Representatietheorie

1 Historische en wiskundige achtergrond

Zij G een eindige groep en k een lichaam. We zullen meestal $k = \mathbb{C}$ nemen, maar we hebben eigenlijk alleen nodig dat k een algebraïsch afgesloten lichaam is van karakteristiek 0.

Definitie 1.1. *Een* representatie *van G (over k) is een groepshomomorfisme $\rho : G \longrightarrow GL(n,k)$ voor een $n \geq 0$. We noemen n de* dimensie *van ρ.*

Zoals bekend is $GL(n,k) = \{A \in M(n,k) : \det A \in k^*\} = M(n,k)^*$.

De matrixring $M(0,k)$ heeft één element: (), met determinant 1. Daarom geldt dat $GL(0,k) = M(0,k)^* = \{()\}$ en de enige representatie van dimensie 0 is het triviale homomorfisme. Voor dimensie 1 geldt dat $GL(1,k) = k^*$. Dit is in het bijzonder een abelse groep. Voor dimensie 2 en hoger geldt dat $GL(n,k)$ niet abels is voor elk lichaam k.

Definitie 1.2. *Twee representaties $\rho, \rho' : G \longrightarrow GL(n,k)$ heten* equivalent *als er een $A \in GL(n,k)$ bestaat zodanig dat voor alle $\sigma \in G$ geldt dat $\rho'(\sigma) = A\rho(\sigma)A^{-1}$.*

Later zullen we een andere definitie van een representatie geven: een representatie van G over k is een $k[G]$-moduul van eindige k-dimensie.

Een probleem dat Richard Dedekind (1831–1916) aan Frobenius (1849–1917) stelde, vormde een aanzet tot de representatietheorie. Dit probleem betrof het begrip *groependeterminant*.

Definitie 1.3. *Zij G een eindige groep. De* groependeterminant *van G is*

$$\det\left[X_{\sigma\tau^{-1}}\right]_{\sigma,\tau\in G} \in \mathbb{C}[X_\sigma : \sigma \in G].$$

Voorbeeld
Voor de groep van orde 2 ziet de groependeterminant er als volgt uit:

$$\begin{vmatrix} X_1 & X_2 \\ X_2 & X_1 \end{vmatrix} = X_1^2 - X_2^2 = (X_1 + X_2)(X_1 - X_2).$$

Voor de groep van orde 3 krijgen we:

$$\begin{vmatrix} X_1 & X_3 & X_2 \\ X_2 & X_1 & X_3 \\ X_3 & X_2 & X_1 \end{vmatrix} = (X_1 + X_2 + X_3)(X_1 + \zeta X_2 + \zeta^2 X_3)(X_1 + \zeta^2 X_2 + \zeta X_3),$$

waarbij $\zeta = e^{\frac{2\pi i}{3}}$ een primitieve derde eenheidswortel is.

Voor abelse groepen G vond Dedekind een uitdrukking voor de groependeterminant:

$$\det\left[X_{\sigma\tau^{-1}}\right]_{\sigma,\tau\in G} = \prod_{\rho} \sum_{\sigma\in G} \rho(\sigma) X_\sigma,$$

waarbij ρ loopt over de groepshomomorfismen $\rho : G \longrightarrow GL(1, \mathbb{C}) = \mathbb{C}^*$. Het aantal van deze groepshomomorfismen is gelijk aan de orde van G.

We noemen $\mathrm{Hom}(G, \mathbb{C}^*) = \hat{G}$ de *duale* van G. Als G eindig en abels is, dan geldt $\#\hat{G} = \#G$. Er bestaat een canoniek isomorfisme tussen $\hat{\hat{G}}$ en G.

De vraag aan Frobenius was nu: hoe zit het met de groependeterminant van niet-abelse groepen? In het geval $G = S_3$ vinden we dat $\det[X_{\sigma\tau^{-1}}]$ het product is van twee factoren van graad 1 en het kwadraat van een factor van graad 2. Wat is de algemene theorie hierachter?

Zij G een eindige groep van orde n. In het algemeen geldt dat

$$\det[X_{\sigma\tau^{-1}}]_{\sigma,\tau\in G} = \prod_{i=1}^{t} P_i^{n_i},$$

met $P_i \in \mathbb{C}[X_\sigma : \sigma \in G]$ irreducibel, homogeen van graad n_i en paarsgewijs verschillend.

Uit het vergelijken van de graden van het rechter- en linkerlid volgt dat $n_1^2 + n_2^2 + n_3^2 + \ldots + n_t^2 = n$. Ook geldt dat t gelijk is aan het aantal conjugatieklassen van G. Verder is n_i voor alle i een deler van n en is het aantal lineaire factoren in de groependeterminant gelijk aan $\#\left(G/[G,G]\right)$, de index van de commutatorondergroep van G in G.

Voorbeeld
We nemen voor G de kwaternionengroep $Q = \{\pm 1, \pm i, \pm j, \pm k\}$, met $n = 8$. De conjugatieklassen zijn $\{1\}$, $\{-1\}$, $\{\pm i\}$, $\{\pm j\}$ en $\{\pm k\}$, dus $t = 5$. De commutatorondergroep $[Q, Q]$ is gelijk aan $\langle -1 \rangle$, dus het aantal lineaire factoren in de groependeterminant is $\frac{8}{2} = 4$. We vinden nu dat $8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2$.

Laat nu G gelijk zijn aan S_4. Dan is $n = 24$ en $t = 5$. De commutatorondergroep is A_4. We vinden nu dat $24 = 1^2 + 1^2 + 2^2 + 3^2 + 3^2$.

Het algemene geval is opgelost door Frobenius:

$$\det[X_{\sigma\tau^{-1}}]_{\sigma,\tau\in G} = \prod_{\rho} \left(\det\left(\sum_{\sigma\in G} \rho(\sigma) X_\sigma \right) \right)^{\dim\rho},$$

waarbij ρ loopt over de irreducibele representaties van G, op equivalentie na. (We zullen later zien wat irreducibiliteit van een representatie betekent.)

