algemene ringen. We beginnen met het definiëren respectievelijk bewijzen van een aantal nuttige begrippen en lemma's.

3.1 Het Jacobson-radicaal

Een van de belangrijke begrippen die we nodig hebben voor het bewijs van de stelling van Jacobson-Herstein is het Jacobson-radicaal. Er zijn meerdere equivalente definities voor het Jacobson-radicaal; zo is het bijvoorbeeld de doorsnede van alle maximale linksidealen en de annihilator van de verzameling simpele linksmodulen. Voor deze scriptie volstaat echter de volgende definitie.

Definitie 3.1.1. *Het Jacobson-radicaal* $\operatorname{rad}(R)$ *bestaat uit alle* $x \in R$ *waarvoor voor alle* $r, s \in R$ *geldt dat* $1 + rxs \in R^\times$.

Lemma 3.1.2. $\operatorname{rad}(R)$ *is een tweezijdig ideaal.*

Bewijs. Voor $x \in \operatorname{rad}(R)$ en $a \in R$ geldt dat $1 + r(ax)s = 1 + (ra)xs \in R^\times$, waaruit volgt dat $ax \in \operatorname{rad}(R)$. Analoog hebben we ook dat $xa \in \operatorname{rad}(R)$. We gaan nu laten zien voor $x, y \in \operatorname{rad}(R)$ dat $1 + r(x + y)s$ een eenheid is. We weten dat $1 + rxs$ een eenheid is, dus laat u zijn inverse zijn. Dan geldt dat

$$(1 + rxs)(1 + urys) = (1 + rxs) + (1 + rxs)urys = 1 + rxs + rys = 1 + r(x + y)s.$$

Aangezien $1 + rxs$ en $1 + (ur)ys$ beide eenheden zijn volgt wegens Lemma 2.1.6 dat $1 + r(x + y)s$ een eenheid is. Dus $\operatorname{rad}(R)$ is ook gesloten onder optellen en aangezien $0 \in \operatorname{rad}(R)$ geldt $\operatorname{rad}(R) \neq \emptyset$, dus het is inderdaad een tweezijdig ideaal. □

Lemma 3.1.3. *Laat* $\{\mathfrak{U}_i\}_{i \in I}$ *de verzameling linksprimitieve idealen van* R *zijn. Dan geldt er dat* $\bigcap_{i \in I} \mathfrak{U}_i \subset \operatorname{rad}(R)$.

Bewijs. Stel dat x in de doorsnede van alle linksprimitieve idealen zit. Als uit het ongerijmde $x \notin \operatorname{rad}(R)$ dan geldt voor zekere $r, s \in R$ dat $1 + rxs$ geen eenheid is. Neem z.v.v.a. aan dat $1 + rxs$ niet linksinverteerbaar is, dan geldt dat $(1 + rxs)$ bevat is in een maximaal linksideaal $\mathfrak{m}$. Zij A de annihilator van het linksmoduul $R/\mathfrak{m}$, er volgt dat $R/\mathfrak{m}$ een trouw R/A moduul is. Wegens de maximaliteit van $\mathfrak{m}$ is $R/\mathfrak{m}$ ook een simpel R/A moduul, dus A is linksprimitief, waardoor $x \in A$, dus ook $(1 + rxs) - rxs = 1 \in A$. Maar dat is een tegenspraak, want $R/\mathfrak{m}$ wordt niet geannihileerd door heel R. Er geldt dus inderdaad dat $x \in \operatorname{rad}(R)$. □

Definitie 3.1.4. *Een ring* R *noemen we* semiprimitief *als* $\operatorname{rad}(R) = 0$.

Lemma 3.1.5. *Er geldt dat* $R/\operatorname{rad}(R)$ *een semiprimitieve ring is.*

Bewijs. Laat $I = \operatorname{rad}(R)$. Stel dat er een $x \in R \setminus I$ is waarvoor $x + I \in \operatorname{rad}(R/I)$. Dan geldt dus voor alle $r, s \in R$ dat $1 + (r + I)(x + I)(s + I) = 1 + rxs + I$ een eenheid is. Laat $u + I$ zijn inverse zijn, we hebben dus dat $1 + I = (1 + rxs + I)(u + I) = (1 + rxs)u + I$ en $1 + I = (u + I)(1 + rxs + I) = u(1 + rxs) + I$. Dat betekent dat we in R hebben dat $1 + a = (1 + rxs)u$ en $1 + b = u(1 + rxs)$, voor zekere $a, b \in \operatorname{rad}(R)$. Wegens de definitie van $\operatorname{rad}(R)$ geldt dat $1 + a, 1 + b \in R^\times$, dus $(1 + rxs)u, u(1 + rxs) \in R^\times$. Wegens Lemma 2.1.7 is dan ook $1 + rxs$ een eenheid. Dat betekent dat $x \in I$, dus $\operatorname{rad}(R/I) = 0$ en daarmee is het een semiprimitieve ring. □

Het volgende lemma zullen we vaak gaan gebruiken.

Lemma 3.1.6. *Zij R een JH-ring en $\phi : R \to S$ een surjectief ringhomomorfisme. Dan is S ook een JH-ring.*

Bewijs. Voor een commutator $cd - dc \in S$ geldt dat er $a, b \in R$ bestaan zodanig dat $\phi(a) = c$ en $\phi(b) = d$, want ϕ is surjectief. Dan geldt wegens de voorwaarde dat er een $n \geq 2$ is zodanig dat $(ab - ba)^n = ab - ba$. Nu geldt dat

$$(cd - dc)^n = (\phi(a)\phi(b) - \phi(b)\phi(a))^n = \phi((ab - ba)^n) = \phi(ab - ba) = cd - dc.$$

Dus S is ook een JH-ring. □

3.2 Delingsringen

Stelling 3.2.1. *Zij R een JH-delingsring, dan is R commutatief.*

Bewijs. We gaan deze stelling bewijzen uit het ongerijmde, dus neem aan dat R niet commutatief is. Merk op dat aangezien R een JH-delingsring is alle commutatoren ongelijk 0 een eindige multiplicatieve orde hebben.

Definitie 3.2.2. *Zij $D = \{xy - yx | x, y \in R\}$ de verzameling van commutatoren.*

Lemma 3.2.3. *Als $y \in R$ commuteert met alle $d \in D$ dan geldt dat $y \in Z(R)$.*

Bewijs. Neem uit het ongerijmde aan dat $xy \neq yx$ voor zekere $x \in R$. Er geldt dat $x(xy) - (xy)x$ en $xy - yx$ beide commutatoren zijn en merk op dat $x(xy) - (xy)x$ gelijk is aan $x(xy - yx)$. We kunnen nu gebruiken dat y met beide elementen commuteert om te krijgen dat $yx(xy - yx) = x(xy - yx)y = xy(xy - yx)$. Aangezien $xy - yx \neq 0$ kunnen we nu aan beide kanten met zijn inverse vermenigvuldigen om $xy = yx$ te krijgen, tegenspraak. □

Omdat we uit het ongerijmde werken geldt dat $F := Z(R)$ niet gelijk is aan R. Wel geldt dat F een lichaam is, wegens Lemma 2.1.18 en aangezien $0, 1 \in Z(R)$. Wegens Lemma 3.2.3 geldt dat als $D \subset F$ dat R dan commutatief is, dus bestaat er een $a \in D$ waarvoor $a \notin F$. Deze a gaan we gebruiken om een tegenspraak af te leiden.

