Rosa Schwarz

r.m.schwarz@umail.leidenuniv.nl

Idempotenten in groepenringen

Bachelorscriptie

Scriptiebegeleider: Prof. Dr. H.W. Lenstra

Datum Bachelorexamen: 24 juni 2015

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

1 Inleiding

Een *idempotent* in een ring R is een element $x \in R$ waarvoor geldt $x^2 = x$. Voorbeelden van idempotenten in een willekeurige ring zijn 0 en 1. Wat kan er in het algemeen gezegd worden over $\mathrm{Id}(R) := \{x \in R \mid x^2 = x\}$, de verzameling idempotenten in een ring R?

In het bijzonder zijn we geïnteresseerd in de idempotenten in groepenringen. Voor een ring R en een groep G, zijn elementen in de groepenring $R[G]$ eindige sommen $\sum_{\sigma \in G} a_\sigma \sigma$ met $a_\sigma \in R$ en $\sigma \in G$. Duidelijk is er een natuurlijke inclusie $\mathrm{Id}(R) \subset \mathrm{Id}(R[G])$, maar wanneer zijn deze verzamelingen gelijk? Noteren we de eenhedengroep van de ring R als R^*, dan bewijzen we de volgende stelling voor commutatieve samenhangende ringen, dat wil zeggen voor commutatieve ringen met $\#\,\mathrm{Id}(R) = 2$.

Stelling 1.1. *Zij R een commutatieve ring en G een eindige groep. Dan geldt $\#\,\mathrm{Id}(R[G]) = 2$ dan en slechts dan als $\#\,\mathrm{Id}(R) = 2$ en voor iedere priem p met $p|\#G$ geldt $p \cdot 1 \notin R^*$.*

Met dit resultaat kunnen we in grotere algemeenheid de volgende hoofdstelling bewijzen.

Stelling 1.2. *Zij R een commutatieve ring en G een eindige groep. Dan geldt $\mathrm{Id}(R) = \mathrm{Id}(R[G])$ dan en slechts dan als voor iedere $e \in \mathrm{Id}(R) \setminus \{1\}$ en voor elke priem $p|\#G$ geldt $pR + eR \neq R$.*

De eerste stelling geeft een nodige en voldoende voorwaarde wanneer de groepenring $R[G]$ precies 0 en 1 bevat als idempotenten. In bijvoorbeeld de ring $\mathbb{Z}$ geldt dat $\#\,\mathrm{Id}(\mathbb{Z}) = 2$. Voor deze specifieke ring kunnen we het volgende zwakkere resultaat formuleren.

Stelling 1.3. *Zij G een eindige abelse groep. Dan geldt $\mathrm{Id}(\mathbb{Z}[G]) = \{0, 1\}$.*

Doordat we hier niet alleen een specifieke ring beschouwen maar ook een abelse groep, is deze stelling duidelijk minder sterk dan de stellingen hierboven. Echter geven we wel een interessant losstaand bewijs hiervoor dat gebruik maakt van eigenschappen van de complexe getallen.

Stelling 1.1 wordt bijvoorbeeld door D. B. Coleman in [8] of door T. W. Müller in [7] stelling 7.8, bewezen voor domeinen R. In deze tekst wordt echter deze aanname niet gemaakt. Het bewijs hier gegeven maakt gebruik van projectieve modulen en Sylow-p-ondergroepen. Voor een projectief moduul kunnen we een rangafbeelding definiëren, een functie $\mathrm{Spec}\, R \to \mathbb{Z}$ van het spectrum van R naar $\mathbb{Z}$, welke we zullen gebruiken.

Stelling 1.2 beantwoordt de algemenere vraag wanneer geldt $\mathrm{Id}(R) = \mathrm{Id}(R[G])$ als we de aanname $\#\,\mathrm{Id}(R) = 2$ laten vallen. Dit laatste resultaat berust op de vorige stelling en gebruikt daardoor ook projectieve modulen. Daarnaast leiden we het af met behulp van onder andere het concept van een noetherse ring.

2 Idempotenten in $\mathbb{Z}[G]$ voor eindige abelse G

Ten eerste beschouwen we de idempotenten in de groepenring $\mathbb{Z}[G]$ voor een eindige abelse groep G. We herhalen de stelling die we gaan bewijzen.

Stelling 2.1. *Zij G een eindige abelse groep. Dan geldt* $\mathrm{Id}(\mathbb{Z}[G]) = \{0, 1\}$.

Deze stelling is niet het sterkste wat kan worden bewezen. In deze tekst wordt later bewezen dat ook voor eindige groepen G geldt $\mathrm{Id}(\mathbb{Z}[G]) = \{0, 1\}$. Ook is er bekend dat voor oneindige groepen geldt $\mathrm{Id}(\mathbb{Z}[G]) = \{0, 1\}$, zie hiervoor D. Passman [5].

Hier bewijzen we deze stelling met behulp van de complexe getallen. Door de inclusie $\mathbb{Z}[G] \subset \mathbb{C}[G]$ te beschouwen en in $\mathbb{C}[G]$ eigenschappen voor idempotenten af te leiden, kunnen we concluderen dat de idempotenten alleen 0 en 1 kunnen zijn.

Definieer $^- : \mathbb{Z}[G] \to \mathbb{Z}[G]$ door

$$\overline{\sum_{\sigma \in G} a_\sigma \sigma} = \sum_{\sigma \in G} a_\sigma \sigma^{-1}.$$

Deze afbeelding staat bekend als de *standaard-involutie* op $\mathbb{Z}[G]$. In $\mathbb{C}$ geldt kennelijk voor alle $x \in \mathrm{Id}(\mathbb{C})$ dat $\bar{x} = x$, waarbij $\bar{x}$ de complex geconjugeerde is. We zullen afleiden dat ook voor $x \in \mathrm{Id}(\mathbb{Z}[G])$ geldt dat $\bar{x} = x$.

Daartoe herhalen we eerst kort een stuk theorie van karakters van eindige abelse groepen. Zij G een eindige abelse groep.

Definitie 2.2. Een *karakter* van G is een homomorfisme $\chi : G \to \mathbb{C}^*$.

Definieer voor twee karakters $\chi_1, \chi_2 : G \to \mathbb{C}^*$ het product $\chi_1\chi_2 : G \to \mathbb{C}^*$ door $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$ voor $g \in G$. Met deze operatie is $\mathrm{Hom}(G, \mathbb{C}^*)$ een groep, de *karaktergroep van G*.

Merk op: voor $g \in G$ met orde $\mathrm{ord}(g) = n$ en $\chi : G \to \mathbb{C}^*$ een karakter geldt $\chi(g)^n = \chi(g^n) = \chi(1) = 1$. Een karakter beeldt dus af naar eenheidswortels, dat wil zeggen elementen $x \in \mathbb{C}$ waarvoor geldt dat er een $n \in \mathbb{Z}_{>0}$ bestaat zodat $x^n = 1$. In dit geval beeldt een karakter af naar e-de eenheidswortels, waar e de *exponent* is van G:

$$e = \mathrm{kgv}\{\mathrm{ord}(g) \mid g \in G\} = \min\{m \in \mathbb{Z}_{>0} \mid \forall g \in G : g^m = 1\}.$$

Laat $\zeta \in \mathbb{C}^*$ een element van orde e zijn, dan geldt dus $\hat{G} = \mathrm{Hom}(G, \langle\zeta\rangle)$.

Verder gebruiken we de volgende stelling uit de theorie over karakters, zoals deze te vinden is in bijvoorbeeld S. Lang [2] hoofdstuk 1 stelling 9.1.

Stelling 2.3. *Zij G een eindige abelse groep. Dan geldt $\#G = \#\hat{G}$.*

We willen een verband leggen tussen de conjugatie in $\mathbb{C}$ en de standaard-involutie op $\mathbb{Z}[G]$.

Voor k een commutatieve ring en R een k-algebra, geldt dat we de verzameling $\mathrm{Alg}_k(k[G], R)$ van k-lineaire ringhomomorfismen $f : k[G] \to R$ kunnen identificeren met de verzameling groepshomomorfismen $G \to R^*$.

Zij $f \in \mathrm{Alg}_k(k[G], R)$. Voor $\sigma \in G \subset k[G]$ geldt $f(\sigma)f(\sigma^{-1}) = 1$ en daarom geldt $f(\sigma) \in R^*$ voor alle $\sigma \in G$. Dan hebben we dat $f_{|G} \in \mathrm{Hom}(G, R^*)$. Voor $\chi \in \mathrm{Hom}(G, R^*)$ geldt dat

$$\chi' : k[G] \to R^*, \sum_{\sigma \in G} a_\sigma \sigma \mapsto \sum_{\sigma \in G} a_\sigma \chi(\sigma)$$

een surjectief k-lineair ringhomomorfisme is. De afbeeldingen

$$\psi : \mathrm{Alg}_k(k[G], R) \to \mathrm{Hom}(G, R^*), f \mapsto f_{|G}$$

en

$$\psi^{-1} : \mathrm{Hom}(G, R^*) \to \mathrm{Alg}_k(k[G], R), \chi \mapsto \chi'$$

zijn dan welgedefinieerde afbeeldingen en elkaars inverse. Nemen we $k = \mathbb{C}$ en $R = \mathbb{C}$, dan geeft het bovenstaande een identificatie tussen de verzameling $S = \{f : \mathbb{C}[G] \to \mathbb{C} \mid f \text{ ringhomomorfisme}, f_{|\mathbb{C}} = \mathrm{id}_{\mathbb{C}}\}$ en $\hat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$. Beschouw de productring $\mathbb{C}^{\hat{G}}$ met coördinaatsgewijze optelling en vermenigvuldiging en definieer de afbeelding ϕ als volgt:

$$\begin{aligned} &\phi : \mathbb{C}[G] \to \mathbb{C}^{\hat{G}} \\ &\sum_{\sigma \in G} a_\sigma \sigma \mapsto \left(\sum_{\sigma \in G} a_\sigma \chi(\sigma) \right)_{\chi \in \hat{G}}. \end{aligned}$$

Stelling 2.4. *De afbeelding ϕ is een ringisomorfisme.*

Bewijs. Ten eerste is ϕ een ringhomomorfisme. De productring $\mathbb{C}^{\hat{G}}$ heeft namelijk coördinaatsgewijze optelling en vermenigvuldiging en op elke coördinaat is $\chi' : \mathbb{C}[G] \to \mathbb{C}$ een ringhomomorfisme.

Voor $\chi \in \hat{G}$ is het ringhomomorfisme $\chi' : \mathbb{C}[G] \to \mathbb{C}$ surjectief en dus geldt $\mathbb{C} \cong \mathbb{C}[G]/\ker \chi'$. De idealen $\ker \chi'$ zijn onderling ondeelbaar, dat wil zeggen dat voor $\chi_1, \chi_2 \in \hat{G}$ met $\chi_1 \neq \chi_2$ geldt $\ker(\chi_1') + \ker(\chi_2') = \mathbb{C}[G]$. Kies namelijk $\sigma \in G$ zodanig dat $\chi_1(\sigma) \neq \chi_2(\sigma)$. Dan hebben we dat $\sigma - \chi_1(\sigma) \in \ker(\chi_1')$ en $\sigma - \chi_2(\sigma) \in \ker(\chi_2')$. De eenheid $\chi_1(\sigma) - \chi_2(\sigma)$ is dus een element van $\ker(\chi_1') + \ker(\chi_2')$ en dat geeft $\ker(\chi_1') + \ker(\chi_2') = \mathbb{C}[G]$.

Toepassen van de Chinese Reststelling op de ring $\mathbb{C}[G]$ en idealen $\ker \chi'$ geeft een surjectieve afbeelding $\mathbb{C}[G] \to \prod_{\chi \in \hat{G}} \mathbb{C}[G]/\ker \chi'$. Analyseren van deze afbeelding en het bovenstaande isomorfisme $\mathbb{C} \cong \mathbb{C}[G]/\ker \chi'$, bewijst dan dat ϕ surjectief is.