Merk op dat $\rho(\sigma)$ een element is van $GL(n, \mathbb{C})$. Daarom is $\sum_{\sigma\in G} \rho(\sigma) X_\sigma$ een element van $M(\dim\rho, \mathbb{C}[X_\sigma : \sigma \in G])$.

2 Oplosbare groepen

We gaan nu een stelling uit de groepentheorie formuleren die met behulp van representatietheorie bewezen wordt. Ter voorbereiding geven we een aantal definities en stellingen.

Definitie 2.1. *Een groep G heet* oplosbaar *als er een keten van ondergroepen*

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_{t-1} \subset G_t = G$$

met $t \in \mathbb{Z}_{\geq 0}$ bestaat zodat voor elke $0 < i \leq t$ geldt dat G_{i-1} normaal is in G_i met G_i/G_{i-1} abels.

De voorwaarden dat G_{i-1} normaal is in G_i en dat G_1/G_{i-1} abels is, zijn equivalent met de voorwaarde dat $G_i \supset G_{i-1} \supset [G_i, G_i]$.

Voorbeeld
De permutatiegroep S_4 is oplosbaar: $\{(1)\} \subset V_4 \subset A_4 \subset S_4$. Merk op dat deze keten niet uniek is: hij kan nog verfijnd worden tot $\{(1)\} \subset \langle (1\ 2)(3\ 4) \rangle \subset V_4 \subset A_4 \subset S_4$.

Met behulp van het volgende procédé kunnen we nagaan of een groep G oplosbaar is en, als dat het geval is, construeert het tegelijk een keten. Een groep G is oplosbaar dan en slechts dan als de keten

$$\ldots \subset [G_{t-1}, G_{t-1}] = G_{t-2} \subset [G_t, G_t] = G_{t-1} \subset G_t = G$$

in een eindig aantal stappen uitmondt in de triviale groep. Op deze manier vinden we altijd een keten zodat de ondergroepen G_{i-1} normaal zijn in G en niet alleen in G_i.

Voorbeeld
Uit deze equivalentie volgt dat S_5 niet oplosbaar is: $[A_5, A_5] = A_5 = [S_5, S_5] \subset S_5$.

Voor een eindige oplosbare groep kunnen we altijd een keten maken waarin de quotiënten G_i/G_{i-1} niet alleen abels, maar zelfs cyclisch zijn. Deze aanpassing sluit in sommige gevallen uit dat in deze keten alle ondergroepen ook normaal zijn in G. De eis dat er een keten

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_{t-1} \subset G_t = G$$

bestaat waarin zowel de quotiënten cyclisch zijn als de ondergroepen normaal in G, is dus sterker dan de eis dat de groep oplosbaar is.

Voor sommige groepen kunnen we meteen zeggen dat ze oplosbaar zijn, zoals we kunnen zien in deze stelling. Het bewijs is te vinden in de syllabus Algebra I.

Stelling 2.2. *Zij p een priemgetal en G een eindige groep waarvan de orde een macht van p is (een "p-groep"). Dan is G oplosbaar.*

Definitie 2.3. *Stel G is een eindige groep en p een priemgetal. Laat p^k de grootste macht van p zijn die de orde van G deelt. Een ondergroep van G van orde p^k noemen we een* Sylow-p-ondergroep *van G.*

Stelling 2.4. *Zij G een eindige groep en p een priemgetal. Dan heeft G een Sylow-p-ondergroep. Elke twee Sylow-p-ondergroepen zijn geconjugeerd.*

Stelling 2.5 (Burnside (1904)). *Stel G is een eindige groep van orde $p^a q^b$ met p, q priem en a, $b \in \mathbb{Z}_{\geq 0}$. Dan is G oplosbaar.*

Deze stelling wordt met representatietheorie bewezen. Er is ook een "elementair" bewijs. Dit is echter een stuk complexer. Een sterker resultaat is de volgende stelling. Het bewijs hiervan is te lang om op dit college te behandelen.

Stelling 2.6 (Feit, Thompson (rond 1966)). *Elke eindige groep van oneven orde is oplosbaar.*

Een gerelateerd begrip is dat van een *simpele groep.*

Definitie 2.7. *Een groep G heet* simpel *als G precies twee normaaldelers heeft, namelijk G zelf en $\{1\}$. Merk op dat $\{1\}$ dus niet simpel is.*

Bekende simpele groepen zijn bijvoorbeeld de A_n voor alle $n \geq 5$. Er bestaat een classificatie van alle eindige simpele groepen (met een bewijs van duizenden pagina's door meer dan honderd wiskundigen).

Als G een niet-simpele groep is, heeft G een normaaldeler N met $N \neq G$ en $N \neq \{1\}$. Een strategie voor het bewijzen van oplosbaarheid van een niet-simpele groep G is de oplosbaarheid via inductie afleiden uit de oplosbaarheid van N en G/N.

De volgende stelling geeft een manier om voor sommige groepen expliciet een N als hierboven te vinden. Het enige bekende bewijs van deze stelling gebruikt representatietheorie.

Stelling 2.8. *Zij G een eindige groep, en $C \subset G$ een conjugatieklasse, zodanig dat $\#C = p^n$ met p priem en $n \geq 1$. Dan is de ondergroep van G voortgebracht door $\{\sigma\tau^{-1} : \sigma, \tau \in C\}$ een normaaldeler van G ongelijk aan $\{1\}$ en G.*

Voorbeeld
Zij $G = S_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$. De conjugatieklassen van S_3 zijn zoals bekend $C_1 = \{(1)\}$, $C_2 = \{(1\ 2\ 3), (1\ 3\ 2)\}$ en $C_3 = \{(1\ 2), (1\ 3), (2\ 3)\}$. Zowel C_2 als C_3 hebben priemmacht-orde en voldoen dus aan de voorwaarden van de stelling. Beide conjugatieklassen geven dezelfde normaaldeler, namelijk $\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. Dit is de A_3, die overigens de enige normaaldeler van S_3 is (naast $\{1\}$ en G).