Lemma 3.2.4. *De karakteristiek van F is groter is dan 0.*

Bewijs. Als de karakteristiek van F gelijk is aan 2 dan is dit duidelijk het geval. Schrijf anders a als $xy - yx$, wat kan aangezien a een commutator is. Dan geldt $2a \in D$, want $2a = (2x)y - y(2x) \in D$. Dus a en $2a$ zijn beide niet-nul commutatoren waardoor hun ordes eindig zijn. Hierdoor kunnen we een $k > 0$ vinden waarvoor $a^k = (2a)^k = 1$, neem bijvoorbeeld het product van de beide ordes. Dan geldt dat $2^k = 2^k a^k = (2a)^k = 1$, dus $2^k = 1$. Hieruit volgt dat de karakteristiek van F groter is dan 0. □

Zij p de karakteristiek van F; deze is dus groter dan 0. Beschouw nu het eindige lichaam $K := \mathbb{F}_p[a] \subset R$ van kardinaliteit p^n voor een zekere $n \geq 1$. Er geldt dus $a^{p^n} = a$. We gaan nu werken in de endomorfismering van R als abelse groep. We zijn namelijk geïnteresseerd in het herhaaldelijk toepassen van δ, het endomorfisme wat x stuurt naar $ax - xa$. Definieer hiervoor de endomorfismen λ en ρ met $\lambda(x) = ax$ en $\rho(x) = xa$. Er

geldt dus dat $\delta = \lambda - \rho$. Merk op dat $(\lambda \circ \rho)(x) = axa = (\rho \circ \lambda)(x)$, dus λ en ρ commuteren. Verder geldt dat deze endomorfismering karakteristiek p heeft, want K en R hebben karakteristiek p. Ook hebben we dat $\lambda^{p^n}(x) = a^{p^n}x = ax = \lambda(x)$ en $\rho^{p^n}(x) = xa^{p^n} = xa = \rho(x)$. Dus geldt er ook dat

$$\delta^{p^n} = (\lambda - \rho)^{p^n} = \lambda^{p^n} - \rho^{p^n} = \lambda - \rho = \delta.$$

Lemma 3.2.5. *Er bestaat een $k_0 \in K^\times$ waarvoor het endomorfisme $\delta - k_0$ (waarbij k_0 als endomorfisme linksvermenigvuldiging met k_0 is) niet injectief is.*

Bewijs. Beschouw het polynoom $X^{p^n} - X \in K[X]$. Alle elementen uit K zijn een nulpunt van dit monische polynoom en zijn graad is gelijk aan de orde van K, dus dit polynoom is te factoriseren als $\prod_{k\in K}(X - k)$. Hierdoor geldt ook dat $\prod_{k\in K}(\delta - k) = \delta^{p^n} - \delta = 0$. Schrijf de linkerkant als $(\prod_{k\in K^\times}(\delta - k)) \circ \delta$. Als voor alle $k \in K^\times$ geldt dat $\delta - k$ injectief is dan is hun samenstelling $\prod_{k\in K^\times}(\delta - k)$ dat ook, dus volgt uit $\prod_{k\in K^\times}(\delta - k) \circ \delta = 0$ dat $\delta = 0$. Maar dan zou a in het centrum liggen, een tegenspraak. □

Wegens Lemma 3.2.5 geldt dat er een $b \neq 0$ bestaat waarvoor $ab - ba = k_0 b$, dus geldt $a - k_0 = bab^{-1}$. Het is hierbij van belang dat $a - k_0 \neq a$ waardoor a en b niet commuteren. Merk verder op dat $b = k_0^{-1}(ab - ba) = a(k_0^{-1}b) - (k_0^{-1}b)a$, dus b is een commutator en heeft daarmee eindige orde.

Onder aanname van de stelling van Wedderburn zouden we nu klaar zijn.

Stelling 3.2.6. (Wedderburn). *Elke eindige delingsring is een lichaam.*

Aangezien a en b eindige orde hebben en aan de commutatierelatie $(a - k_0)b = ba$ voldoen geldt dat $K[b]$ een eindige delingsring is, maar omdat $a - k_0 \neq a$ geldt dat $K[b]$ niet commutatief is, dus dat zou een tegenspraak met de stelling van Wedderburn betekenen.

Dit is ook hoe het boek **[7]** dit bewijst. Ik streef er echter naar in deze scriptie om het bewijs voor de stelling van Jacobson-Herstein zo elementair mogelijk op te bouwen en met dank aan de bijdrage van Hendrik Lenstra kunnen we het ook op een andere manier afmaken. Dit heeft als bijkomend gevolg dat we de stelling van Wedderburn op een nieuwe manier bewijzen. In een eindige niet-commutatieve delingsring geldt immers ook dat elke niet-nul commutator een eindige orde heeft, waardoor dit een JH-ring is.

Zij m het kleinste positieve gehele getal waarvoor b^m commuteert met a. Dit bestaat aangezien b eindige orde heeft waardoor 1 een macht is van b en die commuteert met a. Beschouw nu $L = K[b^m]$ en kijk naar het deellichaam M van L dat bestaat uit alle invarianten van het automorfisme $\sigma : x \mapsto b \cdot x \cdot b^{-1}$. Het is a priori niet duidelijk dat het beeld van σ altijd in L ligt, maar aangezien σ additief en multiplicatief is, en omdat verder $\sigma(1) = 1$, $\sigma(b^m) = b^m$, $\sigma(a) = a - k_0$ geldt dat σ goed gedefinieerd is op voortbrengers waardoor σ inderdaad een automorfisme is. Dit maakt dat M het invariantenlichaam is van de ondergroep van $\mathrm{Aut}(L)$ voorgebracht door σ, waardoor L een Galoisuitbreiding is van M. Er geldt dat $\sigma^i(x) = b^i \cdot x \cdot (b^i)^{-1}$ en aangezien m de kleinste macht is waarvoor b^m commuteert met a geldt dat de orde van σ in $\mathrm{Aut}(L)$ gelijk is aan m. Dus de Galoisgroep heeft kardinaliteit m.

Kijk nu naar de normafbeelding $N : L \to M$ gegeven door $\alpha \mapsto \prod_{i=1}^{m} \sigma^i(\alpha)$. Aangezien $\sigma^i(x) = b^i \cdot x \cdot (b^i)^{-1}$ geldt dat

$$N(\alpha) = b\alpha b^{-1} \cdot b^2\alpha b^{-2} \cdot \ldots \cdot b^m\alpha b^{-m} = b\alpha \cdot b\alpha \cdot \ldots \cdot b\alpha \cdot b^{-m} = (b\alpha)^m \cdot b^{-m}.$$

Wegens Lemma 2.2.4 geldt dat de normafbeelding surjectief is, waardoor we een $c \in L$ kunnen vinden waarvoor $N(c) = b^{-m}$, oftewel $(bc)^m = 1$. Dit maakt dat

$$(bc-1)((bc)^{m-1} + (bc)^{m-2} + \ldots + bc + 1) = (bc)^m - 1 = 0.$$

Als $bc = 1$ dan zou $b = c^{-1}$ bevat zijn in L, maar b en a commuteren niet. Er geldt dus dat $bc - 1 \neq 0$ en we krijgen de relatie $(bc)^{m-1} + (bc)^{m-2} + \ldots + bc + 1 = 0$. We gaan deze relatie gebruiken om een tegenspraak te krijgen met Lemma 2.2.5. Vermenigvuldig hiervoor voor een $x \in L$ deze relatie aan de linkerkant met $\sigma^m(x) = x$, we krijgen dat

$$\sigma^m(x)(bc)^{m-1} + \sigma^m(x)(bc)^{m-2} + \ldots + \sigma^m(x)bc + x = 0.$$