Als laatste concluderen we dat ϕ bijectief is door de dimensies van de $\mathbb{C}$-vectorruimtes $\mathbb{C}[G]$ en $\mathbb{C}^{\hat{G}}$ te vergelijken. De dimensie van $\mathbb{C}[G]$ is gelijk aan $\#G$ en de dimensie van $\mathbb{C}^{\hat{G}}$ is gelijk aan $\#\hat{G} = \#G$. Omdat ϕ een surjectieve $\mathbb{C}$-lineaire afbeelding is, volgt uit de gelijke dimensies dat ϕ bijectief is. Dus ϕ is een ringisomorfisme. □

Dit geeft als volgt een verband tussen de conjugatie op $\mathbb{C}$ en de standaardinvolutie op $\mathbb{Z}[G]$. Merk op dat ook voor $k = \mathbb{Z}$ en $R = \mathbb{C}$ het bovenstaande een identificatie geeft van $V = \{f : \mathbb{Z}[G] \to \mathbb{C} \mid f \text{ ringhomomorfisme}\}$ en $\hat{G}$.

Propositie 2.5. *Zij G een eindige abelse groep en V de verzameling van ringhomomorfismen $\mathbb{Z}[G] \to \mathbb{C}$. Dan geldt*

1. *voor alle $f \in V$ en voor alle $r \in \mathbb{Z}[G]$ dat $f(\bar{r}) = \overline{f(r)}$.*
2. *$\bigcap_{f \in V} \ker f = \{0\}$.*

Bewijs. 1. Zij $f \in V$. Voor $\sigma \in G$ geldt $f(\sigma) \in \langle \zeta \rangle$ en dus $f(\sigma)\overline{f(\sigma)} = 1$. Dus geldt $\overline{f(\sigma)} = f(\sigma)^{-1} = f(\sigma^{-1}) = f(\bar{\sigma})$. Voor $\sigma \in G$ geldt dus $\overline{f(\sigma)} = f(\bar{\sigma})$ en met lineaire voortzetting hebben we dat

$$\begin{array}{ccc} \mathbb{Z}[G] & \xrightarrow{\bar{}} & \mathbb{Z}[G] \\ \downarrow f & & \downarrow f \\ \mathbb{C} & \xrightarrow{\bar{}} & \mathbb{C} \end{array}$$

commuteert.

2. We hebben een inclusie $\mathbb{Z}[G] \to \mathbb{C}[G]$. Stel $x \in \mathbb{Z}[G]$ en $x \in \bigcap_{f \in V} \ker f$. Per aanname geldt voor alle $f \in V$ dat $f(x) = 0$ en door de identificatie van V en $\hat{G}$, geldt voor alle $\chi \in \hat{G}$ dat $\chi'(x) = 0$. Beschouw $x \in \mathbb{C}[G]$ en het isomorfisme $\phi : \mathbb{C}[G] \to \mathbb{C}^{\hat{G}}$ uit stelling 2.4. Dan geldt $\phi(x) = (\chi'(x))_{\chi \in \hat{G}} = 0$. Omdat ϕ een isomorfisme is, geldt dan $x = 0$. □

Lemma 2.6. *Zij V de verzameling van ringhomomorfismen $\mathbb{Z}[G] \to \mathbb{C}$. Voor $r, s \in \mathbb{Z}[G]$ geldt $r = s$ dan en slechts dan als $f(r) = f(s)$ voor alle $f \in V$.*

Bewijs. Uiteraard impliceert $r = s$ de gelijkheid $f(r) = f(s)$ voor alle $f \in V$. Als geldt $f(r) = f(s)$ voor alle $f \in V$ en dus $f(r - s) = 0$ voor alle $f \in V$, dan geldt $r - s \in \bigcap_{f \in V} \ker f$. Uit propositie 2.5 (2) volgt dan $r - s = 0$ en $r = s$. □

Deze lemma's kunnen we toepassen om de stelling te bewijzen.

Bewijs stelling 2.1. Stel $x \in \mathrm{Id}(\mathbb{Z}[G])$, dan geldt $x^2 = x$. Uit lemma 2.6 volgt dat $f(x^2) = f(x)$ voor alle $f \in V$. Dan geldt $f(x)^2 = f(x)$ oftewel $f(x) \in \mathrm{Id}(\mathbb{C})$ voor alle $f \in V$. Dan gebruiken we een eigenschap van idempotenten in $\mathbb{C}$ om te concluderen dat $f(x) = \overline{f(x)}$ voor alle $f \in V$. Met propositie 2.5 (1) volgt dan $f(x) = f(\bar{x})$ voor alle $f \in V$ en met lemma 2.6 krijgen we $x = \bar{x}$.

Voor een idempotent $x = \sum_{\sigma \in G} a_\sigma \sigma \in \mathrm{Id}(\mathbb{Z}[G])$ gelden dus de volgende gelijkheden:

$$\begin{gathered} x\bar{x} = x^2 = x, \\ \left(\sum_{\sigma \in G} a_\sigma \sigma\right)\left(\sum_{\sigma \in G} a_\sigma \sigma^{-1}\right) = \left(\sum_{\sigma \in G} a_\sigma \sigma\right), \\ \sum_{\sigma \in G} a_\sigma^2 = a_1, \\ \sum_{\sigma \in G, \sigma \neq 1} a_\sigma^2 = a_1 - a_1^2. \end{gathered}$$

Hier geldt $\sum_{\sigma\in G,\sigma\neq 1} a_\sigma^2 \geq 0$ en $a_1 - a_1^2 \leq 0$. Dan volgt dat beide gelijk zijn aan 0 en dus dat $a_\sigma = 0$ voor alle $\sigma \in G, \sigma \neq 1$ en $a_1 = 1$ óf $a_1 = 0$. Dus geldt $x = 0$ of $x = 1$ en $\mathrm{Id}(\mathbb{Z}[G]) \subset \{0, 1\}$. We hebben al de inclusie $\{0, 1\} = \mathrm{Id}(\mathbb{Z}) \subset \mathrm{Id}(\mathbb{Z}[G])$ dus dit bewijst dat $\mathrm{Id}(\mathbb{Z}[G]) = \{0, 1\}$. □

3 Projectieve modulen

3.1 Definitie

Om dit later in bewijzen van belangrijke stellingen te kunnen gebruiken, introduceren we de definitie en een aantal eigenschappen van projectieve modulen. In de hele tekst bedoelen we standaard met een R-moduul, zonder verdere specificaties van links of rechts, een links-R-moduul.

Zij M een R-moduul. Dan induceert een R-lineaire afbeelding $f : A \to B$ van R-modulen een homomorfisme

$$f_* : \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B), \phi \mapsto f \circ \phi,$$

van abelse groepen.

Propositie 3.1. *Zij R een ring en M een R-moduul. Laat*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C$$

een exacte rij zijn van R-modulen en R-lineaire afbeeldingen. Dan is

$$0 \to \mathrm{Hom}_R(M, A) \xrightarrow{f_*} \mathrm{Hom}_R(M, B) \xrightarrow{g_*} \mathrm{Hom}_R(M, C)$$

een exacte rij van abelse groepen.

Het bewijs hiervan is een korte opgave. Merk wel op dat in het algemeen gegeven een korte exacte rij

$$0 \to A \to B \to C \to 0$$

niet hoeft te gelden dat de rij

$$0 \to \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B) \to \mathrm{Hom}_R(M, C) \to 0$$

exact is.

Voorbeeld 3.2. Laat $R = \mathbb{Z}$ zijn. Dan is een R-moduul een abelse groep. Stel $M = \mathbb{Z}/2\mathbb{Z}$ en beschouw de exacte rij

$$0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \to 0,$$

waarbij f vermenigvuldiging is met 2 en g de quotiëntafbeelding. In de rij

$$0 \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{f_*} \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{g_*} \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

is de afbeelding g_* niet surjectief. Er geldt namelijk dat $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \cong 0$, maar ook geldt $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

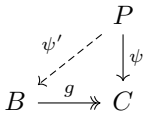
Met andere woorden, de functor $\mathrm{Hom}_R(M,-)$ van R-modulen naar abelse groepen is linksexact, maar in de regel niet voor alle R-modulen M rechtsexact. Dit leidt tot de volgende definitie.

Definitie 3.3. Een R-moduul P heet *projectief*, als $\mathrm{Hom}_R(P,-)$ een exacte functor is van R-modulen naar abelse groepen.

Er wordt dus geëist dat $\mathrm{Hom}_R(P,-)$ voor een projectief R-moduul P ook rechtsexact is, oftewel voor een surjectieve afbeelding $B \xrightarrow{g} C$ eisen we dat

$$\mathrm{Hom}_R(P,B) \xrightarrow{g_*} \mathrm{Hom}_R(P,C)$$

surjectief is. Dit betekent dat voor elke $\psi \in \mathrm{Hom}_R(P,C)$, er een $\psi' \in \mathrm{Hom}_R(P,B)$ moet bestaan zodat $g \circ \psi' = \psi$ oftewel zodat het onderstaande diagram commuteert.



Een directe som van twee projectieve modulen is weer projectief. Algemener hebben we de volgende propositie.

Propositie 3.4. *Zij $\{P_\alpha\}_{\alpha\in A}$ een familie R-modulen voor een zekere indexverzameling A. Dan is de directe som $P = \bigoplus_{\alpha\in A} P_\alpha$ projectief dan en slechts dan als P_α projectief is voor alle $\alpha \in A$.*

Bewijs. Er is een natuurlijke equivalentie van functoren

$$\mathrm{Hom}_R(\bigoplus_\alpha P_\alpha, -) \cong \prod_\alpha \mathrm{Hom}_R(P_\alpha,-),$$

van R-modulen naar abelse groepen. Beschouw namelijk de natuurlijke transformatie gegeven door het volgende groepshomomorfisme voor een R-moduul M:

$$\tau_M : \mathrm{Hom}_R(\bigoplus_\alpha P_\alpha, M) \to \prod_\alpha \mathrm{Hom}_R(P_\alpha,M), \phi \mapsto \prod_\alpha \phi_{|P_\alpha}.$$

De inverse van τ_M volgt uit de universele eigenschap van de directe som.

Dan zien we dat de functor $\mathrm{Hom}_R(\bigoplus_\alpha P_\alpha,-)$ exact is dan en slechts dan als $\prod_\alpha \mathrm{Hom}_R(P_\alpha,-)$ exact is. Hieruit volgt dat $\mathrm{Hom}_R(\bigoplus_\alpha P_\alpha,-)$ exact is dan en slechts dan als $\mathrm{Hom}_R(P_\alpha,-)$ exact is voor alle $\alpha \in A$. □

Propositie 3.5. *Een vrij R-moduul $\bigoplus_{i\in I} R$ is projectief.*

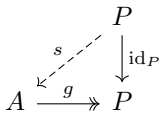
Bewijs. Laat B, C twee R-modulen zijn. Omdat geldt $\mathrm{Hom}_R(R,B) \cong B$ en $\mathrm{Hom}_R(R,C) \cong C$ als R-modulen, induceert een surjectieve R-lineaire afbeelding $g : B \to C$ ook een surjectieve afbeelding $g_* : \mathrm{Hom}_R(R,B) \to \mathrm{Hom}_R(R,C)$. Dan is de ring R zelf een projectief R-moduul. Daarmee geeft propositie 3.4 dat een vrij R-moduul $\bigoplus_{i\in I} R$ projectief is. □

Met propositie 3.4 kunnen we ook de volgende classificatie voor projectieve R-modulen afleiden.