We zullen nu gebruik makend van stelling 2.8 de stelling van Burnside bewijzen. Hiervoor hebben we een aantal feiten uit de groepentheorie nodig.

Zij G een groep en $N \subset G$ een normaaldeler. Dan is G oplosbaar dan en slechts dan als N en G/N beide oplosbaar zijn.

Als G een eindige groep van priemmacht-orde is, met $\#G > 1$, dan geldt $\#Z(G) > 1$. Hier is $Z(G) = \{\sigma \in G : \forall \tau \in G : \tau\sigma = \sigma\tau\}$ het *centrum* van G. $Z(G)$ is een normaaldeler van G en elke ondergroep van $Z(G)$ ook.

Iedere abelse groep van priemmacht-orde is oplosbaar. Merk op dat dit met inductie naar de groepsorde volgt uit het vorige feit. Immers, $Z(G)$ is een normaaldeler van G die ongelijk aan $\{1\}$ is. We kunnen ook aannemen dat $Z(G) \neq G$ geldt. (Indien $Z(G)$ wel gelijk aan G is, is G abels en dus oplosbaar.) Volgens de inductiehypothese zijn $Z(G)$ en $G/Z(G)$ oplosbaar. Hieruit volgt dat G ook oplosbaar is.

Stel G is een groep en $\tau \in G$. De *normalisator* van τ in G is $N_G(\tau) = \{\sigma \in G : \sigma\tau = \tau\sigma\}$. Zij C de conjugatieklasse van τ: $C = \{\sigma\tau\sigma^{-1} : \sigma \in G\}$. Nu geldt dat $\#C = [G : N_G(\tau)]$ (de index van $N_G(\tau)$ in G).

Bewijs van de stelling van Burnside:

Zij G een eindige groep van orde $p^a q^b$ met p, q priem en a, $b \in \mathbb{Z}_{\geq 0}$. We passen inductie naar de orde van G toe.

Als $\#G = 1$ is G duidelijk oplosbaar en zijn we klaar. Als G van priemmacht-orde is, is G volgens het derde feit oplosbaar en zijn we ook klaar.

Stel dus dat $\#G = p^a q^b$ met $p \neq q$, $a \geq 1$, $b \geq 1$. We gaan een normaaldeler $N \subset G$ construeren met $N \neq \{1\}$, $N \neq G$.

Laat $H \subset G$ een Sylow-q-ondergroep zijn, dus $\#H = q^b$. Kies een $\tau \in Z(H)$, $\tau \neq 1$. (Zo'n τ bestaat wegens het tweede feit.) Dan commuteert τ met alle elementen van H en geldt dus $H \subset N_G(\tau)$. Dus $[G : N_G(\tau)] \mid [G : H] = p^a$, dus $[G : N_G(\tau)] = p^n$ met $0 \leq n \leq a$.

Als $n = 0$, dan is $N_G(\tau) = G$. Dit betekent dat $\forall \sigma \in G : \sigma\tau\sigma^{-1} = \tau$ en dus is $\langle\tau\rangle$ een normaaldeler van G. We kunnen nu $N = \langle\tau\rangle$ nemen, want $N \neq \{1\}$. Als N gelijk aan G is, is G cyclisch en dus oplosbaar, dus we kunnen aannemen dat $N \neq G$.

Stel nu dat $n \geq 1$. Zij C de conjugatieklasse van τ. Dan is $\#C = [G : N_G(\tau)] = p^n$. Stelling 2.8 geeft nu de gezochte N.

De groepen N en G/N hebben nu beide orde kleiner dan $\#G$. Het product van de twee ordes is $p^a q^b$, dus $\#N$ en $\#G/N$ zijn beide het product van twee priemmachten. Volgens de inductiehypothese zijn N en G/N nu oplosbaar. Hieruit volgt dat G oplosbaar is. □

De volgende stelling geeft ook een manier om een normale ondergroep te construeren.

Stelling 2.9 (Frobenius (1901)). *Zij G een groep die transitief werkt op een eindige verzameling X. Noteer $n_\sigma = \#\{x \in X : \sigma x = x\}$ voor $\sigma \in G$. Neem aan dat $n_\sigma \leq 1$ voor alle $\sigma \in G$, $\sigma \neq 1$. Dan geldt dat $\{1\} \cup \{\sigma \in G : n_\sigma = 0\}$ een normale ondergroep van G is die transitief op X werkt.*

Voorbeeld
Zij $G = S_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$ werkend op $\{1, 2, 3\} = X$. We vinden $n_\sigma = 3$ voor $\sigma = 1$, $n_\sigma = 0$ als σ een 3-cykel is, en $n_\sigma = 1$ als σ een 2-cykel is. De stelling geeft nu dat $\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ een normaaldeler van S_3 is. Dit is wederom de A_3.

Zij $G = D_5$, werkend op de vijf hoekpunten van een regelmatige vijfhoek. Dan is $n_\sigma = 5$ als $\sigma = 1$, $n_\sigma = 0$ als σ een rotatie is, en $n_\sigma = 1$ als σ een spiegeling is. Uit de stelling volgt nu dat de rotaties (inclusief de identiteit) een normale ondergroep van D_5 vormen.

Zij $X = k$ een eindig lichaam van orde q. Laat $G = \{\sigma : k \to k : \exists a \in k^*, b \in k : \forall x \in k : \sigma(x) = ax + b\}$. De orde van G is $q(q-1)$. Als de a behorend bij een $\sigma \in G$ ongelijk aan 1 is, heeft σ exact één dekpunt, namelijk $x = -b(a-1)^{-1}$. Als $a = 1$ en $b = 0$, is σ de identiteit met q dekpunten. Als $a = 1$ en $b \neq 0$ heeft σ geen dekpunten. De stelling zegt nu dat de $\sigma \in G$ met $a = 1$ een normale ondergroep van G vormen.