We hebben de commutatierelatie $\sigma(x)bc = bcx$ welke gebruikt wordt om af te leiden dat $\sigma^m(x)(bc)^i = \sigma^i(\sigma^{m-i}(x))(bc)^i = (bc)^i\sigma^{m-i}(x)$. Hiermee kunnen we dit omschrijven tot

$$(bc)^{m-1}\sigma(x) + (bc)^{m-2}\sigma^2(x) + \ldots + bc\sigma^{m-1}(x) + x = 0.$$

We hebben dus een relatie tussen elementen uit de Galoisgroep, wat wegens Lemma 2.2.5 betekent dat alle coëfficiënten gelijk aan 0 moeten zijn (waardoor in feite geldt dat $L[b] = \bigoplus_{i=1}^{m} L(bc)^i$). Maar $1 \neq 0$, dus we krijgen inderdaad een tegenspraak. □

3.3 Linksprimitieve ringen

Het boek **[7]** gebruikt hier de volledige Jacobson density theorem, maar we hebben daarvan slechts een deel nodig.

Stelling 3.3.1. *Zij R een linksprimitieve JH-ring, dan is R commutatief.*

Bewijs. R is linksprimtief, dus zij V een trouw simpel R moduul. Zij verder k de ring $\mathrm{End}_R(V)$. Wegens Lemma 2.3.3 geldt dat k een delingsring is. De natuurlijke afbeelding $R \to \mathrm{End}_k(V)$ is injectief want de kern is de annihilator van V. Er geldt dus dat R een deelring van een endomorfismering is. We onderscheiden twee gevallen.

Stel eerst dat $\dim_k V = 1$, dus $\mathrm{End}_k(V) \cong k^{opp}$. Zij $v_0 \in V \setminus \{0\}$, aangezien V simpel is moet gelden dat $R \cdot v_0 = V$ dus voor alle $\phi \in k^{opp}$ en alle $r \cdot v_0 \in R \cdot v_0 = V$ geldt dat $\phi(r \cdot v_0) = r \cdot \phi(v_0)$. Ieder endomorfisme in k^{opp} ligt dus vast door zijn werking op v_0. Aangezien linksvermenigvuldiging met r een endomorfisme van ${}_kV$ is dat v_0 stuurt naar $r \cdot v_0$ krijgen we een surjectieve afbeelding $R \to k^{opp}$. Aan de andere kant krijgen we door samenstelling van de natuurlijke afbeelding $R \to \mathrm{End}_k(V)$ en het isomorfisme $\mathrm{End}_k(V) \cong k^{opp}$ een injectieve afbeelding $R \to k^{opp}$. Dit zijn dezelfde afbeeldingen, aangezien ze beide $r \in R$ sturen naar linksvermenigvuldiging met r. We zien dus dat $R \cong k^{opp}$, waardoor we Stelling 3.2.1 kunnen gebruiken om te concluderen dat R commutatief is.

Stel nu dat $\dim_k V > 1$ en zij $v_1, v_2 \in V$ twee lineair onafhankelijke vectoren. Zij verder $V' := kv_1 + kv_2$, het opspansel van v_1 en v_2. Beschouw de deelring $R' \subset R$ gegeven door alle elementen $r \in R$ waarvoor geldt dat $r(V') \subset V'$. We gaan laten zien dat de natuurlijke afbeelding $R' \to \mathrm{End}_k(V')$ surjectief is.

Lemma 3.3.2. *De natuurlijke afbeelding $R' \to \mathrm{End}(V'_k)$ is surjectief.*

Bewijs. Zij $f \in \mathrm{End}_k(V')$. We zoeken een $r \in R$ waarvoor $f(v_1) = rv_1$ en $f(v_2) = rv_2$. Hiervoor stappen we over naar $\overline{V} := V^2$, $\overline{k} := \mathrm{End}_R(\overline{V})$ en $\overline{f} := (f, f)$. Merk op dat $\overline{k} = \mathrm{End}_R(V^2) \cong \mathbb{M}_2(\mathrm{End}_R(V)) = \mathbb{M}_2(k)$. We gaan laten zien dat $\overline{f} \in \mathrm{End}_{\overline{k}}(\overline{V})$. Neem hiervoor een zekere $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \overline{k}^{opp}$ (met $a, b, c, d \in k^{opp}$), dan geldt dat voor iedere $(w_1, w_2) \in \overline{V}$ dat

$$\overline{f}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(w_1, w_2)\right) = \overline{f}(w_1a + w_2b, w_1c + w_2d) = (f(w_1a + w_2b), f(w_1c + w_2d)) =$$

$$(f(w_1)a + f(w_2)b, f(w_1)c + f(w_2)d) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(f(w_1), f(w_2)) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\overline{f}(w_1, w_2).$$

Er geldt dus inderdaad dat $\overline{f} \in \mathrm{End}_{\overline{k}}(\overline{V})$. Beschouw nu het R-deelmoduul W van $\overline{V}$ voortgebracht door $(v_1, v_2) \in \overline{V}$. Aangezien $\overline{V} = V \oplus V$ geldt dat $\overline{V}$ semisimpel is, dus met Lemma 2.3.10 kunnen we een deelmoduul W' van $\overline{V}$ vinden zodat $\overline{V} = W \oplus W'$. Zij $e \in \overline{k}^{opp}$ de projectie van $\overline{V}$ op W onder deze decompositie. Hierdoor krijgen we dat $\overline{f}((v_1, v_2)) = \overline{f}(e(v_1, v_2)) = e\overline{f}((v_1, v_2) \in W$, dus $\overline{f}((v_1, v_2)) = (f(v_1), f(v_2))$ is van de vorm (rv_1, rv_2) voor een zekere $r \in R$. Daarmee hebben we inderdaad een $r \in R$ gevonden waarvoor $f(v_1) = rv_1$ en $f(v_2) = rv_2$. □

Aangezien R' een deelring is van R is het ook een JH-ring en wegens de surjectiviteit van de natuurlijke afbeelding $R' \to \mathrm{End}_k(V')$ geldt met Lemma 3.1.6 dat $\mathrm{End}_k(V') \cong \mathbb{M}_2(k)$ ook een JH-ring is. Dit kan echter niet waar zijn, er geldt namelijk voor de matrices $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ en $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ dat $ab - ba = b$ en $b^2 = 0$, dus b^n voor $n \geq 2$ kan nooit gelijk zijn aan b. Dit maakt dat $\mathbb{M}_2(k)$ geen JH-ring is, dus er bestaat helemaal geen simpele JH-ring R zodanig dat $\dim_k V > 1$. □

3.4 Semiprimitieve ringen

Stelling 3.4.1. *Zij R een semiprimitieve JH-ring, dan is R commutatief.*

Bewijs. Zij $\{\mathfrak{U}_i\}_{i \in I}$ de verzameling linksprimitieve idealen van R. Voor ieder linksprimitief ideaal $\mathfrak{U}_i$ geldt dat de quotiëntafbeelding $R \to R/\mathfrak{U}_i$ een surjectief homomorfisme is, dus wegens Lemma 3.1.6 geldt dat $R/\mathfrak{U}_i$ ook een JH-ring is. Verder geldt dat $R/\mathfrak{U}_i$ een linksprimitieve ring is, dus wegens Stelling 3.3.1 geldt dat $R/\mathfrak{U}_i$ commutatief is. Kijk dan naar de afbeelding $R \to \prod_{i \in I} R/\mathfrak{m}_i$ die gegeven is door de samenstelling van quotiëntafbeeldingen. De kern van deze afbeelding is de doorsnede van alle linksprimitieve idealen. Wegens Lemma 3.1.3 geldt dat deze doorsnede bevat is in het Jacobson radicaal, maar $\mathrm{rad}(R) = 0$ dus de afbeelding is injectief. Dat maakt R isomorf aan zijn beeld, een deelring van een commutatieve ring. Hierdoor geldt dat ook R commutatief is. □

3.5 Algemene ringen

We hebben nu voldoende tools in handen om Stelling 1.0.2, de stelling van Jacobson-Herstein, in zijn geheel te bewijzen.