Propositie 3.6. *Zij P een R-moduul. Dan zijn de volgende uitspraken equivalent:*

1. *P is projectief;*
2. *elke surjectieve R-lineaire afbeelding $g : A \to P$ heeft een rechtsinverse;*
3. *er bestaat een R-moduul Q zo dat $P \oplus Q$ vrij is.*

Bewijs. Eigenschap 2 wil zeggen dat er een R-lineaire afbeelding $s : P \to A$ bestaat met $g \circ s = \mathrm{id}_P$. Voor de implicatie $1 \Rightarrow 2$, laat een surjectieve R-lineaire afbeelding $g : A \to P$ gegeven zijn. Beschouw $\mathrm{id}_P \in \mathrm{Hom}_R(P, P)$. Dan hebben we het onderstaande diagram.



Omdat P projectief is, volgt nu dat er een $s \in \mathrm{Hom}_R(P, A)$ bestaat zo dat $g \circ s = \mathrm{id}_P$.

Voor de implicatie $2 \Rightarrow 3$, beschouw de volgende afbeelding

$$g : F = \bigoplus_{p \in P} R \to P, e_p \mapsto p,$$

waar e_p de p-de basisvector is. Dit is een surjectieve R-lineaire afbeelding en deze heeft dus een rechtsinverse, een R-lineaire afbeelding $s : P \to F$ met $g \circ s = \mathrm{id}_P$. Dan splitst de exacte rij

$$0 \to \ker(g) \to F \xrightarrow{g} P \to 0.$$

Dan is $Q = \ker(g)$ dus een R-moduul waarvoor geldt dat $P \oplus Q$ vrij is.

Voor $3 \Rightarrow 1$, stel dat Q een R-moduul is zo dat $P \oplus Q$ vrij is. Omdat een vrij moduul projectief is, geldt dat $P \oplus Q$ projectief is. Dan volgt met propositie 3.4, dat P en Q projectief zijn. □

Voorbeelden van niet-vrije projectieve modulen zijn de volgende.

Voorbeeld 3.7. Stel $R = R_1 \times R_2$, het product van twee ringen beide ongelijk aan de nulring. Dan is $R_1 \times 0$ een projectief R-moduul. Er geldt namelijk $(R_1 \times 0) \oplus (0 \times R_2) = R$, dus hebben we via (3) van propositie 3.6 dat $R_1 \times 0$ projectief is. Daarentegen is $R_1 \times 0$ niet vrij over R. Voor $r \in 0 \times R_2 \subset R$, geldt namelijk dat $r(R_1 \times 0) = 0$.

Voorbeeld 3.8. Een ander voorbeeld sluit aan bij ringentheorie. Bekend is dat $R = \mathbb{Z}[\sqrt{-5}]$ is geen hoofdideaaldomein is. De afbeelding

$$\mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_2, a + b\sqrt{-5} \mapsto (a + b) \bmod 2$$

is namelijk een surjectief homomorfisme waarvan de kern $\mathfrak{p} = (2, \sqrt{-5} - 1)$ geen hoofdideaal is. Dus is $\mathfrak{p}$ niet vrij over R van rang 1. Maar dan is $\mathfrak{p}$ ook niet vrij. Stel namelijk dat $\mathfrak{p} \cong R^{(I)}$. Laat $K = \mathbb{Q}(\sqrt{-5})$ zijn. Dan is K een R-moduul en K is de localisatie van R bij de multiplicatief gesloten verzameling $S = R \setminus \{0\}$. Voor $K = S^{-1}R$ en een R-moduul M hebben we een isomorfisme $K \otimes_R M \cong S^{-1}M$ van R-modulen. Dit en het feit dat localisatie exact is, geeft dat voor de exacte rij

$$0 \to \mathfrak{p} \to R \to \mathbb{F}_2 \to 0,$$

geldt dat de rij

$$0 \to \mathfrak{p} \otimes_R K \to K \to \mathbb{F}_2 \otimes_R K \to 0$$

ook exact is. Hier geldt dat $\mathbb{F}_2 \otimes_R K \cong 0$, omdat het tensorproduct van een torsiegroep met een deelbare groep 0 is. Met de exactheid van de rij, krijgen we dan dat $\mathfrak{p} \otimes_R K \cong K$, maar we hebben ook de K-vectorruimte isomorfismes

$$\mathfrak{p} \otimes_R K \cong R^{(I)} \otimes_R K \cong (R \otimes_R K)^{(I)} \cong K^{(I)}.$$

Dan zou I een verzameling van 1 element moeten zijn en $\mathfrak{p}$ vrij zijn van rang 1. Dan zou het ideaal echter een hoofdideaal zijn en dat geeft een tegenspraak.

Dus $\mathfrak{p} = (2, \sqrt{-5} - 1)$ is niet vrij over R. Wel is $\mathfrak{p}$ een projectief moduul, beschouw namelijk de afbeelding $2R \oplus (\sqrt{-5} - 1)R \xrightarrow{+} \mathfrak{p}, (x, y) \mapsto x + y$. Dit geeft een exacte rij

$$0 \to \ker(+) \to 2R \oplus (\sqrt{-5} - 1)R \xrightarrow{+} \mathfrak{p} \to 0,$$

die splitst via de sectie

$$s : \mathfrak{p} \to 2R \oplus (\sqrt{-5} - 1)R, x \mapsto (-2x, 3x).$$

Deze afbeelding is welgedefinieerd, want er geldt duidelijk $-2x \in 2R$, maar ook $3x \in (\sqrt{-5} - 1)R$. Er geldt namelijk $\mathfrak{p}^2 = 2R$ en dus $(\sqrt{-5} + 1)x \in 2R$ en $\frac{3x(\sqrt{-5}+1)}{6} \in R$. Dan volgt $\frac{3x}{\sqrt{-5}-1} \in R$ en dus is s welgedefinieerd en een sectie omdat $+ \circ s = \mathrm{id}_{\mathfrak{p}}$. Dan geldt $\mathfrak{p} \oplus \ker(+) \cong 2R \oplus (\sqrt{-5} - 1)R$, een vrij R-moduul. Dus $\mathfrak{p}$ is een niet-vrij projectief R-moduul.

3.2 Verandering van ring

Gegeven een ringhomomorfisme $\lambda : R \to S$ is er een natuurlijke manier om van een projectief R-moduul een projectief S-moduul te construeren. Dit is handig om bewijzen te herleiden tot simpele gevallen.

Laat R en S twee ringen zijn en $\lambda : R \to S$ een ringhomomorfisme. Stel M is een S-moduul, dan is M een R-moduul door de vermenigvuldiging rm voor $r \in R$ en $m \in M$ te definiëren als

$$rm := \lambda(r)m.$$

Dus er bestaat een natuurlijke functor van de categorie ${}_S\mathbf{Mod}$ van S-modulen naar de categorie ${}_R\mathbf{Mod}$ van R-modulen.

Andersom, bestaat er gegeven een ringhomomorfisme $\lambda : R \to S$ ook een natuurlijke functor van ${}_R\mathbf{Mod}$ naar ${}_S\mathbf{Mod}$. Stel M is een (links-)R-moduul. Dan is M een $R, \mathbb{Z}$-bimoduul en S is een S, R-bimoduul via λ. Dan is $M_S = S \otimes_R M$ een $S, \mathbb{Z}$-bimoduul, oftewel een (links-)S-moduul. Dus er bestaat een functor:

$$\begin{aligned} F : {}_R\mathbf{Mod} &\to {}_S\mathbf{Mod} \\ M &\mapsto S \otimes_R M = M_S \\ (\phi : M \to N) &\mapsto (\mathrm{id}_S \otimes \phi : M_S \to N_S)\,. \end{aligned}$$

Voor rechtsmodulen bestaat er analoog een functor van $\mathbf{Mod}_S$ naar $\mathbf{Mod}_R$ en andersom van $\mathbf{Mod}_R$ naar $\mathbf{Mod}_S$ met behulp van het juiste tensorproduct.

Lemma 3.9. *Zij $\lambda : R \to S$ een ringhomomorfisme en F een vrij R-moduul met basis B. Dan is de afbeelding*

$$\begin{aligned} F_S = S \otimes_R F &\to S^{(B)} \\ s \otimes \left(\sum_{b \in B} r_b b \right) &\mapsto (r_b s)_{b \in B} \end{aligned}$$

een S-lineair isomorfisme.

Bewijs. Omdat F een vrij R-moduul is met basis B, is $F_S = S \otimes_R F$ een vrij S-moduul met basis $\{1 \otimes b \mid b \in B\}$. De afbeelding is duidelijk S-lineair en op de bases kunnen we nagaan dat de inverse is gegeven door

$$\begin{aligned} S^{(B)} &\to S \otimes_R F \\ (s_b)_{b \in B} &\mapsto \sum_{b \in B} (s_b \otimes b). \end{aligned}$$

□

Lemma 3.10. *Zij $\lambda : R \to S$ een ringhomomorfisme en P een eindig voortgebracht projectief R-moduul. Dan is $P_S = S \otimes_R P$ een eindig voortgebracht projectief S-moduul.*

Bewijs. Ten eerste is P_S een eindig voortgebracht S-moduul. Een surjectieve afbeelding $R^n \to P$ voor zekere $n \in \mathbb{Z}_{\geq 0}$ induceert namelijk een surjectieve afbeelding $S^n \to P_S$ omdat de functor $S \otimes_R -$ rechtsexact is. Omdat P projectief is en eindig voortgebracht, bestaat er een projectief moduul Q en een vrij eindig voortgebracht R-moduul F zodat $F = P \oplus Q$. Dan geldt

$$F_S = S \otimes_R F = (S \otimes_R P) \oplus (S \otimes_R Q).$$

Met lemma 3.9 is F_S een vrij S-moduul en dus is de directe som $P_S \oplus Q_S$ vrij. Dan is P_S een projectief S-moduul. □

3.3 Vrijheid van projectieve modulen over lokale ringen

Definitie 3.11. De ring R is een *lokale* ring, als R een uniek maximaal linksideaal heeft.

Stelling 3.12. *Zij R een lokale ring. Dan is ieder eindig voortgebracht projectief R-moduul vrij.*

Voor lokale ringen zijn dus geen voorbeelden te geven van niet vrije projectieve modulen, zoals in voorgaande paragrafen is gedaan. Kaplansky [6] heeft bewezen dat elk projectief moduul over een lokale ring vrij is, maar deze sterkere variant is in dit artikel echter geen benodigdheid. Wij geven een bewijs voor eindig voortgebrachte modulen gebaseerd op het bewijs in T. Y. Lam [3].

Ten eerste herhalen we hieronder Nakayama's Lemma, zie S. Lang [2] hoofdstuk X, lemma 4.1. Het Jacobson radicaal $\mathcal{J}$ van een ring R is de doorsnede van alle maximale linksidealen.

Lemma 3.13 (Nakayama's Lemma)**.** *Zij R een ring en $\mathcal{J}$ het Jacobson radicaal van R. Zij M een eindig voortgebracht R-moduul waarvoor geldt $M = \mathcal{J}M$. Dan geldt $M = 0$.*

Voor een eindig voortgebracht projectief R-moduul, heeft dit lemma het volgende gevolg.

Propositie 3.14. *Zij Q een eindig voortgebracht R-moduul en P een eindig voortgebracht projectief R-moduul. Zij $\gamma \in \mathrm{Hom}_R(Q, P)$ en laat $\mathcal{J}$ het Jacobsonradicaal van R zijn. Beschouw de geïnduceerde afbeelding*

$$\bar{\gamma} = \mathrm{id}_{R/\mathcal{J}} \otimes \gamma : R/\mathcal{J} \otimes_R Q \to R/\mathcal{J} \otimes_R P.$$

Stel $\bar{\gamma}$ is een isomorfisme. Dan is γ een isomorfisme.