3 Modulen

Definitie 3.1. *Zij R een ring. Een* R-moduul *(of een* links-R-moduul*) is een abelse groep M met een afbeelding $R \times M \to M$, $(r, m) \mapsto rm$ waarvoor, voor alle $r, s \in R$ en $m, n \in M$, geldt dat*

$$\begin{aligned} r(m+n) &= rm + rn \\ (r+s)m &= rm + sm \\ (rs)m &= r(sm) \\ 1m &= m. \end{aligned}$$

De eis dat de onderliggende groep abels is, is niet strict noodzakelijk, aangezien deze volgt uit de eigenschappen van de moduul-afbeelding. Ook gelden de relaties $r0 = 0$, $0m = m$ en $-1m = -m$. Deze zijn ook af te leiden uit de andere eigenschappen.

Een equivalente definitie is de volgende: een *R-moduul* is een abelse groep M met een homomorfisme $\varphi : R \to \mathrm{End}(M)$. Uit deze definitie is snel te zien dat gegeven twee ringen R_1 en R_2, een ringhomomorfisme $f : R_1 \to R_2$ en een R_2-moduul M, er van M een R_1-moduul gemaakt kan worden door φ samen te stellen met f tot $\varphi' : R_1 \xrightarrow{f} R_2 \xrightarrow{\varphi} \mathrm{End}(M)$.

In het geval dat de onderliggende abelse groep multiplicatief geschreven wordt, wordt de moduul-afbeelding rm ook wel genoteerd als m^r of ${}^r m$. Merk op dat bij gebruik van r^m de eigenschap $(rs)m = r(sm)$ de tegen-intuïtieve vorm $m^{(rs)} = (m^s)^r$ heeft.

Behalve links-R-modulen (die we kortweg R-modulen zullen noemen) bestaan er ook *rechts-R-modulen*. We noteren hier de moduul-afbeelding meestal als rechtsvermenigvuldiging. De definitie hiervan is bijna hetzelfde als die van een links-R-moduul, met als uitzondering dat $m(rs) = (mr)s$ (in plaats van $(rs)m = r(sm)$).

Een alternatieve definitie voor een rechts-R-moduul is de volgende: een *rechts-R-moduul* is een abelse groep M met een homomorfisme $\varphi : R^{\mathrm{opp}} \to \mathrm{End}(M)$, of, equivalent, een *antihomomorfisme* $\varphi : R \to \mathrm{End}(M)$.

Herinner: de ring R^{opp} heeft dezelfde onderliggende optelgroep als R maar heeft als vermenigvulding $\cdot_{\mathrm{opp}}$, gedefinieerd door $r \cdot_{\mathrm{opp}} s = s \cdot r$. Een *antihomomorfisme* f tussen twee ringen is een ringhomomorfisme waarvoor $f(rs) = f(s)f(r)$ geldt, in plaats van $f(rs) = f(r)f(s)$.

Definitie 3.2. *Stel R en S zijn ringen. Een* R-S-bimoduul *is een abelse groep M die een links-R-moduul- en een rechts-S-moduulstructuur heeft zodanig dat $r(ms) = (rm)s$, voor alle $r \in R$, $s \in S$, $m \in M$.*

Homomorfismen tussen R-modulen zijn als volgt gedefinieerd.

Definitie 3.3. *Zij R een ring en M en N twee R-modulen. Een* R-homomorfisme *of* R-lineaire afbeelding *van M naar N is een groepshomomorfisme $f : M \to N$ zodanig dat voor alle $r \in R$, $x \in M$ geldt dat $f(rx) = rf(x)$.*

Definitie 3.4. *Zij $f : M \to N$ een R-lineaire afbeelding. Dan heet f een* isomorfisme *tussen R-modulen als er een R-lineaire afbeelding $g : N \to M$ bestaat zodat $fg = id_N$ en $gf = id_M$.*

Analoog aan ringen kunnen we nu de volgende verzamelingen definiëren:
$Hom_R(M,N) = \{R\text{-lineare afbeeldingen van } M \text{ naar } N\}$. Dit is een (additieve) groep met puntsgewijze optelling.
$End_R(M) = Hom_R(M,M)$. De *endomorfismen* vormen een ring met puntsgewijze optelling als optelling en samenstelling van afbeeldingen als vermenigvuldiging.
$Aut_R(M) = End_R(M)^* = \{R\text{-lineare isomorfismen van } M \text{ naar } M\}$. De *automorfismen* vormen een (multiplicatieve) groep met samenstelling van afbeeldingen.

Definitie 3.5. *Zij R een ring en M een R-moduul. Een* deelmoduul *of* deel-R-moduul *van M is een ondergroep N van M zodanig dat $\forall r \in R, x \in N : rx \in N$.*

Voorbeeld
Elke abelse groep M is een $\mathbb{Z}$-moduul. Kies hiervoor φ als volgt.

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & \mathrm{End}(M) \\ x & \longmapsto & \big(y \mapsto \underbrace{y + \ldots + y}_{x \text{ keer}}\big) \end{array}$$

Een linksideaal van een ring R is een R-moduul.

Om het nut van modulen te illusteren, zullen we het bestaan van de Jordannormaalvorm voor matrices over $\mathbb{C}$ bewijzen met behulp van modulen. Hiervoor geven we eerst twee definities en een stelling.

Zij R een hoofdideaaldomein (Engels: principal ideal domain, of PID) en M een R-moduul. Definieer voor $x \in M$ het homomorfisme $g : R \to Rx \subset M$ door $r \mapsto rx$. De kern van g is de *annihilator* van x (notatie: $\mathrm{Ann}(x)$) en is een ondergroep van R. Omdat R een hoofdideaaldomein is, is er een $y \in R$ met $\mathrm{Ann}(x) = (y)$.