Bewijs. Wegens Lemma 3.1.5 geldt dat $R/\operatorname{rad}(R)$ semiprimitief is. De bijbehorende quotiëntafbeelding is surjectief, dus wegens Lemma 3.1.6 is $R/\operatorname{rad}(R)$ ook een JH-ring. We kunnen dus Stelling 3.4.1 gebruiken om te concluderen dat $R/\operatorname{rad}(R)$ commutatief is. Er geldt hierdoor voor alle $a, b \in R$ dat $ab - ba \in rad(R)$ en wegens de voorwaarde geldt dat $(ab-ba)^n = ab - ba$, dus $(ab-ba)(1-(ab-ba)^{n-1}) = 0$. Omdat $ab - ba \in \operatorname{rad}(R)$ geldt dat $1-(ab-ba)^{n-1}$ een eenheid is, dus we krijgen dat $ab - ba = 0$ en R is inderdaad commutatief. □

4 Elementaire bewijzen

In het vorige hoofdstuk hebben we de stelling van Jacobson-Herstein bewezen. Het bewijs gebruikt een aantal geavanceerde technieken en rust veelvuldig op het keuzeaxioma aangezien we meermaals met maximale idealen werken. Er zijn daarentegen wel elementaire bewijzen op te schrijven van het gevolg dat n-ringen commutatief zijn. Een 2-ring wordt bijvoorbeeld ook wel een Boolese ring genoemd en het bewijs dat Boolese ringen commutatief zijn is een klassiek bewijs.

Stelling 4.0.1. *Elke* 2*-ring is commutatief.*

Bewijs. Merk op dat $-1 = (-1)^2 = 1$. Er geldt ook dat $0 = (x+y)^2 - (x+y) = xy + yx$, dus $xy = -yx = yx$. □

In dit hoofdstuk onderzoeken we voor welke n we op eenzelfde manier kunnen bewijzen dat alle n-ringen commutatief zijn. Hiervoor ontwikkelen we eerst een aantal algemene technieken. Dit zijn generalisaties van de technieken uit de presentatie van Mike Daas **[2]**.

4.1 Algemene technieken

Definitie 4.1.1. *Een polynoom $P(x) \in \mathbb{Z}[x]$ over een ring R is* centraal *als voor elke $r \in R$ geldt dat $P(r)$ centraal is. Zij voor het gemak $Z_R \subset \mathbb{Z}[x]$ de verzameling centrale polynomen over R.*

Lemma 4.1.2. *Zijn $P(x), Q(x) \in \mathbb{Z}[x]$ centraal over R en zij $S(x) \in \mathbb{Z}[x]$ een polynoom. Dan geldt dat $P(x) + Q(x)$, $S(P(x))$ en $P(S(x))$ centraal zijn.*

Bewijs. Aangezien $Z(R)$ gesloten is onder optellen geldt dat $P(x) + Q(x) \in Z_R$. Omdat de coëfficiënten van $S(x)$ in het centrum zitten en het centrum gesloten is onder optellen en vermenigvuldiging geldt dat ook $S(P(x))$ centraal is. Verder geldt dat het beeld van $P(S(x))$ bevat is in het beeld van $P(x)$ en het beeld van $P(x)$ zat al in het centrum, dus $P(S(x)) \in Z_R$. □

Opmerking 4.1.3. Met andere woorden, de verzameling centrale polynomen over een ring R is een ideaal van de bijna-ring $\mathbb{Z}[x]$ onder optelling en samenstelling. We noemen $\mathbb{Z}[x]$ onder optelling en samenstelling een bijna-ring, aangezien aan alle ringaxioma's behalve linksdistributiviteit voldaan wordt.

Onze aanpak zal zijn om naar centrale polynomen te kijken. Zo geldt bijvoorbeeld in een n ring dat $x^n - x$ een centraal polynoom is, want dat is altijd gelijk aan 0. Dit is natuurlijk een triviaal feit, maar we kunnen hier met Lemma 4.1.2 ook andere centrale polynomen uit afleiden. We zullen dit regelmatig gaan gebruiken om uit $P(x) \in Z_R$ af te leiden dat ook $P(x+1) - P(x) - P(1) + P(0) \in Z_R$. Het is best vaak handig dit toe te passen, want hierdoor reduceren we de graad van het polynoom waar we mee werken en we willen natuurlijk uiteindelijk laten zien dat x een centraal polynoom is. Vandaar dat we deze operatie formeel definiëren.

Definitie 4.1.4. *Definieer $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ als $\phi(P(x)) = P(x+1) - P(x) - P(1) + P(0)$.*

Lemma 4.1.5. *Zij n een even positief geheel getal. Dan heeft iedere n-ring karakteristiek 1 of 2.*

Bewijs. Er geldt $-1 = (-1)^n = 1$. □

Lemma 4.1.6. *In een n-ring geldt voor iedere $k \geq 0$ dat $x = x^{n^k}$*

Bewijs. Er geldt $x = x^n = (x^n)^n = x^{n^2} = \ldots = x^{n^k}$. □

Er geldt zelfs iets sterkers.

Lemma 4.1.7. *In een n-ring R geldt voor iedere $k \geq 0$ dat $x = x^{k(n-1)+1}$.*

Bewijs. We bewijzen dit met inductie. Voor $k = 0$ staat er dat $x = x$ en dat is waar. Verder geldt wanneer $x = x^{k(n-1)+1}$ ook dat

$$x = x^{k(n-1)} \cdot x = x^{k(n-1)} \cdot x^n = x^{(k+1)(n-1)+1}.$$

Er geldt dus inderdaad dat $x = x^{k(n-1)+1}$. □

Gevolg 4.1.8. *Een n-ring is in het bijzonder een $k(n-1)+1$-ring. Elke m waarvoor geldt dat $m \equiv 1 \mod n-1$ kunnen we schrijven als $k(n-1)+1$ voor een zekere $k \geq 0$, dus volgt dat als we voor zo een m hebben bewezen dat iedere m-ring commutatief is, dat elke n-ring dat dan ook is.*

Lemma 4.1.9. *In een gereduceerde ring geldt dat idempotenten centraal zijn.*

Bewijs. Zij $e \in R$ idempotent, dan geldt voor alle $x \in R$ dat

$$(exe - ex)^2 = exexe - exex - exexe + exex = 0.$$

Aangezien R gereduceerd is volgt dat $exe = ex$. Analoog krijgen we ook $exe = xe$, dus $ex = xe$. Dit betekent dat e in het centrum zit. □