Bewijs. De functor $R/\mathcal{J} \otimes_R -$ is een rechtsexacte functor. Als quotiënt van P is $\operatorname{coker}\gamma$ ook een eindig voortgebracht R-moduul. De functor toepassen op de exacte rij

$$Q \xrightarrow{\gamma} P \to \operatorname{coker}\gamma \to 0,$$

geeft de volgende exacte rij

$$(R/\mathcal{J}) \otimes_R Q \xrightarrow{\bar{\gamma}} (R/\mathcal{J}) \otimes_R P \to (R/\mathcal{J}) \otimes_R \operatorname{coker}\gamma \to 0.$$

De exactheid geeft dan $(R/\mathcal{J}) \otimes_R \operatorname{coker}\gamma \cong \operatorname{coker}\bar{\gamma}$ en omdat $\bar{\gamma}$ een isomorfisme is, geldt $\operatorname{coker}\bar{\gamma} = 0$. Dan geldt dat $0 = (R/\mathcal{J}) \otimes_R \operatorname{coker}\gamma \cong \operatorname{coker}\gamma/\mathcal{J}\operatorname{coker}\gamma$. Dus geldt $\operatorname{coker}\gamma = \mathcal{J}\operatorname{coker}\gamma$ en Nakayama's Lemma impliceert dan dat geldt $\operatorname{coker}\gamma = 0$. Daarmee is γ surjectief.
Beschouw de exacte rij

$$0 \to \ker\gamma \to Q \xrightarrow{\gamma} P \to 0.$$

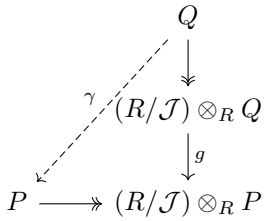
Omdat P een projectief R-moduul is, heeft γ een rechtsinverse en splitst de rij. Daarom is $\ker(\gamma)$ eindig voortgebracht en is de rij

$$0 \to (R/\mathcal{J}) \otimes_R \ker\gamma \to (R/\mathcal{J}) \otimes_R Q \xrightarrow{\bar{\gamma}} (R/\mathcal{J}) \otimes_R P \to 0$$

ook exact. Vervolgens geeft de exactheid van de rij en het feit dat $\bar{\gamma}$ een isomorfisme is, dat $(R/\mathcal{J}) \otimes_R \ker\gamma \cong \ker\bar{\gamma} = 0$. Zo hebben we dus dat $0 = (R/\mathcal{J}) \otimes_R \ker\gamma \cong \ker\gamma/\mathcal{J}\ker\gamma$. Dan impliceert Nakayama's Lemma dat geldt $\ker\gamma = 0$. Dus γ is een isomorfisme. □

Propositie 3.15. *Laat P en Q eindig voortgebrachte projectieve R-modulen zijn. Stel er geldt $(R/\mathcal{J}) \otimes_R Q \cong (R/\mathcal{J}) \otimes_R P$ als $R/\mathcal{J}$-modulen. Dan geldt $Q \cong P$ als R-modulen.*

Bewijs. Stel P en Q zijn beide eindig voortgebrachte projectieve R-modulen en stel dat $g : (R/\mathcal{J}) \otimes_R Q \to (R/\mathcal{J}) \otimes_R P$ een $R/\mathcal{J}$-lineair isomorfisme is. Er zijn natuurlijke surjecties $Q \to (R/\mathcal{J}) \otimes_R Q \cong Q/\mathcal{J}Q$ en $P \to (R/\mathcal{J}) \otimes_R P \cong P/\mathcal{J}P$. Omdat Q een projectief R-moduul is, bestaat er een afbeelding $\gamma \in \mathrm{Hom}_R(Q, P)$ zodanig dat het diagram



commuteert. De commutativiteit geeft dan dat $\bar{\gamma} = g$. Bovendien is $g = \bar{\gamma}$ een isomorfisme, dus geldt wegens propositie 3.14 dat γ een R-lineair isomorfisme is en $Q \cong P$ als R-modulen. □

Bewijs stelling 3.12. Voor een lokale ring R geldt dat het Jacobson radicaal $\mathcal{J}$ gelijk is aan het unieke maximale linksideaal, zie S. Lang [2] hoofdstuk XVII stelling 6.1. Dan is $R/\mathcal{J}$ een delingsring en daarmee is elk $R/\mathcal{J}$-moduul vrij: uit de lineaire algebra is namelijk bekend dat een vectorruimte over een delingsring een basis heeft. Dus voor een eindig voortgebracht projectief R-moduul P geldt dat $(R/\mathcal{J}) \otimes_R P$ isomorf is als $R/\mathcal{J}$-moduul met een vrij $R/\mathcal{J}$-moduul. Dan geeft propositie 3.15 dat P isomorf is met een vrij R-moduul. □

4 De rang van een projectief moduul

In deze paragraaf nemen we R een commutatieve ring. Noteer het spectrum van R, oftewel de verzameling priemidealen van R, met $\mathrm{Spec}\, R$. Voor een priemideaal $\mathfrak{p} \subset R$ bedoelen we met $R_\mathfrak{p}$ de localisatie van de ring R bij de multiplicatief gesloten verzameling $S = R \setminus \mathfrak{p}$ (dus $S^{-1}R = R_\mathfrak{p}$). Evenzo is $M_\mathfrak{p}$ voor een R-moduul M de localisatie bij $S = R \setminus \mathfrak{p}$. De ring $R_\mathfrak{p}$ is een lokale ring, waar $\mathfrak{p}_\mathfrak{p} = \{a/s : a \in \mathfrak{p}, s \in S = R \setminus \mathfrak{p}\}$ het unieke maximale ideaal is.

Definitie 4.1. Zij R een commutatieve ring en M een eindig voortgebracht R-moduul. De *rang van M bij een priemideaal* $\mathfrak{p}$ is

$$\mathrm{rang}_{M/R}(\mathfrak{p}) := \dim_{k(\mathfrak{p})}(k(\mathfrak{p}) \otimes_R M),$$

waar $k(\mathfrak{p}) = Q(R/\mathfrak{p})$ het quotiëntenlichaam van $R/\mathfrak{p}$ is.

De rang van een moduul is een functie

$$\mathrm{rang}_{M/R} : \mathrm{Spec}\, R \to \mathbb{Z}, \mathfrak{p} \mapsto \mathrm{rang}_{M/R}(\mathfrak{p}).$$

Merk op dat voor R-modulen M, N en voor lokalisatie bij S geldt

$$S^{-1}(M/N) \cong S^{-1}M/S^{-1}N,$$

dus geldt de gelijkheid $k(\mathfrak{p}) = Q(R/\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$.

Lemma 4.2. *Zij R een commutatieve ring en $\mathfrak{p} \subset R$ een priemideaal. Laat M en N eindig voortgebrachte R-modulen zijn. Dan geldt*

$$\mathrm{rang}_{M\oplus N/R}(\mathfrak{p}) = \mathrm{rang}_{M/R}(\mathfrak{p}) + \mathrm{rang}_{N/R}(\mathfrak{p}).$$

Bewijs. Er geldt

$$k(\mathfrak{p}) \otimes_R (M \oplus N) \cong (k(\mathfrak{p}) \otimes_R M) \oplus (k(\mathfrak{p}) \otimes_R N).$$

□

Lemma 4.3. *Zij R een ring en $M = \bigoplus_{i\in I} R$ een eindig voortgebracht vrij R-moduul. Dan geldt voor alle priemidealen $\mathfrak{p} \subset R$ dat*

$$\mathrm{rang}_{M/R}(\mathfrak{p}) = \#I.$$

Bewijs. Voor het R-moduul R geldt $\dim_{k(\mathfrak{p})}(k(\mathfrak{p}) \otimes_R R) = \dim_{k(\mathfrak{p})} k(\mathfrak{p}) = 1$. Wegens lemma 4.2 is de rang van M dan gelijk aan $\#I$ voor alle priemidealen $\mathfrak{p} \subset R$. □

Voorbeeld 4.4. Zij R een commutatieve ring, $\mathfrak{p} \subset R$ een priemideaal en G een eindige groep. Dan is $R[G]$ een vrij R-moduul en er geldt $R[G] = \bigoplus_{\sigma\in G} R\sigma$. Dan geldt dus met lemma 4.3 dat

$$\mathrm{rang}_{R[G]/R}(\mathfrak{p}) = \#G.$$

Lemma 4.5. *Zij R een commutatieve ring en M een eindig voortgebracht R-moduul zodanig dat voor elk priemideaal $\mathfrak{p} \subset R$ geldt $\mathrm{rang}_{M/R}(\mathfrak{p}) = 0$. Dan geldt $M = 0$.*

Bewijs. Voor een R-moduul M geldt dat $M = 0$ dan en slechts dan als voor alle priemidealen $\mathfrak{p}$ van R geldt $M_\mathfrak{p} = 0$. Voor ieder priemideaal $\mathfrak{p} \subset R$ geldt $\mathrm{rang}_{M/R}(\mathfrak{p}) = 0$ oftewel

$$\dim_{k(\mathfrak{p})}(k(\mathfrak{p}) \otimes_R M) = 0.$$

Om die reden geldt $k(\mathfrak{p}) \otimes_R M = 0$, waar $k(\mathfrak{p}) = Q(R/\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$. Voor ieder priemideaal $\mathfrak{p} \subset R$ geldt dat

$$0 = (k(\mathfrak{p}) \otimes_R M)_\mathfrak{p} \cong (k(\mathfrak{p}))_\mathfrak{p} \otimes_{R_\mathfrak{p}} M_\mathfrak{p} = ((R/\mathfrak{p})_\mathfrak{p})_\mathfrak{p} \otimes_{R_\mathfrak{p}} M_\mathfrak{p} \cong (R/\mathfrak{p})_\mathfrak{p} \otimes_{R_\mathfrak{p}} M_\mathfrak{p}.$$

Hiermee hebben we dus dat $0 = (R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}) \otimes_{R_\mathfrak{p}} M_\mathfrak{p} \cong M_\mathfrak{p}/(\mathfrak{p}_\mathfrak{p} M_\mathfrak{p})$. Dan voldoet $M_\mathfrak{p}$ aan de voorwaarde van Nakayama's Lemma, namelijk $M_\mathfrak{p} = \mathfrak{p}_\mathfrak{p} M_\mathfrak{p}$, en dus geldt $M_\mathfrak{p} = 0$ voor ieder priemideaal $\mathfrak{p} \subset R$. Dus geldt $M = 0$. □

Voor projectieve modulen hadden we voor de rang de volgende alternatieve equivalente definitie kunnen geven, zoals deze wordt gegeven door T. Y. Lam in [3]. Voor P een eindig voortgebracht projectief R-moduul geldt namelijk wegens lemma 3.10 dat $P_\mathfrak{p} \cong R_\mathfrak{p} \otimes_R P$ eindig voortgebracht en projectief $R_\mathfrak{p}$-moduul is. Omdat $R_\mathfrak{p}$ een lokale ring is, volgt dan uit stelling 3.12 dat $P_\mathfrak{p}$ een vrij eindig voortgebracht moduul is.

Definitie 4.6. Zij R een commutatieve ring en P een eindig voortgebracht projectief R-moduul. De *rang van P bij een priemideaal $\mathfrak{p}$* is

$$\operatorname{rang}_{P/R}(\mathfrak{p}) := \operatorname{rang}_{R_\mathfrak{p}} P_\mathfrak{p},$$

de rang van $P_\mathfrak{p}$ als vrij eindig voortgebracht $R_\mathfrak{p}$-moduul.