Definitie 3.6. *Een voortbrenger van* $\mathrm{Ann}(x)$*, gedefinieerd als hierboven, heet een* orde *van x. Merk op dat de orde gedefinieerd is op vermenigvuldiging met eenheden van R na.*

Definitie 3.7. *Een element $x \in M$ heet* torsie *als de orde van x niet nul is, dus als* $\mathrm{Ann}(x) \neq \{0\}$*. Anders geformuleerd, een element $x \in M$ is torsie als er een $r \in R$ bestaat met $rx = 0$. De torsie-elementen van M vormen een ondergroep $T(M) \subset M$. Als R een commutatieve ring is, is $T(M)$ zelfs een deelmoduul van M.*

Stelling 3.8. *Zij R een hoofdideaaldomein en M een eindig voortgebracht R-moduul. Dan bestaat er een $r \geq 0$ en een R-lineair isomorfisme*

$$M \cong_R T(M) \oplus R^r.$$

r heet de rang *van M. $T(M)$ is isomorf met $\bigoplus_{\mathfrak{p}} M(\mathfrak{p})$, waarbij $\mathfrak{p}$ loopt over de priemidealen van R. Hier is $M(\mathfrak{p})$ het deelmoduul van M van elementen waarvan de orde een macht van $\mathfrak{p}$ is.*

$$M(\mathfrak{p}) \cong_R R/(\mathfrak{p}^{k_1}) \oplus \ldots \oplus R/(\mathfrak{p}^{k_m})$$

met $m \geq 0$, $k_1 \geq k_2 \ldots \geq k_m \geq 0 \in \mathbb{Z}$ uniek bepaald door $\mathfrak{p}$.

Zie voor het bewijs het bewijs van stelling 9.11 in het Algebra 1 dictaat.

Deze structuurstelling van eindig voortgebrachte modulen over een hoofdideaaldomein zullen we gebruiken om het bestaan van de Jordan-normaalvorm te bewijzen.

Zij V een eindig-dimensionale $\mathbb{C}$-vectorruimte en $A \in \mathrm{End}(V)$.

V is een $\mathbb{C}[X]$-moduul. Immers, V is een $\mathbb{C}$-vectorruimte, dus er bestaat een homomorfisme $\mathbb{C} \to \mathrm{End}(V)$: scalaire vermenigvuldiging. We breiden nu scalaire vermenigvuldiging uit tot het homomorfisme $\varphi : \mathbb{C}[X] \to \mathrm{End}(V)$ door $\varphi(X) = A$ te stellen.

De moduul-vermenigvuldiging van $\sum a_i X^i \in \mathbb{C}[X]$ met $x \in V$ ziet er nu als volgt uit: $(\sum a_i X^i)x = \sum a_i A^i(x)$.

V is volledig torsie. Immers, als de rang van V groter dan 0 zou zijn, zou V oneindige dimensie over $\mathbb{C}$ hebben volgens stelling 3.8. (Want $\mathbb{C}[X]$ heeft oneindige dimensie over $\mathbb{C}$.)

Aangezien de priemidealen van $\mathbb{C}[X]$ de vorm $(X - \lambda)$ hebben, geeft stelling 3.8 nu dat V isomorf is met $\bigoplus V_i$, waarbij V_i isomorf is met $\mathbb{C}[X]/(X - \lambda_i)^{n_i}$. Merk op dat de λ_i niet noodzakelijk verschillend hoeven te zijn.

Kies als basis voor V_i de elementen $(X - \lambda_i)^{n_i - 1}, (X - \lambda_i)^{n_i - 2}, \ldots, (X - \lambda_i), 1$. Vermenigvuldiging van de basiselementen met $(X - \lambda_i)$ beeldt 1 af op $(X - \lambda_i)$, $(X - \lambda_i)$ op $(X - \lambda_i)^2$, …, $(X - \lambda_i)^{n_i - 2}$ op $(X - \lambda_i)^{n_i - 1}$ en $(X - \lambda_i)^{n_i - 1}$ op 0. Dit geeft de volgende matrices voor $A - \lambda I$ en A beperkt tot V_i, ten opzichte van de gekozen basis:

$$A - \lambda I = \begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}, \qquad \text{dus } A = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

□

4 Modulen en representatietheorie

Het zal blijken dat een representatie van G over k een $k[G]$-moduul is. Hierbij is $k[G]$ de *groepenring* van G over k.

Definitie 4.1. *Zij k een ring en G een groep. De* groepenring $k[G]$ *van G over k is*

$$k[G] = \Big\{ \sum_{\sigma \in G} a_\sigma \sigma : a_\sigma \in k, a_\sigma = 0 \text{ voor alle } \sigma \in G \text{ op eindig veel } \sigma \text{ na} \Big\}.$$

Twee elementen $\sum_\sigma a_\sigma \sigma$ en $\sum_\sigma b_\sigma \sigma$ zijn gelijk precies als $\forall \sigma \in G : a_\sigma = b_\sigma$.

De groepenring $k[G]$ is een ring met de volgende optelling en vermenigvuldiging:

$$\Big(\sum_\sigma a_\sigma\sigma\Big)+\Big(\sum_\sigma b_\sigma\sigma\Big)=\Big(\sum_\sigma (a_\sigma+b_\sigma)\sigma\Big),$$
$$\Big(\sum_\sigma a_\sigma\sigma\Big)\Big(\sum_\sigma b_\sigma\sigma\Big)=\Big(\sum_{\rho\in G}\sum_{\sigma,\tau\in G,\sigma\tau=\rho}(a_\sigma b_\tau)\rho\Big)=\Big(\sum_{\rho\in G}\sum_{\sigma\in G}(a_\sigma b_{\sigma^{-1}\rho})\rho\Big).$$

Merk op dat k bevat is in $k[G]$ als deelring ($x\in k\mapsto x\cdot 1\in k[G]$) en G in $k[G]^*$ als ondergroep ($g\in G\mapsto 1\cdot g\in k[G]$) als $k\neq\{0\}$.

Als we twee elementen $(\ldots+a\sigma+\ldots)$ en $(\ldots+b\tau+\ldots)$ van $k[G]$ vermenigvuldigen, volgt dat $(a\sigma)(b\tau)=(ab)(\sigma\tau)$, en dus dat $\sigma b=b\sigma$.

Het volgende lemma maakt het verband tussen $k[G]$-modulen en representaties van k over G expliciet.