Lemma 4.1.10. *Voor $n \geq 2$ geldt dat iedere n-ring R gereduceerd is.*

Bewijs. Stel dat we een $x \in R$ hebben met $x^2 = 0$. Aangezien R een n-ring is geldt dat $x = x^n = x^2 \cdot x^{n-2} = 0$, dus R is gereduceerd. □

Lemma 4.1.11. *In iedere n-ring R is het polynoom x^{n-1} centraal.*

Bewijs. Er geldt dat $(x^{n-1})^2 = x^{2n-2} = x^n \cdot x^{n-2} = x \cdot x^{n-2} = x^{n-1}$, dus x^{n-1} is idempotent. Wegens Lemma 4.1.10 en Lemma 4.1.9 geldt nu dat x^{n-1} centraal is. □

Lemma 4.1.12. *In een n-ring R geldt voor $d = \gcd\{m^n - m | m \in \mathbb{N}\}$ dat d een deler is van de karakteristiek van R.*

Bewijs. De n-ring voorwaarde vertelt ons dat voor alle $m \in \mathbb{N}$ en $\overline{m} = 1_R + \ldots + 1_R$ (de som van m énen in de ring) geldt dat $\overline{m}^n - \overline{m} = 0_R$. Aangezien $\overline{m}^n - \overline{m} = \overline{m^n - m}$ geldt dat $m^n - m$ een deler is van de karakteristiek van R. Omdat d een eindig aantal priemfactoren heeft, bestaat er een eindige verzameling $A \subset \{m^n - m | m \in \mathbb{N}\}$ waarvoor $d = \gcd A$, dus met Bezout op de elementen van $\overline{A}$ krijgen we dat $\overline{d} = 0_R$. □

Lemma 4.1.13. *De d uit het vorige lemma is gelijk aan het product van alle p priem waarvoor $p - 1 | n - 1$.*

Bewijs. Merk allereerst op dat d kwadraatvrij is, want als voor een zeker priemgetal p zou gelden dat $p^2 | d$, dan moet ook gelden dat $p^2 | p^n - p = p(p^{n-1} - 1)$, maar $p^{n-1} - 1$ is helemaal niet deelbaar door p, tegenspraak. Zij p nu een priemgetal met $p | d$ en zij $\overline{a}$ een voortbrenger van $(\mathbb{Z}/p\mathbb{Z})^\star$. Dan geldt dat $a^n - a \equiv 0 \mod p$, dus $a^{n-1} \equiv 1 \mod p$ en aangezien a een orde heeft van $p - 1$ volgt dat $p - 1 | n - 1$. Verder geldt dat alle p met $p - 1 | n - 1$ ook daadwerkelijk een deler zijn van d, aangezien voor alle $p | m$ geldt dat $p | m^n - m$ en als $p \not| m$ dan geldt dat $m^n \equiv (m^{p-1})^{\frac{n-1}{p-1}} \cdot m \equiv m \mod p$. □

Lemma 4.1.14. *In een n-ring R geldt dat $\phi^{n-2}(x^{n-1}) = (n-1)!x$ een centraal polynoom is.*

Bewijs. We weten dat $x^{n-1} \in Z_R$. Beschouw nu $\phi^{n-2}(x^{n-1})$. Aangezien ϕ de graad van een niet-constant polynoom doet afnemen geldt dat de graad van $\phi^{n-2}(x^{n-1})$ maximaal gelijk is aan $n - 1 - (n - 2) = 1$. Omdat er per constructie geen constante coëfficiënt voorkomt in het beeld van ϕ, geldt dat $\phi^{n-2}(x^{n-1})$ een graad 1 monoom is. De coëfficiënt van dit monoom kunnen we uitrekenen door in iedere stap de kopcoëfficiënt te bekijken. Wegens het binomium van Newton geldt dat deze in iedere stap met de graad van het polynoom wordt vermenigvuldigd, dus we krijgen dat $\phi^{n-2}(x^{n-1}) = (n-1)!x$. Met Lemma 4.1.2 volgt dat $(n-1)!x$ centraal is. □

Opmerking 4.1.15. In de meeste gevallen is Lemma 4.1.12, waaruit volgt dat dx centraal is, strikt krachtiger dan Lemma 4.1.14. Maar als n een priemgetal is geldt dat $n | d$ wegens de kleine stelling van Fermat, terwijl n dan natuurlijk geen deler is van $(n-1)!$. Hierdoor kunnen we met Bezout laten zien dat $\frac{d}{n}x$ centraal is.

Lemma 4.1.16. *Als $x^2 + x$ een centraal polynoom is in de ring R dan is R commutatief.*

Bewijs. Als het polynoom $p(x) = x^2 + x$ centraal is dan is voor alle $y \in R$ het polynoom $p(x+y) - p(x) - p(y) = xy + yx$ ook centraal (in feite is $xy + yx$ een centraal polynoom in twee variabelen). In het bijzonder geldt dan dat $x(xy + yx) = (xy + yx)x$, waaruit volgt dat $x^2y = yx^2$. Dit betekent dat x^2 centraal is, dus ook $(x^2 + x) - x^2 = x$. □

4.2 Kleine gevallen

Met alle opgebouwde technieken uit de vorige paragraaf kunnen we beginnen met het bewijzen van een aantal kleine gevallen.

Stelling 4.2.1. *Elke* 3*-ring is commutatief.*

Bewijs. Wegens opmerking 4.1.15 geldt dat $2x$ centraal is. Uit Lemma 4.1.2 volgt dat $\phi(x^3 - x) = 3x^2 + 3x$ centraal is, dus $x^2 + x \in Z_R$. Wegens Lemma 4.1.16 zijn we klaar. □

Stelling 4.2.2. *Elke* 4*-ring is commutatief.*

Bewijs. Er geldt dat $(x^2 + x)^2 = x^2 + x$, dus wegens Lemma 4.1.9 is $x^2 + x$ centraal en met Lemma 4.1.16 zijn we klaar. □

Stelling 4.2.3. *Elke* 5*-ring is commutatief.*

Bewijs. Wegens opmerking 4.1.15 geldt dat $6x$ centraal is. Uit Lemma 4.1.2 volgt dat $\phi(x^5 - x) = 5x^4 + 4x^3 + 4x^2 + 5x \in Z_R$. Maar we weten al dat x^4 centraal is, dus ook $\phi(4x^3 + 4x^2 + 5x) = 12x^2 + 20x$ is centraal. Daaruit volgt $2x \in Z_R$ en als we dat combineren met $4x^3 + 4x^2 + 5x \in Z_R$ dan krijgen we dat $x \in Z_R$. □

Stelling 4.2.4. *Elke* 6*-ring is commutatief.*

Bewijs. Uit Lemma 4.1.2 volgt dat $\phi(x^5) = 5x^4 + 10x^3 + 10x^2 + 5x = x^4 + x \in Z_R$ en $\phi(x^6 - x) = 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x = x^4 + x^2 \in Z_R$. Hieruit volgt dat $(x^4 + x) + (x^4 + x^2) = x^2 + x$ centraal is, dus wegens Lemma 4.1.16 zijn we klaar. □