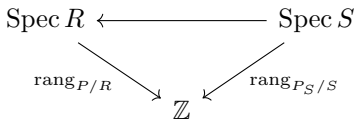
Dat deze definitie equivalent is met de vorige, kunnen we als volgt inzien. Zij P een eindig voortgebracht projectief R-moduul en stel $P_\mathfrak{p} \cong (R_\mathfrak{p})^n$ voor een zekere $n \in \mathbb{Z}_{\geq 0}$. Ook geldt $\operatorname{rang}_{P/R}(\mathfrak{p}) = \dim_{k(\mathfrak{p})}(k(\mathfrak{p}) \otimes_R P) = n$ omdat we met behulp van lemma 3.9 de volgende $k(\mathfrak{p})$-lineaire isomorfismes hebben:

$$k(\mathfrak{p}) \otimes_R P \cong (k(\mathfrak{p}) \otimes_{R_\mathfrak{p}} R_\mathfrak{p}) \otimes_R P \cong k(\mathfrak{p}) \otimes_{R_\mathfrak{p}} P_\mathfrak{p} \cong k(\mathfrak{p}) \otimes_{R_\mathfrak{p}} (R_\mathfrak{p})^n \cong (k(\mathfrak{p}))^n.$$

Deze definitie helpt met het bewijzen van het volgende lemma. Zij $\lambda : R \to S$ een ringhomomorfisme van commutatieve ringen, dan induceert λ een afbeelding

$$\operatorname{Spec} S \to \operatorname{Spec} R, \ \mathfrak{p} \mapsto \lambda^{-1}(\mathfrak{p}).$$

Lemma 4.7. *Laat R en S commutatieve ringen zijn en $\lambda : R \to S$ een ringhomomorfisme. Zij P een eindig voortgebracht projectief R-moduul. Dan is het moduul $P_S = S \otimes_R P$ een eindig voortgebracht projectief S-moduul en het volgende diagram commuteert.*



Bewijs. Het moduul $P_S = S \otimes_R P$ is een eindig voortgebracht projectief S-moduul wegens lemma 3.10. We gebruiken de volgende universele eigenschap van lokalisatie. Laat $T \subset R$ een multiplicatief gesloten verzameling zijn en $f : R \to T^{-1}R, r \mapsto \frac{r}{1}$. Voor een ringhomomorfisme $g : R \to S$ met $g(T) \subset S^*$, bestaat er dan een uniek ringhomomorfisme $h : T^{-1}R \to S$ zo dat $g = h \circ f$.

Laat $\mathfrak{q} \subset S$ een priemideaal zijn en $\mathfrak{p} = \lambda^{-1}(\mathfrak{q})$. Laat $f_\mathfrak{p}$ het ringhomomorfisme $f_\mathfrak{p} : R \to R_\mathfrak{p}, r \mapsto \frac{r}{1}$ zijn en $f_\mathfrak{q}$ het ringhomomorfisme $f_\mathfrak{q} : S \to S_\mathfrak{q}, s \mapsto \frac{s}{1}$. Voor $f_\mathfrak{q} \circ \lambda : R \to S_q$ geldt, omdat $\lambda(R \setminus \mathfrak{p}) \subset S \setminus \mathfrak{q}$, dat

$$f_\mathfrak{q} \circ \lambda(T) = f_\mathfrak{q} \circ \lambda(R \setminus \mathfrak{p}) \subset f_q(S \setminus \mathfrak{q}) \subset S_\mathfrak{q}^*.$$

Dan geeft de universele eigenschap van lokalisatie een afbeelding $\mu : R_\mathfrak{p} \to S_\mathfrak{q}$, zo dat

$$\begin{array}{ccc} R & \xrightarrow{\lambda} & S \\ \downarrow{\scriptstyle f_{\mathfrak{p}}} & & \downarrow{\scriptstyle f_{\mathfrak{q}}} \\ R_{\mathfrak{p}} & \xrightarrow{\mu} & S_{\mathfrak{q}} \end{array}$$

commuteert.

Nu willen we bewijzen dat $\operatorname{rang}_{P/R}(\mathfrak{p}) = \operatorname{rang}_{P_S/S}(\mathfrak{q})$, oftewel dat

$$\operatorname{rang}_{R_{\mathfrak{p}}} P_{\mathfrak{p}} = \operatorname{rang}_{S_{\mathfrak{q}}} (P_S)_{\mathfrak{q}}.$$

Beschouw eerst $(P_S)_{\mathfrak{q}}$. Dit moduul is isomorf met $P_S \otimes_S S_{\mathfrak{q}}$ en er geldt

$$(P_S)_{\mathfrak{q}} \cong P_S \otimes_S S_{\mathfrak{q}} = (P \otimes_R S) \otimes_S S_{\mathfrak{q}} \cong P \otimes_R (S \otimes_S S_{\mathfrak{q}}) \cong P \otimes_R S_{\mathfrak{q}}.$$

Deze isomorfismes zijn $S_{\mathfrak{q}}$-lineair. Merk op dat hierbij $S_{\mathfrak{q}}$ een R-moduul structuur heeft verkregen via de R-moduul structuur van S. Uit het bovenstaande diagram en de afbeelding μ, wordt $S_{\mathfrak{q}}$ een $R_{\mathfrak{p}}$-moduul. Dan is $S_{\mathfrak{q}}$ hier een R-moduul via de $R_{\mathfrak{p}}$-moduul structuur, maar omdat het bovenstaande diagram commuteert, komt deze R-moduul structuur van $S_{\mathfrak{q}}$ overeen met die hierboven. Het tensorproduct van $P_{\mathfrak{p}} \cong P \otimes_R R_{\mathfrak{p}}$ met $S_{\mathfrak{q}}$ over R_p is een $S_{\mathfrak{q}}$-moduul en we hebben de volgende S_q-lineaire isomorfismes:

$$P_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{q}} \cong (P \otimes_R R_{\mathfrak{p}}) \otimes_{R_{\mathfrak{p}}} S_q \cong P \otimes_R (R_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} S_q) \cong P \otimes_R S_q.$$

Stel $\operatorname{rang}_{R_{\mathfrak{p}}} P_{\mathfrak{p}} = n$, oftewel $P_{\mathfrak{p}} \cong (R_{\mathfrak{p}})^n$, dan geldt

$$(P_S)_{\mathfrak{q}} \cong P_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{q}} \cong (R_{\mathfrak{p}})^n \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{q}} \cong (R_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{q}})^n \cong (S_{\mathfrak{q}})^n$$

en dus geldt $\operatorname{rang}_{S_{\mathfrak{q}}} (P_S)_{\mathfrak{q}} = n$. Dus de rangen zijn gelijk. □

De rang is een functie van het spectrum naar $\mathbb{Z}$. Het spectrum $\operatorname{Spec} R$ is een topologische ruimte met de Zariski-topologie, waar de gesloten verzamelingen gegeven worden door

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supset I\}$$

voor een ideaal $I \subset R$. Een basis voor de open verzamelingen wordt gegeven door de verzamelingen

$$D(f) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \not\ni f\},$$

voor $f \in R$. Het spectrum $\operatorname{Spec} R$ met deze topologie is compact.

Propositie 4.8. *Zij P een eindig voortgebracht projectief R-moduul. Geef $\operatorname{Spec} R$ de Zariski-topologie en $\mathbb{Z}$ de discrete topologie. Dan is de afbeelding $\operatorname{rang}_{P/R} : \operatorname{Spec} R \to \mathbb{Z}$ continu.*

Nuttig voor het bewijs is het volgende lemma.

Lemma 4.9. *Zij R een commutatieve ring, S een multiplicatief gesloten verzameling van R en M een eindig voortgebracht R-moduul. Dan geldt $S^{-1}M = 0$ dan en slechts dan als er een $s \in S$ bestaat zo dat $sM = 0$.*

Bewijs. Neem aan dat geldt $sM = 0$ voor een zekere $s \in S$ en zij $\frac{m}{t} \in S^{-1}M$ willekeurig. Dan geldt $0 = sm = s(1m - t0)$, dus $\frac{m}{t} = \frac{0}{1}$. Dit geldt voor alle $\frac{m}{t} \in S^{-1}M$, dus geldt $S^{-1}M = 0$.

Laat $m_1, ..., m_n \in M$ voortbrengers zijn van M als R-moduul en stel $S^{-1}M = 0$. Dan geldt in het bijzonder voor alle i dat $\frac{m_i}{1} = \frac{0}{1}$ en dus bestaat er voor alle i een $s_i \in S$ zo dat $0 = s_i(1m_i - 1 \cdot 0) = s_i m_i$. Laat $s = s_1 \cdots s_n \in S$ het product van alle s_i zijn en $m = \sum_{i=1}^{n} r_i m_i \in M$ willekeurig. Dan geldt $sm = 0$, omdat R commutatief is en $s\sum_{i=1}^{n} r_i m_i = \sum_{i=1}^{n} r_i s m_i = 0$. Dus geldt voor deze $s \in S$ dat $sM = 0$. □

Bewijs propositie 4.8. Stel $\text{rang}_{P/R}(\mathfrak{p}) = n$ voor een zekere $n \in \mathbb{Z}$. Omdat $\{n\} \subset \mathbb{Z}$ open is, willen we dat $(\text{rang}_{P/R})^{-1}(n)$ open is in $\operatorname{Spec} R$.
Het $R_\mathfrak{p}$-moduul $P_\mathfrak{p} \cong R_\mathfrak{p} \otimes_R P$ is een vrij moduul. Laat $\frac{p_1}{s_1}, ..., \frac{p_n}{s_n}$ voortbrengers zijn van $P_\mathfrak{p}$ als $R_\mathfrak{p}$-moduul met $p_i \in P$ en $s_i \in R \setminus \mathfrak{p}$. Omdat de s_i eenheden zijn in de ring $R_\mathfrak{p}$, is ook $\frac{p_1}{1}, ..., \frac{p_n}{1}$ een basis voor $P_\mathfrak{p}$ als $R_\mathfrak{p}$-moduul. Beschouw de R-lineaire afbeelding

$$f : R^n \to P, e_i \mapsto p_i$$

waar e_i de standaard i-de basisvector is. Met deze definitie is de geïnduceerde afbeelding $f_\mathfrak{p} : (R_\mathfrak{p})^n \to P_\mathfrak{p}$ een isomorfisme. Daarom geldt $(\text{coker}(f))_\mathfrak{p} = 0$ en met lemma 4.9 bestaat er een $s \in R \setminus \mathfrak{p}$ zo dat $s(\text{coker}(f)) = 0$. Lokalisatie bij de multiplicatief gesloten verzameling $\{1, s, s^2, ...\}$ geeft bij de volgende exacte rij

$$0 \to \ker(f) \to R^n \to P \to \text{coker}(f) \to 0,$$

de exacte rij

$$0 \to (\ker(f))_s \to R_s^n \to P_s \to (\text{coker}(f))_s \to 0.$$

Lemma 4.9 geeft dan dat $(\text{coker}(f))_s = 0$, dus de afbeelding $f_s : R_s^n \to P_s$ is surjectief. Hetzelfde argument kunnen we toepassen op $\ker(f_s)$. Omdat P_s een projectief R_s-moduul is, splitst de afbeelding f_s en is $\ker(f_s)$ een eindig voortgebracht R_s-moduul. Er geldt $\{1, s, s^2, ...\} \subset R \setminus \mathfrak{p}$ en dus induceert f_s ook het isomorfisme $f_\mathfrak{p} : (R_\mathfrak{p})^n \to P_\mathfrak{p}$. Daarmee geldt $(\ker(f_s))_\mathfrak{p} = 0$. Wegens lemma 4.9 bestaat er dan een $t \in R \setminus \mathfrak{p}$ zo dat $t(\ker(f_s)) = 0$. Beschouw nu $u = st \in R \setminus \mathfrak{p}$. Localisatie bij $\{1, u, u^2, ...\}$ voor de exacte rij

$$0 \to (\ker(f))_s \to R_s^n \to P_s \to 0$$

levert dan

$$0 \to (\ker(f))_u \to R_u^n \to P_u \to 0.$$

Lemma 4.9 geeft $0 = (\ker f)_u$, dus $f_u : R_u^n \to P_u$ is een isomorfisme.