Lemma 4.2. *Zij k een ring, G een groep en $k[G]$ de groepenring van G over k. Dan is een $k[G]$-moduul hetzelfde als een k-moduul V met een groepshomomorfisme $G\to \mathrm{Aut}_k(V)$.*

Voorbeeld
Zij k een lichaam en V het k-moduul k^n. Dan is $\mathrm{End}_k(V)=M(n,k)$ en $\mathrm{Aut}_k(V)=GL(n,k)$. Het geven van een $k[G]$-moduul structuur aan V is nu het geven van een homomorfisme $G\to GL(n,k)$.

Bewijs van lemma 4.2
Neem een k-moduul V en een groepshomomorfisme $\rho: G\to \mathrm{Aut}_k(V)$. Geef nu V een $k[G]$-moduulstructuur door

$$\begin{array}{rcl} k[G]\times V & \longrightarrow & V \\ \Big(\sum\limits_{\sigma\in G}^{<\infty} a_\sigma\sigma\Big)v & \longmapsto & \sum\limits_{\sigma\in G}^{<\infty} a_\sigma\rho(\sigma)(v)\end{array}$$

Ga zelf na dat deze afbeelding voldoet aan de axioma's voor een moduul.

Omgekeerd, neem een $k[G]$-moduul W. Maak hiervan een k-moduul V door de moduulafbeelding te beperken van $k[G]$ tot k. Definieer $\rho: G\to \mathrm{Aut}_k(V)$ door $\rho(\sigma)=(v\in V\mapsto \sigma v)$. □

We zullen nu voor twee kleine groepen G de structuur van $k[G]$ bekijken. Als $G=\{1\}$, is $k[G]=k$.

Zij G een groep van orde 2 ($G=\langle\sigma\rangle$ met $\sigma^2=1$) en k een ring. Beschouw het volgende ringhomomorfisme f:

$$\begin{array}{rcl} f: k[G] & \longrightarrow & k\times k \\ a+b\sigma & \mapsto & (a+b,a-b).\end{array}$$

De kern van f is $\{a+b\sigma\in k[G]: a=b=-b\}$. Dus als $a+b\sigma$ een element van de kern is, moet $2b=0$ gelden. Stel nu dat $2=1+1\in k^*$. Dan volgt $b=2^{-1}2b=0$, de kern van f is $\{0\}$ en f is dus injectief.

Precies als $(1,0)$ een element van het beeld van f is, is f surjectief. Immers, $(1,1)$ is $f(1)$ en $(1,1)$ en $(1,0)$ brengen samen $k \times k$ voort. Per definitie is $(1,0)$ een element van het beeld van f dan en slechts dan als er $a, b \in k$ bestaan met $a+b=1$ en $a-b=0$, dus als er een $a \in k$ bestaat met $2a=1$. Dit betekent dat f surjectief is dan en slechts dan als $2 \in k^*$.

Hieruit volgt dat f een ringisomorfisme is, dan en slechts dan als $2 \in k^*$.

Voorbeeld
Beschouw $\mathbb{Z}[G]$. $f(1)=(1,1)$ en $f(\sigma)=(1,-1)$. Dit betekent dat $(c,d) \in \mathbb{Z} \times \mathbb{Z}$ in het beeld van f zit dan en slechts dan als $c \equiv d (\mathrm{mod}\ 2)$.

Stel R_1 en R_2 zijn ringen, en zij $R = R_1 \times R_2$. Laat M_1 een R_1-moduul zijn, en M_2 een R_2-moduul. Dan is $M = M_1 \times M_2$ een R-moduul via $(r_1, r_2)(m_1, m_2) = (r_1 m_1, r_2 m_2)$. (Ga zelf na dat deze afbeelding aan de eisen voldoet.)

Omgekeerd wordt elk R-moduul N op een unieke manier zo verkregen. Definieer namelijk $M_1 = (1,0)N = \{(1,0)x : x \in N\}$. Dit is een deel-$R$-moduul van N. M_1 wordt geannihileerd door $\{0\} \times R_2$ want $(0,b)(1,0)x = (0,0)x = 0$. De afbeelding $\varphi : R \to \mathrm{End}(M_1)$ verkregen door het beeld van de moduulafbeelding $R \to \mathrm{End}(N)$ te beperken tot $\mathrm{End}(M_1)$ heeft dus $\{0\} \times R_2$ in zijn kern. De afbeelding φ induceert dus een afbeelding van $R/(\{0\} \times R_2) \cong R_1$ naar $\mathrm{End}(M_1)$. Dit maakt van M_1 een R_1-moduul. Definieer analoog het R_2-moduul $M_2 = (0,1)N$. Ga zelf na dat de afbeelding $M_1 \times M_2 \to N$ gegeven door $(u,v) \mapsto u+v$ een R-lineair isomorfisme is.

Als ook L_1 een R_1 moduul is, L_2 een R_2 moduul, en $L = L_1 \times L_2$, dan is er een afbeelding

$$\begin{array}{rcl} \mathrm{Hom}_{R_1}(M_1, L_1) \times \mathrm{Hom}_{R_2}(M_2, L_2) & \longrightarrow & \mathrm{Hom}_R(M, L) \\ (f_1, f_2) & \longmapsto & \big(f : (x,y) \mapsto (f_1(x), f_2(y))\big). \end{array}$$

Controleer zelf dat deze bijectief is.

Het bovenstaande is direct te generaliseren tot eindige producten $R = \prod_{i=1}^{n} R_i$ van ringen.

Laat nu k een lichaam van karakteristiek ongelijk aan 2 zijn, en G weer een groep van orde 2, $G = \langle \sigma \rangle$. Dan is $k[G] \xrightarrow{\sim} k \times k$ gegeven door $\sigma \mapsto (1,-1)$ een ringisomorfisme.