Stelling 4.2.5. *Elke* 7*-ring is commutatief.*

Bewijs. Wegens opmerking 4.1.15 geldt dat $6x$ centraal is. Uit Lemma 4.1.2 volgt dat $\phi(x^6) = 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x \in Z_R$, dus $3x^4 + 2x^3 + 3x^2 \in Z_R$. Als we dit polynoom verdubbelen dan krijgen we dat $4x^3 \in Z_R$. Er geldt dat

$$\phi^2(x^7 - x) = \phi(7x^6 + 21x^5 + 35x^4 + 35x^3 + 21x^2 + 7x) =$$

$$42x^5 + 210x^4 + 490x^3 + 630x^2 + 434x \in Z_R.$$

Daaruit volgt dat $4x^3 + 2x \in Z_R$ en omdat $4x^3$ centraal is dus ook $2x$ centraal. Uit $7x^6 + 21x^5 + 35x^4 + 35x^3 + 21x^2 + 7x \in Z_R$ volgt nu dat $x^5 + x^4 + x^3 + x^2 + x \in Z_R$. Dan geldt ook dat $(x^3)^5 + (x^3)^4 + (x^3)^3 + (x^3)^2 + (x^3) = 2x^6 + 3x^3 \in Z_R$, dus ook $x^3 \in Z_R$. Nu geldt dat $\phi(x^3) = 3x^2 + 3x \in Z_R$, dus ook $x^2 + x \in Z_R$. Wegens Lemma 4.1.16 zijn we klaar. □

4.3 Enkele oneindige families

Het bewijs voor $n = 6$ blijkt te generaliseren, middels de volgende stelling. Deze stelling is een generalisatie van een stelling uit de presentatie van Mike Daas **[2]**.

Stelling 4.3.1. *Voor $k, l \geq 1$ geldt dat elke $2^k + 2^l$-ring een $2^{\gcd(k+1,l+1)}$-ring is en andersom.*

Bewijs. Allereerst geldt dat

$$2^k + 2^l \equiv 2^{-1} \cdot (2^{k+1} + 2^{l+1}) \equiv 2^{-1} \cdot (1+1) \equiv 1 \mod 2^{\gcd(k+1,l+1)} - 1.$$

Met Gevolg 4.1.8 zien we dat alle $2^{\gcd(k+1,l+1)}$-ringen ook $2^k + 2^l$-ringen zijn. Anderzijds, beschouw een $2^k + 2^l$-ring. Door $x + 1$ in te vullen en Lemma 4.1.5 te gebruiken krijgen we dat

$$x^{2^k+2^l} + 1 = x + 1 = (x+1)^{2^k+2^l} = (x+1)^{2^k}(x+1)^{2^l} =$$

$$(x^{2^k} + 1)(x^{2^l} + 1) = x^{2^k+2^l} + x^{2^k} + x^{2^l} + 1.$$

Hieruit volgt dat $x^{2^k} = x^{2^l}$, waardoor geldt dat $x = x^{2^k+2^l} = x^{2^k} \cdot x^{2^l} = x^{2^{k+1}}$ en analoog ook $x = x^{2^{l+1}}$. Via Bezout bestaan er $p, q \in \mathbb{Z}$ met $p(k+1) + q(l+1) = \gcd(k+1, l+1)$. Aangezien $k+1$ en $l+1$ groter of gelijk aan $\gcd(k+1, l+1)$ zijn is precies één van p en q niet-positief. Neem zonder verlies van algemeenheid aan dat $q \leq 0$. Dan geldt dat

$$x = x^{(2^{k+1})^p} = x^{2^{p(k+1)}} = x^{2^{\gcd(k+1,l+1)+|q|(l+1)}} = x^{2^{\gcd(k+1,l+1)} \cdot 2^{|q|(l+1)}} =$$

$$(x^{2^{|q|(l+1)}})^{2^{\gcd(k+1,l+1)}} = (x^{(2^{l+1})^{|q|}})^{2^{\gcd(k+1,l+1)}} = x^{2^{\gcd(k+1,l+1)}}.$$

Dit voltooit de equivalentie. □

Aangezien we de gevallen $n = 2$ en $n = 4$ reeds bewezen hebben zijn we in een klap klaar voor alle $n = 2^k + 2^l$ met $\gcd(k+1, l+1) \in \{1, 2\}$. In het bijzonder hebben we hiermee de oneindige families $n = 2^m + 2$ en $n = 3 \cdot 2^m$ voor $m \geq 1$ bewezen (door respectievelijk $k = m, l = 1$ en $k = m, l = m+1$ te kiezen).

4.4 Priemmachten

In deze paragraaf kijken we naar p^n-ringen. Dit is gebaseerd op het artikel van Martin Brandenbrug **[1]**, maar Lemma 4.4.1 bewijzen we, in tegenstelling tot Brandenburg, door gebruik te maken van de door ons opgebouwde technieken. Het bewijs van Brandenburg is korter (hij laat zien dat $\mathbb{F}_p[x^{p^{n-1}} + \ldots + x^p + x]$ als ring voortgebracht is door idempotenten), maar zoals later zal blijken geeft dit bewijs meer inzicht in waar onze technieken toe in staat zijn.

Lemma 4.4.1. *Voor een priemgetal p en een geheel getal n met $\gcd(p, n) = 1$ geldt in elke p^n-ring met $p = 0$ dat $x^{p^{n-1}} + x^{p^{n-2}} + \ldots + x^p + x$ centraal is.*

Bewijs. Definieer voor het gemak $P(x) = x^{p^{n-1}} + x^{p^{n-2}} + \ldots + x^p + x$ en beschouw het polynoom $P(x)^{p-1}$. We weten al dat x^{p-1} centraal is, dus met Lemma 4.1.2 geldt dat $P(x)^{p-1} \in Z_R$. We gaan laten zien dat $\phi^{p-2}(P(x)^{p-1}) = -n^{-1}P(x)$. Hiervoor gaan we kijken naar $\mathbb{F}_{p^n}$, wat duidelijk een p^n-ring is met $p = 0$. De graad van $P(x)^{p-1}$ is $p^n - p < p^n$, dus zijn alle resulterende polynomen uniek bepaald door de waardes die ze aannemen op $\mathbb{F}_{p^n}$. We gaan aantonen dat $\phi^{p-2}(P(x)^{p-1})$ en $-n^{-1}P(x)$ op ieder element van $\mathbb{F}_{p^n}$ dezelfde waarde aannemen. Daarvoor hebben we eerst een aantal lemma's nodig.

Lemma 4.4.2. *Voor $\alpha, \beta \in \mathbb{F}_{p^n}$ geldt dat $P(\alpha + \beta) = P(\alpha) + P(\beta)$ en $P(\alpha) \in \mathbb{F}_p$.*

Bewijs. Er geldt dat

$$P(\alpha+\beta) = (\alpha+\beta)^{p^{n-1}} + \ldots + (\alpha+\beta) = \alpha^{p^{n-1}} + \ldots + \alpha + \beta^{p^{n-1}} + \ldots + \beta = P(\alpha) + P(\beta).$$

Verder geldt dat $P(x)^p = (x^{p^{n-1}} + \ldots + x^p + x)^p = x^{p^{n-1}} + \ldots + x^p + x = P(x)$. Dus voor alle $\alpha \in \mathbb{F}_{p^n}$ geldt dat $P(\alpha)$ een nulpunt is van het polynoom $x^p - x$. We weten dat de verzameling nulpunten van $x^p - x$ precies gelijk is aan $\mathbb{F}_p$, dus $P(\alpha) \in \mathbb{F}_p$. □

Lemma 4.4.3. *Voor alle $\alpha \in \mathbb{F}_{p^n}$ bestaat er precies één $k \in \mathbb{F}_p$ zodanig dat $\alpha + k$ een nulpunt is van $P(x)$.*

Bewijs. Voor $k \in \mathbb{F}_p$ geldt dat $P(\alpha + k) = P(\alpha) + P(k) = P(\alpha) + nk$ en dit is gelijk aan 0 dan en slechts dan als $k = -n^{-1}P(\alpha)$. □

Zij X de verzameling nulpunten van $P(x)$ in $\mathbb{F}_{p^n}$. Voor $\alpha \in \mathbb{F}_{p^n} \setminus X$ geldt dus dat $P(\alpha) \in \mathbb{F}_p^\times$, waardoor $P(\alpha)^{p-1} = 1$. We gaan nu $\phi^{p-2}(P(x)^{p-1})$ uitrekenen.