Dan geldt $R_\mathfrak{q}^n \cong P_\mathfrak{q}$ voor alle priemidealen $\mathfrak{q}$ zo dat $u \in R \setminus \mathfrak{q}$ oftewel zo dat $u \notin \mathfrak{q}$. Dan geldt $\text{rang}_{P/R}(\mathfrak{q}) = n$ voor alle $q \in D(u)$. Dus is $\text{rang}_{P/R}$ constant n op de open verzameling $D(u)$ en dus is $\text{rang}_{P/R}$ continu. □

Het spectrum R kan in verband worden gebracht met de idempotenten van R.

Lemma 4.10. *Zij $R \neq 0$ een commutatieve ring. Dan zijn equivalent*

1. $\operatorname{Spec} R$ *is niet samenhangend;*

2. *R heeft een idempotent ongelijk aan 0 en 1;*

3. *$R \cong R_1 \times R_2$ waar zowel R_1 als R_2 een commutatieve ring is ongelijk aan de nulring.*

Bewijs. Voor de implicatie $3 \Rightarrow 1$, neem aan dat $R \cong R_1 \times R_2$ waar zowel R_1 als R_2 een commutatieve ring is ongelijk aan de nulring. Beschouw de idealen $R_1 \times 0$ en $0 \times R_2$. Dan geldt

$$V(R_1 \times 0) \cup V(0 \times R_2) = V((R_1 \times 0) \cap (0 \times R_2)) = V(0) = \operatorname{Spec} R,$$

en

$$V(R_1 \times 0) \cap V(0 \times R_2) = V((R_1 \times 0) + (0 \times R_2)) = V(R) = \emptyset.$$

Dan is $\operatorname{Spec} R$ de vereniging van twee gesloten disjuncte niet-lege verzamelingen $V(R_1 \times 0)$ en $V(0 \times R_2)$ en is dus niet samenhangend.

Voor de implicatie $1 \Rightarrow 2$, neem aan dat $\operatorname{Spec} R$ niet samenhangend is. Dan is $\operatorname{Spec} R$ de disjuncte vereniging van twee niet-lege gesloten verzamelingen $V(\mathfrak{a})$ en $V(\mathfrak{b})$ voor $\mathfrak{a}, \mathfrak{b} \subset R$ idealen. Dan geldt

$$V(1) = \emptyset = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b}).$$

Het feit dat $V(\mathfrak{a} + \mathfrak{b}) = V(1)$ impliceert dat het radicaal $r(\mathfrak{a} + \mathfrak{b})$ gelijk is aan $r(1) = (1) = R$, dus geldt $\mathfrak{a} + \mathfrak{b} = (1)$. Kies $a \in \mathfrak{a}$ en $b \in \mathfrak{b}$ zo dat $a + b = 1$. Ook geldt

$$\operatorname{Spec} R = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cdot \mathfrak{b}) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{ab} \subset \mathfrak{p}\},$$

dus $\mathfrak{ab} \subset \mathfrak{p}$ voor alle $\mathfrak{p} \in \operatorname{Spec} R$ en $\mathfrak{ab} \subset \mathcal{N}$, waar $\mathcal{N}$ het nilradicaal is van R. Dan geldt $ab \in \mathcal{N}$ en dus bestaat er een $n \geq 1$ zodanig dat $(ab)^n = 0$. Beschouw $(a^n) + (b^n)$. Omdat $a \in r(a^n)$ en $b \in r(b^n)$, geldt $r(a^n) + r(b^n) = (1)$ en dus geldt $(a^n) + (b^n) = (1)$. Daarom bestaat er een $e \in (a^n)$ zo dat $e + (1 - e) = 1$ met $1 - e \in (b^n)$. Dan geldt $e - e^2 = e(1 - e) \in (a^n)(b^n) = (ab)^n = (0)$ en dus geldt $e = e^2$ en is e een idempotent. Stel $e = 1$, dan geldt $1 \in (a^n)$ en $1 \in \mathfrak{a}$, een tegenspraak. Stel $e = 0$, dan geldt $1 - e = 1$ en $1 \in (b^n)$ en $1 \in \mathfrak{b}$, een tegenspraak. Dus $e \in R$ is een idempotent ongelijk aan 0 en 1.

Voor de laatste implicatie, $2 \Rightarrow 3$, neem aan dat $e \in R$ een idempotent is ongelijk aan 0 of 1. Zoals eerder gezien, is $1 - e$ dan ook een idempotent ongelijk aan 0 of 1, dus $e, 1 - e \notin R^*$. De idealen $(e) \neq R$ en $(1 - e) \neq R$ zijn onderling ondeelbaar, want er geldt $(e) + (1 - e) = R$. Dan volgt met de Chinese Reststelling dat

$$\phi : R \to R/(e) \times R/(1 - e)$$

een surjectief ringhomomorfisme is met kern $(e)(1 - e) = (e) \cap (1 - e) = (0)$. Dan is ϕ een isomorfisme en geldt $R \cong R/(e) \times R/(1 - e)$, waar zowel $R/(e)$ als $R/(1 - e)$ ongelijk is aan de nulring. □

Dit lemma houdt in dat een ring R een samenhangend spectrum heeft dan en slechts dan als R niet de nulring is en geen idempotenten heeft ongelijk aan 0 of 1. We noemen een commutatieve ring R *samenhangend* als geldt $\#\operatorname{Id}(R) = 2$. De samenhangendheid van het spectrum heeft voor de continue functie $\operatorname{rang}_{P/R} : \operatorname{Spec} R \to \mathbb{Z}$ het volgende gevolg.

Gevolg 4.11. *Zij $R \neq 0$ een commutatieve ring en stel dat 0 en 1 de enige idempotenten zijn in R. Dan heeft elk eindig voortgebracht projectief R-moduul P constante rang, d.w.z.* $\text{rang}_{P/R} : \text{Spec}\, R \to \mathbb{Z}$ *is constant.*

Bijvoorbeeld voor een lokale commutatieve ring R geldt dat alle projectieve R-modulen P constante rang hebben. Voor een lokale niet per se commutatieve ring R geldt namelijk het volgende.

Lemma 4.12. *Zij R een lokale ring. Dan heeft R geen idempotenten ongelijk aan 0 en 1.*

Bewijs. Stel $e \in R$ is een idempotent. Dan is ook $1 - e$ is een idempotent ongelijk aan 0 en 1. Voor een lokale ring R geldt dat niet-eenheden gesloten zijn onder optelling, zie T. Y. Lam [4] hoofdstuk 7 stelling 19.1. Omdat geldt $e + 1 - e = 1$, is de som van e en $1 - e$ een eenheid en is dus een van beide een eenheid. Daarentegen hebben we dat $e(1 - e) = 0$ en dan volgt dat e of $1 - e$ gelijk is aan 0. □

5 Een lokale groepenring

Definitie 3.11 geeft dat een ring lokaal is wanneer deze een uniek maximaal linksideaal heeft.

Stelling 5.1. *Zij p een priem, k een lichaam van karakteristiek p en G een eindige p-groep. Dan is de groepenring $k[G]$ lokaal.*

Ten eerste kunnen we voor een groepenring $k[G]$ als in de stelling een maximaal ideaal aanwijzen.

Definitie 5.2. Zij G een groep en k een ring. De *augmentatie-afbeelding* is het ringhomomorfisme

$$i_G : k[G] \to k, \sum_{\sigma \in G} a_\sigma \sigma \mapsto \sum_{\sigma \in G} a_\sigma.$$

De kern $I_G = \ker i_G$ heet het *augmentatie-ideaal*.

De afbeelding i_G is surjectief. Als k een lichaam is, dan is de kern I_G een maximaal ideaal in $k[G]$ omdat geldt $k[G]/I_G \cong k$, een lichaam.

Lemma 5.3. *Zij G een groep en k een ring. Laat $S \subset k[G]$ de verzameling $\{\sigma - 1 \mid \sigma \in G\}$ zijn. Dan geldt $I_G = (S)$, het linksideaal voortgebracht door S.*

Bewijs. Ten eerste hebben we dat $S \subset I_G$, omdat voor alle $\sigma \in G$ geldt $i_G(\sigma - 1) = 1 - 1 = 0$. Omdat i_G een ringhomomorfisme is, volgt dat $(S) \subset I_G$. Voor de andere inclusie, zij $\sum_{\sigma \in G} a_\sigma \sigma \in I_G$. Dan geldt $\sum_{\sigma \in G} a_\sigma = 0$ en

$$\sum_{\sigma \in G} a_\sigma \sigma = \sum_{\sigma \in G} a_\sigma \sigma - \sum_{\sigma \in G} a_\sigma = \sum_{\sigma \in G} a_\sigma (\sigma - 1) \in (S).$$

Dus geldt $I_G \subset (S)$ en $I_G = (S)$. □

Lemma 5.4. *Zij k een ring, G een groep en H een normale ondergroep van G. Laat $\pi : G \to G/H$ het natuurlijke groepshomomorfisme zijn. Dan induceert π een k-lineair ringhomomorfisme*

$$\pi' : k[G] \to k[G/H], \sum_{\sigma \in G} a_\sigma \sigma \mapsto \sum_{\sigma \in G} a_\sigma \pi(\sigma)$$

waarvoor geldt $\ker \pi' = (I_H) = k[G] \cdot I_H$*, het linksideaal voortgebracht door* I_H*.*

Bewijs. Omdat π een groepshomomorfisme is, geldt dat π' een ringhomomorfisme is, welke duidelijk k-lineair is.

Voor $\tau \in H$, geldt $\pi'(\tau - 1) = 0$. Dus de voortbrengers van I_H, zie lemma 5.3, zijn elementen van $\ker \pi'$. Omdat π' een ringhomomorfisme is, geldt dan dat $I_H \subset \ker \pi'$ en $k[G] \cdot I_H \subset \ker \pi'$.

Om de inclusie $\ker \pi' \subset k[G] \cdot I_H$ te bewijzen, stel $x = \sum_{\sigma \in G} a_\sigma \sigma \in \ker \pi'$. Laat P een verzameling representanten zijn van de linkernevenklassen G/H. Dan geldt

$$x = \sum_{\sigma \in G} a_\sigma \sigma = \sum_{\rho \in P} \rho \left(\sum_{\tau \in H} a_{\rho,\tau} \tau \right)$$

voor zekere $a_{\rho,\tau} \in k$. Omdat voor iedere $\tau \in H$ geldt $\pi'(\tau) = 1$, geldt

$$0 = \pi'(x) = \sum_{\rho \in P} \pi'(\rho) \left(\sum_{\tau \in H} a_{\rho,\tau} \right).$$

Voor verschillende representanten ρ_1, ρ_2 geldt $\pi'(\rho_1) \neq \pi'(\rho_2)$, dus hebben we dat voor elke $\rho \in P$ moet gelden $\sum_{\tau \in H} a_{\rho,\tau} = 0$. Dus geldt $\sum_{\tau \in H} a_{\rho,\tau} \tau \in I_H$ voor iedere $\rho \in P$ en $x \in k[G] \cdot I_H$. □

Bewijs stelling 5.1. We bewijzen we met inductie naar n dat voor alle $n \geq 0$ geldt dat $(I_G)^{p^n} = (0)$ voor een eindige p-groep G met orde $\#G = p^n$.