Stel nu dat V een $k[G]$-moduul is, dus een k-vectorruimte V met een een k-lineaire actie van G op V. Omdat elk $k[G]$-moduul V het product van een k-moduul V_1 waarop σ als 1 werkt en een k-moduul V_2 waarop σ als -1 werkt, is, hebben we het $k[G]$-lineaire isomorfisme $V \cong_{k[G]} V_1 \times V_2$, waarbij $\sigma(v_1, v_2) = (v_1, -v_2)$.

Als we dus een eindig-dimensionale representatie van G over k hebben, $\rho : G \to GL(n,k)$, dan kunnen we door basisverandering bewerkstelligen dat

$$\rho(\sigma) = \left(\begin{array}{ccc|ccc} 1 & & 0 & & & \\ & \ddots & & & 0 & \\ 0 & & 1 & & & \\ \hline & & & -1 & & 0 \\ & 0 & & & \ddots & \\ & & & 0 & & -1 \end{array}\right).$$

Algemener, als G een eindige cyclische groep is, $G = \langle\sigma\rangle$ met $\sigma^m = 1$, waarbij $m \neq 0$ in k en $X^m - 1$ verder m nulpunten in k heeft $(1, \zeta, \zeta^2, \ldots, \zeta^{m-1})$, dan hebben we het volgende isomorfisme:

$$\begin{array}{rcl} k[G] & \xrightarrow{\sim} & k \times k \times k \times \ldots \times k \\ \sigma & \longmapsto & (1, \zeta, \zeta^2, \ldots, \zeta^{m-1}). \end{array}$$

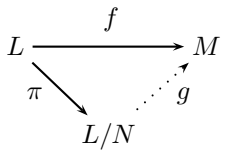
Na een basisverandering kunnen we dan $\rho(\sigma)$ schrijven als

$$\rho(\sigma) = \left(\begin{array}{c|c|c|c} \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} & & & \begin{matrix} & & \\ & 0 & \\ & & \end{matrix} \\ \hline & \begin{matrix} \zeta & & 0 \\ & \ddots & \\ 0 & & \zeta \end{matrix} & & \\ \hline & & \ddots & \\ \hline & & & \begin{matrix} \zeta^{m-1} & & 0 \\ & \ddots & \\ 0 & & \zeta^{m-1} \end{matrix} \\ \hline \begin{matrix} & & \\ & 0 & \\ & & \end{matrix} & & & \end{array}\right).$$

Stel R is een ring, en L en M zijn R-modulen. N heet een *deel-R-moduul* van M als N een ondergroep van M is en $\forall r \in R, x \in N : rx \in N$. Het quotient M/N is een R-moduul door als vermenigvulding $r(x + N) = (rx) + N$ te nemen. (Ga zelf na dat dit onafhankelijk van de gekozen representant x van een element van M/N is.)

Stelling 4.3 (Isomorfiestelling). *Stel $f : L \to M$ is R-lineair. Dan is $\ker f$ een deel-R-moduul van L en is het beeld fL een deel-R-moduul van M. De geïnduceerde afbeelding $L/\ker f \to fL$ is een isomorfisme van R-modulen.*

Stelling 4.4 (Homomorfiestelling). *Stel $f : L \to M$ is R-lineair en $N \subset L$ is een deel-R-moduul met $N \subset \ker f$. Dan is er een unieke R-lineaire afbeelding $g : L/N \to M$ zodat het volgende diagram commutatief is.*



Hier is π de canonieke afbeelding van L naar L/N.

Stelling 4.5. *Stel K, N zijn deel-R-modulen van M. Dan zijn $K \cap N$ en $K + N = \{x + y : x \in K, y \in N\}$ deel-R-modulen van M en de volgende afbeelding is een R-lineair isomorfisme:*

$$\begin{array}{rcl} K/(K \cup N) & \xrightarrow{\sim} & (K + N)/N \\ x + (K \cup N) & \longmapsto & x + N. \end{array}$$

5 Exacte rijen

Definitie 5.1. *Zij R een ring, en K, L en M drie R-modulen. Een rij*

$$K \xrightarrow{f} L \xrightarrow{g} M$$

heet exact *(bij L) als* $\ker g = \operatorname{im} f$.

Merk op dat hieruit volgt dat $gf = 0$.

Een rij $K \to L \to M \to N$ heet exact als de rij exact is bij L en bij M. In het algemeen heet een rij exact als hij exact is op welk punt waar dit gedefinieerd is.

Voorbeeld
$0 \xrightarrow{f} L \xrightarrow{g} M$ is exact $\Leftrightarrow \ker g = 0 \Leftrightarrow g$ is injectief.

$K \xrightarrow{f} L \xrightarrow{g} 0$ is exact $\Leftrightarrow \operatorname{im} f = L \Leftrightarrow f$ is surjectief.

$K \xrightarrow{f} 0 \xrightarrow{g} M$ is altijd exact.

$0 \xrightarrow{f} L \xrightarrow{g} 0$ is exact $\Leftrightarrow L = 0$.

$0 \longrightarrow L \xrightarrow{f} M \longrightarrow 0$ is exact $\Leftrightarrow f$ is een isomorfisme.

$0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$ is exact $\Leftrightarrow K$ kan (via f) opgevat worden als deelmoduul van L en M kan (van g) geïdentificeerd worden met L/K.