Lemma 4.4.4. *Voor $k \in \mathbb{F}_p$, $\alpha \in X$ en $i \geq 0$ geldt dat*

$$\phi^i(P(x)^{p-1})(\alpha + k) = \phi^i(P(x)^{p-1})(k).$$

Bewijs. We bewijzen dit met inductie naar i. Voor $i = 0$ geldt er dat

$$P(x)^{p-1}(\alpha + k) = P(\alpha + k)^{p-1} = (P(\alpha) + P(k))^{p-1} = P(k)^{p-1} = P(x)^{p-1}(k).$$

Dus voor $i = 0$ zijn we klaar. Neem nu aan dat we de bewering bewezen hebben voor $i = m$ en bekijk de bewering voor $i = m + 1$. Zij $Q(x) = \phi^m(P(x)^{p-1})$. Dan geldt dat

$$\begin{aligned}\phi^{m+1}(P(x)^{p-1})(\alpha+k) = \phi(Q(x))(\alpha+k) =& (Q(x+1) - Q(x) - Q(1))(\alpha+k) = \\ Q(\alpha+k+1) - Q(\alpha+k) - Q(1) =& Q(k+1) - Q(k) - Q(1) = \\ (Q(x+1) - Q(x) - Q(1))(k) = \phi(Q(x))(k) =& \phi^{m+1}(P(x)^{p-1})(k).\end{aligned}$$

Daarmee is de inductiestap en dus het lemma bewezen. □

Wegens Lemma 4.4.3 en Lemma 4.4.4 volstaat het om $\phi^{p-2}(P(x)^{p-1})$ uit te rekenen als we het domein beperken tot $\mathbb{F}_p$. Voor $k \in \mathbb{F}_p$ geldt dat $P(x)^{p-1}(k) = x^{p-1}(k)$ (namelijk 0 als $k = 0$ en 1 anders). Dat betekent ook dat $\phi^{p-2}(P(x)^{p-1})(k) = \phi^{p-2}(x^{p-1})(k)$. Met Lemma 4.1.14 en de stelling van Wilson volgt $\phi^{p-2}(x^{p-1}) = (p-1)!x = -x$. Door de

bovenstaande lemma's te combineren kunnen we nu $\phi^{p-2}(P(x)^{p-1})$ geheel uitrekenen. Wegens Lemma 4.4.3 geldt dat elk element van $\mathbb{F}_{p^n}$ te schrijven is als $\alpha + k$ met $\alpha \in X$ en $k \in \mathbb{F}_p$. Met Lemma 4.4.4 krijgen we $\phi^{p-2}(P(x)^{p-1})(\alpha + k) = \phi^{p-2}(P(x)^{p-1})(k) = -k$. Anderzijds geldt ook dat $-n^{-1}P(\alpha + k) = -n^{-1}(P(\alpha) + P(k)) = -n^{-1}(nk) = -k$. Dus er geldt dat $\phi^{p-2}(P(x)^{p-1}) = -n^{-1}P(x)$. We concluderen dat $x^{p^{n-1}} + \ldots + x$ een centraal polynoom is. □

Met dit lemma volgt direct dat als in een p-ring geldt $p = 0$, die ring dan commutatief is. In een p^2-ring met $p = 0$ kunnen we dat hier ook uit ook afleiden, maar dan moeten we wel met twee variabelen gaan werken.

Stelling 4.4.5. *Als voor een priem p in een p^2-ring R geldt dat $p = 0$, dan is R commutatief.*

Bewijs. Het geval $p = 2$ hebben we al bewezen, dus neem aan dat $p \neq 2$.

Definitie 4.4.6. *Definieer $[x^i y^j]$ als de som van alle monomen waar x precies i keer in voorkomt en y precies j keer. Hierdoor geldt dat $(x + y)^n = \sum_{i=0}^{n} [x^i y^{n-i}]$.*

Uit Lemma 4.4.1 volgt dat $(x + y)^p + (x + y) - (x^p + x) - (y^p + y) = \sum_{i=1}^{p-1} [x^i y^{p-i}]$ centraal is. Voor $\lambda \in \mathbb{F}_p$ kunnen we x vervangen door λx en dan krijgen we dat $\sum_{i=1}^{p-1} \lambda^i [x^i y^{p-i}]$ centraal is. We gaan nu al deze centrale polynomen bij elkaar optellen. Wegens Lemma 2.4.5 geldt dat

$$\sum_{\lambda=1}^{p-1} \sum_{i=1}^{p-1} \lambda^i [x^i y^{p-i}] = \sum_{i=1}^{p-2} [x^i y^{p-i}] \left(\sum_{\lambda=1}^{p-1} \lambda^i \right) + \left(\sum_{\lambda=1}^{p-1} \lambda^{p-1} \right) [x^{p-1} y] = (p-1)[x^{p-1} y].$$

Hierdoor geldt dat $[x^{p-1}y]$ centraal is. Aangezien $[x^{p-1}y] = x^{p-1}y + \ldots + yx^{p-1} \in Z_R$ geldt dat $x(x^{p-1}y + \ldots + yx^{p-1}) = (x^{p-1}y + \ldots + yx^{p-1})x$. Gelijke termen wegstrepen aan beide kanten geeft dat $x^p y = yx^p$. Dit geldt voor alle $x, y \in R$, dus x^p is centraal. Daaruit volgt dat ook $(x^p + x) - x^p = x$ centraal is. □

Helaas is dit bewijs niet makkelijk te generaliseren naar hogere priemmachten. Om te laten zien hoe gecompliceerd het bewijs voor hogere priemmachten kan worden, presenteren we hier het bewijs voor $n = 8$ uit het artikel van Yoshihito Morita **[8]**.

Stelling 4.4.7. *Elke 8-ring is commutatief.*

Bewijs. Aangezien $(x^4 + x^2 + x)^2 = x^4 + x^2 + x$ volgt uit Lemma 4.1.9 dat $x^4 + x^2 + x$ centraal is. Hierdoor geldt dat

$$(x + y)^4 + (x + y)^2 + (x + y) - (x^4 + x^2 + x) - (y^4 + y^2 + y) = \sum_{i=1}^{3} [x^i y^{4-i}] + xy + yx$$

ook centraal is. Dus hebben we

$$\left(\sum_{i=1}^{3} [x^i y^{4-i}] + xy + yx \right) y = y \left(\sum_{i=1}^{3} [x^i y^{4-i}] + xy + yx \right).$$

Door gelijke termen weg te strepen (elke term die begint en eindigt met een y komt aan beide kanten voor) en te gebruiken dat $(x^4+x^2+x)y = y(x^4+x^2+x)$ krijgen we dat

$$x\left(\sum_{i=1}^{3}[x^{i-1}y^{4-i}]\right)y + xy^2 = y\left(\sum_{i=1}^{3}[x^{i-1}y^{4-i}]\right)x + y^2x.$$