Voor $n = 0$, geldt $G = \{1\}$ en $I_G = 0$. Stel $n = 1$ en $\#G = p$. Dan is G een cyclische groep van orde p en daarmee een abelse groep. Laat $a \in G$ een voortbrenger van G zijn. Nu geldt dat S gelijk is aan $\{\sigma - 1 \mid \sigma \in G\} = (a-1)$, het ideaal voortgebracht door $a - 1$. Bij uitdelen naar het ideaal $(a-1)$ krijgen we namelijk $a \equiv 1 \bmod (a-1)$ en dus $a^k \equiv 1 \bmod (a-1)$ voor $0 < k \leq p$. Het lichaam k heeft karakteristiek p, dus er geldt dat $(a-1)^p = a^p - 1 = 1 - 1 = 0 \in k[G]$. Daarom geldt voor $x \in I_G = (a-1)$ dat $x^p = 0$ en $(I_G)^p = (k[G] \cdot (a-1))^p = (0)$.

Zij G een eindige p-groep met $\#G = p^n$ voor $n \geq 1$. Uit de theorie voor eindige p-groepen halen we dat het centrum $Z(G)$ van G niet triviaal is, zie hiervoor bijvoorbeeld S. Lang [2] hoofdstuk I stelling 6.5. Dan is $Z(G)$ een groep met orde p^k voor $k \geq 1$ en dus geeft de stelling van Cauchy dat $Z(G)$ een ondergroep H heeft van orde p. Deze ondergroep H is normaal in G. Beschouw voor deze $H \subset G$ het groepshomomorfisme $\pi : G \to G/H$ en het geïnduceerde surjectieve ringhomomorfisme

$$\pi' : k[G] \to k[G/H], \sum_{\sigma \in G} a_\sigma \sigma \mapsto \sum_{\sigma \in G} a_\sigma \pi(\sigma).$$

Merk op dat $\pi'(I_G) \subset I_{G/H}$, omdat de samenstelling $i_{G/H} \circ \pi'$ gelijk is aan de augmentatie-afbeelding i_G. Omdat G/H een eindige p-groep is met orde p^{n-1}, volgt met de inductiehypothese dat $(I_{G/H})^{p^{n-1}} = (0)$ en dus $(I_G)^{p^{n-1}} \subset \ker \pi'$.

Wegens lemma 5.4 geldt $\ker \pi' = k[G] \cdot I_H$ en daarmee hebben we dat

$$k[G]/(k[G] \cdot I_H) \cong k[G/H].$$

De inductiehypothese voor H geeft dat $(I_H)^p = (0)$. Omdat $H \subset Z(G)$, geldt $I_H \subset Z(k[G])$ en commuteert I_H met elementen van de ring $k[G]$. Daarmee volgt $(\ker \pi')^p = (k[G] \cdot I_H)^p = k[G](I_H)^p = (0)$. Omdat we hadden $(I_G)^{p^{n-1}} \subset \ker \pi'$ volgt de gewenste conclusie $(I_G)^{p^n} = (0)$.

Hieruit volgt dat $k[G]$ lokaal is: het augmentatie-ideaal I_G is nilpotent en dus is deze bevat in elk maximaal linksideaal, zie S. Lang [2] hoofdstuk XVII stelling 6.1. Echter I_G is zelf een maximaal linksideaal en daarom is I_G het unieke maximale linksideaal van $k[G]$. □

6 Idempotenten in groepenringen

6.1 Idempotenten in een groepenring over een samenhangende ring

We kunnen nu stelling 1.1 bewijzen, die we voor het gemak van de lezer herhalen.

Stelling 6.1. *Zij R een commutatieve ring en G een eindige groep. Dan geldt $\#\operatorname{Id}(R[G]) = 2$ dan en slechts dan als $\#\operatorname{Id}(R) = 2$ en voor iedere priem p met $p|\#G$ geldt $p \cdot 1 \notin R^*$.*

Gevolg 4.11 geeft dat als $\#\operatorname{Id}(R) = 2$, de functie $\operatorname{rang}_{P/R}$ voor een eindig voortgebracht projectief R-moduul P constant is. Noteer $\operatorname{rang}_{P/R}$ voor het gehele getal waarvoor geldt $\operatorname{rang}_{P/R}(\mathfrak{p}) = \operatorname{rang}_{P/R}$ voor alle priemidealen $\mathfrak{p} \subset R$. Het bewijs van stelling 6.1 berust dan op de volgende stelling.

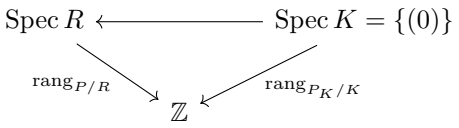
Stelling 6.2. *Stel $\#\operatorname{Id}(R) = 2$ en voor iedere priem p met $p|\#G$ geldt $p \cdot 1 \notin R^*$. Zij P een eindig voortgebracht projectief $R[G]$-moduul. Dan is P een eindig voortgebracht projectief R-moduul en $\#G|\operatorname{rang}_{P/R}$.*

Bewijs. Zij P een eindig voortgebracht projectief $R[G]$-moduul. Dan bestaat er wegens propositie 3.6 een $R[G]$-moduul Q zodat $P \oplus Q \cong R[G]^{(I)}$ voor een eindige verzameling I. Omdat $R[G]$ vrij en eindig voortgebracht is als R-moduul, volgt dan dat $P \oplus Q \cong R[G]^{(I)} \cong R^{(J)}$ voor een eindige verzameling J. Dan is P dus een eindig voortgebracht projectief R-moduul.

Het bewijs van $\#G|\operatorname{rang}_{P/R}$ wordt gegeven in drie stappen. Ten eerste is de stelling waar als $R = k$ een lichaam van karakteristiek p met p een priem en G een p-groep. De ring $k[G]$ is namelijk lokaal, dus een projectief $k[G]$-moduul P is een vrij moduul. Ook is $k[G]$ een vrij k-moduul met $\operatorname{rang}_{k[G]/k} = \#G$. Dus P is een vrij k-moduul met $\#G|\operatorname{rang}_{P/k}$.

De tweede stap bewijst dat de stelling waar is voor $G \neq 1$ een p-groep en een ring R zoals in de stelling. Voor G een p-groep, beschouw het ideaal $(p \cdot 1) \subset R$.

Omdat $p \cdot 1 \notin R^*$, geldt $(p \cdot 1) \neq R$. Dus $(p \cdot 1)$ is bevat in een maximaal ideaal $\mathfrak{m}$. Laat $K = R/\mathfrak{m}$ het restklasselichaam zijn, dan is de karakteristiek van K gelijk aan p. Lemma 4.7 geeft dat het diagram



commuteert. De ringen $R[G]$ en K zijn R-algebra's, dus is het tensorproduct $K \otimes_R (R[G])$ ook een R-algebra en ring. Het moduul $P_K = K \otimes_R P$ is dan een $K \otimes_R (R[G])$-moduul. Uit lemma 3.9 halen we een K-lineair isomorfisme $K \otimes_R R[G] \cong K[G]$. Voor P_K hebben we dan de volgende $K \otimes_R (R[G])$-lineaire en dus $K[G]$-lineaire isomorfismes

$$K \otimes_R P \cong K \otimes_R (R[G] \otimes_{R[G]} P) \cong (K \otimes_R R[G]) \otimes_{R[G]} P \cong K[G] \otimes_{R[G]} P.$$

Dan is P_K met lemma 3.10 een eindig voortgebracht en projectief $K[G]$-moduul. Dan geldt met de eerste stap dat $\#G | \operatorname{rang}_{P_K/K}$ en het commutatieve diagram geeft dan dat ook $\#G | \operatorname{rang}_{P/R}$.

Als laatste is de stelling zoals beschreven waar. Stel $p | \#G$ priem willekeurig. Laat S_p een Sylow-p-ondergroep zijn van G en P een eindig voortgebracht projectief $R[G]$-moduul. Dan geldt dat P ook projectief is als $R[S_p]$-moduul, want $R[G]$ is vrij als $R[S_p]$-moduul. Dan geldt met het bovenstaande dat $\#S_p | \operatorname{rang}_{P/R}$. Omdat voor iedere priem p dus geldt $\#S_p | \operatorname{rang}_{P/R}$, volgt $\#G = (\prod_{p|\#G} \#S_p) | \operatorname{rang}_{P/R}$.

□

Bewijs stelling 6.1. Stel $\#\operatorname{Id}(R[G]) = 2$. Dan bewijzen we $\#\operatorname{Id}(R) = 2$ en dat voor elke priem p met $p | \#G$ geldt $p \cdot 1 \notin R^*$. Wegens de natuurlijke inclusie $\operatorname{Id}(R) \subset \operatorname{Id}(R[G])$ geldt dan ook dat $\#\operatorname{Id}(R) \leq 2$. Als zou gelden $\#\operatorname{Id}(R) = 1$, dan geldt $R = 0$ en dus $R[G] = 0$ maar dan zou gelden $\#\operatorname{Id}(R[G]) = 1$; een tegenspraak. Dus hebben we dat $\#\operatorname{Id}(R) = 2$. Stel p is een priem met $p | \#G$ waarvoor geldt $p \cdot 1 \in R^*$. De Stelling van Cauchy geeft dat G een ondergroep van orde p bevat. Laat $H \subset G$ een ondergroep zijn van orde p. Dan geldt dat

$$e = p^{-1} \sum_{\sigma \in H} \sigma$$

een idempotent is van $R[G]$ ongelijk aan 0 of 1, omdat dit element ook voor een $\sigma \in H, \sigma \neq 1$ een coëfficient heeft ongelijk aan 0 en omdat geldt

$$\left(p^{-1} \sum_{\sigma \in H} \sigma\right)^2 = p^{-1} \left(p^{-1} \left(\sum_{\sigma \in H} \sigma\right)^2\right) = p^{-1} \left(p^{-1} \left(\#H \sum_{\sigma \in H} \sigma\right)\right) = p^{-1} \sum_{\sigma \in H} \sigma.$$

Dit bewijst de implicatie van links naar rechts.

Stel nu dat R een ring is zo dat geldt $\#\operatorname{Id}(R) = 2$ en voor iedere priem p met $p | \#G$ geldt $p \cdot 1 \notin R^*$. Zij $e \in \operatorname{Id}(R[G])$ een willekeurige idempotent, dan geldt

$$R[G] = R[G]e \oplus R[G](1 - e).$$

Een element $x \in R[G]$ kan namelijk geschreven worden als $x = x \cdot e + x \cdot (1-e)$ en daarnaast geldt $R[G]e \cap R[G](1-e) = 0$ want $e(1-e) = 0$. Dan zijn $R[G]e$ en $R[G](1-e)$ met propositie 3.6 eindig voortgebrachte projectieve $R[G]$-modulen. We weten dat $\text{rang}_{R[G]/R} = \#G$ en met lemma 4.2 volgt dat geldt

$$\text{rang}_{R[G]e/R} + \text{rang}_{R[G](1-e)/R} = \#G.$$

Uit stelling 6.2 volgt nu dat geldt $\#G | \text{rang}_{R[G]e/R}$ en $\#G | \text{rang}_{R[G](1-e)/R}$. De vergelijking geeft dan dat een van beide rangen gelijk moet zijn aan 0. Neem aan dat $\text{rang}_{R[G]e/R} = 0$. Dan geldt met lemma 4.5 dat $R[G]e = 0$ en dus dat $e = 0$. Als $\text{rang}_{R[G](1-e)/R} = 0$, dan volgt dat $e = 1$. Dus geldt $e = 0$ óf $e = 1$ en dus geldt $\#\,\text{Id}(R[G]) = 2$. □

6.2 Idempotenten in groepenringen

Voor een niet per se samenhangende ring R en een eindige groep G is een nodige en voldoende voorwaarde voor $\text{Id}(R[G]) = \text{Id}(R)$ gegeven door stelling 1.2 die we hier herhalen.

Stelling 6.3. *Zij R een commutatieve ring en G een eindige groep. Dan geldt $\text{Id}(R) = \text{Id}(R[G])$ dan en slechts dan als voor iedere $e \in \text{Id}(R) \setminus \{1\}$ en voor elke priem $p | \#G$ geldt $pR + eR \neq R$.*

Merk op dat voor R gelijk aan de nulring de verzameling $\text{Id}(R) \setminus \{1\}$ leeg is en daarmee de eis aan de rechter zijde een lege eis is. Maar voor $R = 0$ geldt $R[G] = 0$ en daarmee geldt ook dan dat $\text{Id}(R) = \text{Id}(R[G])$.

In het bewijs van deze stelling gebruiken we het begrip noethers. Een commutatieve ring R heet *noethers* als er geen oneindige stijgende keten

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq ...$$

van idealen in R bestaat. Een commutatieve ring R is noethers dan en slechts dan als ieder ideaal in R door een eindige verzammeling $S \subset R$ wordt voortgebracht. Voor theorie over noetherse ringen, zie hoofstuk 7 in [1]. Een belangrijke stelling hieruit is de basisstelling van Hilbert (Hilbert's Basis Theorem).

Stelling 6.4 (Basisstelling van Hilbert)**.** *Zij R een noetherse ring. Dan is de polynoomring $R[X]$ noethers.*

Als een commutatieve ring R noethers is, dan volgt met inductie dat de ring $R[X_1, ..., X_n]$ ook noethers is.

Lemma 6.5. *Zij A een noetherse ring. Dan is $\text{Id}(A)$ een eindige verzameling en dan geldt $A \cong \prod_{i \in I} A_i$, een eindig product van samenhangende ringen A_i.*

Bewijs. Ten eerste geldt dat A slechts eindig veel idempotenten heeft. Stel namelijk dat $\text{Id}(A)$ oneindig veel elementen bevat. Dan heeft A zeker een idempotent ongelijk aan 0 of 1 en dan geeft lemma 4.10 dat $A \cong A_1 \times B_1$ waar zowel A_1 als B_1 een ring ongelijk aan de nulring is. Omdat er geldt $\#\,\text{Id}(A) = \#\,\text{Id}(A_1) \cdot \#\,\text{Id}(B_1)$, heeft A_1 of B_1 oneindig veel idempotenten. Stel zonder de algemeenheid te schaden dat A_1 oneindig veel idempotenten heeft.

De projectie $\pi_1 : A_1 \times B_1 \to A_1$ naar A_1 is een surjectief ringhomomorfisme met kern $0 \times A_2$ en dus met een kern ongelijk aan 0. Beschouw de compositie

$$g_1 : A \xrightarrow{\sim} A_1 \times B_1 \xrightarrow{\pi_1} A_1$$

en laat $I_1 = \ker g_1$ zijn.

Omdat A_1 oneindig veel idempotenten heeft, kunnen we het bovenstaande voor A_1 herhalen. Dan geldt $A_1 \cong A_2 \times B_2$ waar A_2 oneindig veel idempotenten heeft en B_2 niet de nulring is. Definiëer de afbeelding

$$g_2 : A_1 \xrightarrow{\sim} A_2 \times B_2 \xrightarrow{\pi_2} A_2$$

en laat $I_2 = \ker(g_2 \circ g_1)$ zijn. Dan geldt $I_1 \subsetneq I_2$, want er is een inclusie $\ker g_1 \subset \ker(g_2 \circ g_1)$ maar geen gelijkheid want $\ker g_2 = 0 \times B_2 \neq 0$.

Dit proces herhalen geeft een oneindige stijgende keten van idealen in A

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots .$$

Dan is A dus niet noethers. Dit bewijst dat voor een noetherse ring A geldt dat het aantal idempotenten in A eindig is. Het bewijs dat A isomorf is met een product van een eindig aantal samenhangende ringen gaat met inductie naar $\#\operatorname{Id}(A)$. Stel $\#\operatorname{Id}(A) = m$. Voor $m = 1$ is A de nulring, welke gelijk is aan het lege product $\prod_{i \in \emptyset} R_i$ van nul samenhangende ringen. Voor $m = 2$ is A een samenhangende ring en dus een product van eindig veel samenhangende ringen. Stel $m > 2$, dan heeft A een idempotent ongelijk aan 0 of 1 en dus volgt met lemma 4.10 dat $A \cong R_1 \times R_2$ waar zowel R_1 als R_2 een ring is ongelijk aan de nulring. Dan geldt $\#\operatorname{Id}(R_1) \neq 1 \neq \#\operatorname{Id}(R_2)$ en met de gelijkheid $\#\operatorname{Id}(A) = \#\operatorname{Id}(R_1) \cdot \#\operatorname{Id}(R_2)$ volgt dat $\#\operatorname{Id}(R_1) < m$ en $\#\operatorname{Id}(R_2) < m$. Merk op dat dan wegens het bovenstaande zowel R_1 als R_2 noethers is. Met de inductiehypothese volgt dan dat $R_1 \cong \prod_{i=1}^{n_1} B_i$ en $R_2 \cong \prod_{j=1}^{n_2} C_j$ waar de B_i en C_j samenhangende ringen zijn. Daarmee hebben we bewezen dat geldt $A \cong R_1 \times R_2 \cong \prod_{i=1}^{n_1} B_i \times \prod_{j=1}^{n_2} C_j \cong \prod_{i=1}^{n} A_i$ voor samenhangende ringen A_i. □

Naast het begrip van een noetherse ring, gaan we ook het volgende begrip gebruiken.

Definitie 6.6. Zij R een commutatieve ring. De ring R is van *eindig type* als een een eindige verzameling $\{x_1, \dots, x_n\} \subset R$ bestaat die de ring R voortbrengt. Dat wil zeggen dat ieder element van R geschreven kan worden als polynoom in $x_1, \dots, x_n$ met coëfficiënten in $\mathbb{Z}$.

Equivalent met de bovenstaande definitie is te zeggen dat een ring van eindig type is als er een surjectief homomorfisme bestaat $\mathbb{Z}[X_1, \dots, X_n] \to R$. Dan geldt $R \cong \mathbb{Z}[X_1, \dots, X_n]/I$ waar I de kern van het homomorfisme is. De ring $\mathbb{Z}$ is noethers en de basisstelling van Hilbert geeft dan dat de ring $\mathbb{Z}[X_1, \dots, X_n]$ noethers is. Dan is het quotient $\mathbb{Z}[X_1, \dots, X_n]/I$ ook noethers en dus is een ring R van eindig type een noetherse ring.

Bewijs stelling 6.3. Stel er bestaat een $e \in \mathrm{Id}(R) \setminus \{1\}$ en een priem p met $p|\#G$ zodanig dat $pR + eR = R$. Zoals gebruikt in lemma 4.10 geeft de Chinese Reststelling een ringisomorfisme

$$R \xrightarrow{\sim} R/eR \times R/(1-e)R.$$

Deze afbeelding induceert een isomorfisme

$$\phi : R[G] \xrightarrow{\sim} (R/eR)[G] \times (R/(1-e)R)[G].$$

In de ring R/eR geldt dat $p \in (R/eR)^*$ omdat geldt $pR + eR = R$. Laat $H \subset G$ een ondergroep zijn van orde p. Dan is het element $p^{-1} \sum_{\sigma \in H} \sigma$ net als in het bewijs van stelling 6.1 een idempotent in $(R/eR)[G]$ ongelijk aan 0 of 1. Dan is het element $(p^{-1} \sum_{\sigma \in H} \sigma, 1)$ een idempotent in $(R/eR)[G] \times (R/(1-e)R)[G]$, welke via het isomorfisme een idempotent geeft in $R[G]$. Deze ligt echter niet in R, want stel $x \in R \subset R[G]$. Dan geldt dat $\phi(x) = ((x + eR), (x + (1-e)R))$ en de eerste term hier $(x + eR) = (x + eR) \cdot 1 \in (R/eR)[G]$ heeft alleen voor $1 \in G$ een niet-nul coëfficient. Dit bewijst $\mathrm{Id}(R) \neq \mathrm{Id}(R[G])$ en de eerste implicatie.

Voor de tweede implicatie, neem aan dat voor alle $e \in \mathrm{Id}(R) \setminus \{1\}$ en voor elke priem $p|\#G$ geldt $pR + eR \neq R$. Er is een natuurlijke inclusie $R \subset R[G]$ en daarmee een inclusie $\mathrm{Id}(R) \subset \mathrm{Id}(R[G])$. Wat nog bewezen moet worden, is dat voor iedere $e \in \mathrm{Id}(R[G])$ geldt $e \in \mathrm{Id}(R)$. We bouwen het bewijs hiervan in drie stappen op. Ten eerste hebben we dat voor een samenhangende ring R geldt $\#\,\mathrm{Id}(R) = 2 = \#\,\mathrm{Id}(R[G])$ met stelling 6.1 en dan volgt dat $\mathrm{Id}(R) = \mathrm{Id}(R[G])$. Voor de tweede stap, laat $R \cong \prod_{i=1}^n R_i$ het product van een eindig aantal samenhangende ringen R_i zijn. Dan geldt dat $R[G] = \prod_{i=1}^n (R_i[G])$. Voor twee ringen R_1, R_2 geldt $\#\,\mathrm{Id}(R_1 \times R_2) = \#\,\mathrm{Id}(R_1) \cdot \#\,\mathrm{Id}(R_2)$ en dan volgt dat

$$\#\,\mathrm{Id}(\prod_{i=1}^n R_i) = \prod_{i=1}^n \#\,\mathrm{Id}(R_i) = 2^n = \prod_{i=1}^n \#\,\mathrm{Id}(R_i[G]) = \#\,\mathrm{Id}(\prod_{i=1}^n (R_i[G])).$$

Dan geldt ook voor een ring $R = \prod_{i=1}^n R_i$ dat $\#\,\mathrm{Id}(R) = \#\,\mathrm{Id}(R[G])$ en dus $\mathrm{Id}(R) = \mathrm{Id}(R[G])$.

Als derde en laatste stap, beschouw een willekeurige commutatieve ring R die voldoet aan de voorwaarden. Zij $e = \sum_{\sigma \in G} a_\sigma \sigma \in \mathrm{Id}(R[G])$. Laat $R' \subset R$ de deelring zijn voortgebracht door $\{a_\sigma\}_{\sigma \in G}$. Dan is R' van eindig type en dus een noetherse ring.

Dan volgt uit lemma 6.5 dat $R' \cong \prod_{i=1}^n R_i$ voor R_i samenhangende ringen. Voor deze ring weten we dus al dat geldt $\mathrm{Id}(R') = \mathrm{Id}(R'[G])$. Omdat voor de idempotent e geldt $e \in R'[G]$, geldt dus ook dat $e \in \mathrm{Id}(R')$. Dus hebben we dat $e \in \mathrm{Id}(R)$. □

Referenties

[1] M. F. Atiyah and I. G. MacDonald, Introduction to Commutative Algebra, Addison-Wesley, Reading MA, 1969.

[2] S. Lang, Algebra, Revised 3rd Edition, Springer-Verlag, New York, 2002.

[3] T. Y. Lam, Serre's Conjecture, Lecture Notes in Mathematics, vol. 635, Springer-Verlag, Berlin, 1978.

[4] T. Y. Lam, A First Course in Noncommutative Rings, Springer-Verlag, New York, 1991.

[5] Donald S. Passman, The algebraic structure of group rings, Wiley, New York, 1977.

[6] I. Kaplansky, Projective Modules, Ann. Math. 68, 1958.

[7] T. W. Müller, Groups: Topological, Combinatorial and Arithmetic Aspects, London Mathematical Society Lecture Notes Series 311, Cambridge University Press, Cambridge, 2004.

[8] D. B. Coleman, Idempotents in Group Rings, Proc. Amer. Math. Soc., Vol. 17 p. 962, 1966.