Schrijf nu beide kanten uit en gebruik dat $x(y^4+y^2+y) = (y^4+y^2+y)x$. We krijgen dat

$$\begin{aligned} x^2y^3 + xyxy^2 + xy^2xy + x^3y^2 + x^2yxy + xyx^2y + xy = \\ y^3x^2 + y^2xyx + yxy^2x + y^2x^3 + yxyx^2 + yx^2yx + yx. \end{aligned} \tag{1}$$

Vervang in deze vergelijking x door xy en vermenigvuldig de vergelijking aan de rechterkant met y^6. Aangezien y^7 centraal is kunnen we in termen met een y^7 deze wegwerken als er in de term ook nog een andere y aanwezig is. We krijgen dat

$$\begin{aligned} xyxy^3 + xy^2xy^2 + xy^3xy + xyxyxy^2 + xyxy^2xy + xy^2xyxy + xy = \\ yxy^3x + y^2xy^2x + y^3xyx + yxyxy^2x + yxy^2xyx + y^2xyxyx + yx. \end{aligned} \tag{2}$$

Vervang nu y door y^7+y en haal er vergelijkingen (1) en (2) van af. Versimpelen geeft dat

$$\begin{aligned} xyx^2y^2 + x^2y^2xy + x^2yxy^2 + xy^2x^2y + xy = \\ yxy^2x^2 + y^2x^2yx + yx^2y^2x + y^2xyx^2 + yx. \end{aligned} \tag{3}$$

Vervang nu x achtereenvolgens door x^2, x^4 en x^4+x^2 en tel alle resulterende vergelijkingen bij elkaar op. We krijgen dat

$$\begin{aligned} xyx^2y^2 + x^2y^2xy + x^2yxy^2 + xy^2x^2y = \\ yxy^2x^2 + y^2x^2yx + yx^2y^2x + y^2xyx^2. \end{aligned} \tag{4}$$

Door vergelijking (3) en vergelijking (4) te combineren vinden we nu dat $xy = yx$. □

4.5 Welke n ontbreken nog?

We hebben inmiddels een bewijs voor alle $n \leq 8$. Voor $n = 9$ kunnen we Lemma 4.4.1 niet toepassen, want we weten immers nog niet dat $3 = 0$. Sterker nog, dat hoeft helemaal niet te gelden aangezien $\mathbb{F}_2$ en $\mathbb{F}_5$ beide 9-ringen zijn. In het algemeen geldt dat $\mathbb{F}_{p^m}$ een p^m-ring is en met Lemma 4.1.8 ook een $k(p^m-1)+1$-ring voor alle $k \geq 1$. Als we dus voor een zekere n willen weten welke eindige lichamen een n-ring zijn dan moeten we kijken naar de priemgetallen p waarvoor $p-1|n-1$. De technieken uit paragraaf 4.1 kunnen prima werken als er veel eindige lichamen een n-ring zijn, zo hebben we bijvoorbeeld het geval $n = 7$ bewezen terwijl $\mathbb{F}_2$, $\mathbb{F}_3$ en $\mathbb{F}_7$ een 7-ring zijn. Maar onze technieken hebben wel limitaties zodra er een $\mathbb{F}_{p^m}$ met $m > 1$ bestaat die een n-ring is. Onze strategie is om telkens te beginnen met de centrale polynomen $x^n - x$ en x^{n-1} en vervolgens Lemma 4.1.2 toe te passen, maar op het lichaam $\mathbb{F}_{p^m}$ geldt

dat deze enkel waardes in $\mathbb{F}_p$ aannemen. Ook voor alle resulterende polynomen na toepassing van Lemma 4.1.2 geldt dat hun beeld bevat is in $\mathbb{F}_p$. Op deze manier kunnen we dus nooit het centraal zijn van x aantonen. We zullen in dat geval dus ergens iets met meerdere variabelen moeten doen, zoals Lemma 4.1.16. Dit is duidelijk terug te zien in het bewijs van Stelling 4.4.5: Lemma 4.4.1 haalt het maximale uit Lemma 4.1.2 en daarna gaan we iets met twee variabelen doen.

In zijn artikel doet Morita het geval $n = 9$ wel, maar hij geeft geen bewijs voor de tweemachten vanaf 16. De tweemachten zijn trouwens voldoende om alle even n te bewijzen. Voor alle even n geldt immers dat $n-1$ een deler is van $2^a - 1$, met a de orde van 2 modulo $n-1$. Hierdoor is elke n-ring ook een 2^a-ring. Het is overigens best vaak mogelijk te reduceren tot een kleinere tweemacht door gebruik te maken van Stelling 4.3.1. Als je twee natuurlijke getallen $k, l \geq 1$ hebt zodanig dat $2^k + 2^l \equiv 1 \mod n-1$ dan geldt dat iedere n-ring ook een $2^k + 2^l$-ring is en dus met Stelling 4.3.1 ook een $2^{\text{ggd}(k+1,l+1)}$-ring. Door $k = l = a - 1$ te kiezen krijgen we dat elke n-ring ook een 2^a ring is, maar regelmatig bestaan er k en l die tot een kleinere tweemacht doen reduceren. Dat geldt bijvoorbeeld voor $n = 14$ en $n = 20$: als we enkel de orde van 2 modulo $n-1$ bekijken kunnen we slechts concluderen dat elke 14 ring een 2^{12}-ring is en elke 20-ring een 2^{18}-ring, maar aangezien $2^1 + 2^6 \equiv 2 - 1 \equiv 1 \mod 13$ en $2^2 + 2^4 \equiv 4 + 16 \equiv 1 \mod 19$ geldt dat zowel elke 14-ring als iedere 20-ring eigenlijk 2-ringen zijn. Aangezien we het geval $n = 2$ reeds bewezen hebben zijn we voor $n = 14$ en $n = 20$ dus ook klaar. De gevallen $n = 11, 13$ en 19 zijn niet in deze scriptie opgenomen omdat hun bewijs niet veel toevoegt, maar deze zijn op vergelijkbare wijzen als in paragraaf 4.2 te bewijzen. Al met al levert dat deze tabel op van de $n \leq 20$ waarvoor met de technieken uit deze scriptie te bewijzen is dat alle n-ringen commutatief zijn:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
bewijs?	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓

5 Referenties

[1] M. Brandenburg, *Equational proofs of Jacobson's theorem*, 2310.05301, arXiv, math.RA, `https://arxiv.org/abs/2310.05301`, 2023.

[2] M. Daas, *Jacobson's Commutativity Theorem*, `https://pub.math.leidenuniv.nl/~daasma/Jacobson_Theorem.pdf`, 2021.

[3] I. Herstein, *A Generalization of a Theorem of Jacobson*, American Journal of Mathematics, vol. 73, no. 4, p756–p762, 1951.

[4] I. Herstein, *A Generalization of a Theorem of Jacobson III*, American Journal of Mathematics, vol. 75, no. 1, p105–p111, 1953.

[5] I. Herstein, *Wedderburn's Theorem and a Theorem of Jacobson*, American Journal of Mathematics, vol. 68, no. 3, p249–p251, 1961.

[6] N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Annals of Mathematics, Vol. 46, No. 4, p695-p707, 1945.

[7] T. Y. Lam, *A first course in noncommutative rings*, Springer Science+Business Media, New York, 2001.

[8] Y. Morita, *Elementary Proofs of the Commutativity of Rings satisfying* $x^n = x$, Memoirs of the Defence Academy, Vol. XVIII, No. 1, p1-p24, 1978.