$0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \xrightarrow{h} N \longrightarrow 0$ is exact $\Leftrightarrow K$ is isomorf met $\ker g$ en N is isomorf met $\operatorname{coker} g$. ($\operatorname{coker} g = M/(\operatorname{im} g)$ is de *cokern* van g.)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & K \oplus M & \xrightarrow{p} & M & \longrightarrow & 0 \\ & & x & \longmapsto & (x,0) & & & & \\ & & & & (x,y) & \longmapsto & y & & \end{array} \qquad \text{is exact}$$

Definitie 5.2. *Een korte exacte rij* $0 \to K \to L \to M \to 0$ splitst *als er een homomorfisme $h : L \to K \oplus M$ is waarvoor het volgende diagram commutatief is:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & L & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_K} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle id_M} & & \\ 0 & \longrightarrow & K & \xrightarrow{i} & K \oplus M & \xrightarrow{p} & M & \longrightarrow & 0. \end{array}$$

Lemma 5.3 (Slangenlemma). *Stel het volgende diagram is commutatief en de twee rijen zijn exact:*

$$\begin{array}{ccccccccc} & & K_1 & \longrightarrow & L_1 & \longrightarrow & M_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & K_2 & \longrightarrow & L_2 & \longrightarrow & M_2. & & \end{array}$$

Dan bestaat er een rij afbeeldingen $\ker f \to \ker g \to \ker h \to \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h$ *en deze is exact.*

Als verder de afbeelding van $K_1 \to L_1$ injectief is, is die van $\ker f \to \ker g$ *dat ook. Als de afbeelding van $L_2 \to M_2$ surjectief is, is die van* $\operatorname{coker} g \to \operatorname{coker} h$ *dat ook.*

Zij I een indexverzameling, R een ring en M_i een R-moduul voor elke $i \in I$.

Dan is de *directe som*

$$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} : x_i \in M_i \text{ voor alle } i \in I, \{i \in I : x_i \neq 0\} \text{ is eindig}\}$$

en het *directe product*

$$\prod_{i \in I} M_i = \{(x_i)_{i \in I} : x_i \in M_i \text{ voor alle } i \in I\}.$$

De directe som is een deel-R-moduul van het directe product. Merk op dat $\bigoplus_{i \in I} M_i = \prod_{i \in I} M_i$ dan en slechts dan als $M_i = 0$ voor bijna alle $i \in I$. (Dit betekent: $M_i = 0$ op eindig veel gevallen na.)

Een directe som $\bigoplus_{i \in I} M$ wordt ook wel als $M^{(I)}$ geschreven en een direct product $\prod_{i \in I} M$ als M^I.

We zullen nu een aantal eigenschappen van modulen introduceren.

Definitie 5.4. *Een R-moduul F heet* vrij *als er een verzameling I is zodat $F \cong R^{(I)}$.*

Noem voor $j \in I$ het beeld van $(\ldots, 0, 1, 0, \ldots) \in R^{(I)}$, waar de 1 op de j-de plaats staat, onder dit isomorfisme e_j. De elementen e_j vormen dan een *basis* van F over R. Dat wil zeggen: voor elke $x \in F$ is er een unieke rij elementen $(r_j)_{j \in I}$, (met $r_j \in R$ en $r_j = 0$ voor bijna alle $j \in I$), zodanig dat $x = \sum_{i \in I} r_j e_j$.

Er geldt dat F een vrij R-moduul is dan en slechts dan als F een R-basis heeft.

Als R een *delingsring* is, dan is elk R-moduul vrij. (Een delingsring is een ring waarin $1 \neq 0$ en elke element ongelijk aan 0 een tweezijdige inverse heeft.)

Lemma 5.5. *Stel dat $0 \to K \to L \to F \to 0$ een korte exacte rij is, en F een vrij moduul. Dan splitst de rij.*

Definitie 5.6. *Zij M een R-moduul. Dan heet M* projectief *als elke korte exacte rij $0 \to K \to L \to M \to 0$ splitst.*

M heet injectief *als elke korte exacte rij $0 \to M \to N \to P \to 0$ splitst.*

M heet semi-simpel *als elke korte exacte rij $0 \to L \to M \to N \to 0$ splitst.*

Voorbeeld
Zij $R = \mathbb{Z}$. Dan is M projectief dan en slechts dan als M vrij is. M is injectief dan en slechts dan M deelbaar is. M is semi-simpel dan en slechts dan als elke $x \in M$ eindige, kwadraatvrije orde heeft.

Definitie 5.7. *Een R-moduul M heet* eindig voortgebracht *als er een surjectieve R-lineaire afbeelding $R^n \to M$ bestaat voor een $n \in \mathbb{Z}_{\geq 0}$.*

Een equivalente definitie is dat een R-moduul M eindig voortgebracht is als er $a_1, \ldots, a_n$ bestaan zodat $\forall x \in M \exists r_1, \ldots r_n \in R : x = r_1 a_1 + \ldots + r_n a_n$. (Merk dat op deze schrijfwijze *niet* uniek hoeft te zien. Als hij dat wel is, is M vrij.)

6 Homomorfismen en tensoren

Zij R een ring, en M en N twee R-modulen.

De R-lineaire afbeeldingen van M naar N vormen een abelse groep $\mathrm{Hom}_R(M, N)$ door $(f_1 + f_2)(x) = f_1(x) + f_2(x) \in N$. (Ga zelf na.)

$\mathrm{Hom}_R(M, N)$ is in het algemeen geen R-moduul. Immers, als f een R-lineaire afbeelding van M naar N is, is rf dat niet noodzakelijk. Namelijk, $(rf)(sx) = r(f(sx)) = rsf(x)$. Dit is niet altijd gelijk aan $s(rf(x)) = srf(x)$. Als R echter commutatief is, is $\mathrm{Hom}_R(M, N)$ wel een R-moduul.

Stel dat R, S en T ringen zijn, M een R-S-bimoduul en N een R-T-bimoduul. Dan is ${}_R\mathrm{Hom}(M, N)$ een S-T-bimoduul door $(sf)(x) = f(xs)$ en $(ft)(x) = f(x)t$. Controleer zelf dat dit aan de eisen voldoet.

Zij L een U-S-bimoduul. Op dezelfde manier is $\mathrm{Hom}_S(M, L)$ een U-R-bimoduul.

Stel dat $f : N \to N'$ een R-T-lineaire afbeelding is. Dan induceert f een S-T-lineaire afbeelding f_* gegeven door:

$$\begin{array}{rcl} {}_R\mathrm{Hom}(M, N) & \xrightarrow{f_*} & {}_R\mathrm{Hom}(M, N') \\ (M \xrightarrow{g} N) & \longmapsto & (M \xrightarrow{fg} N'). \end{array}$$

Merk op dat fg een samenstelling is van R-lineaire afbeeldingen, dus fg is ook R-lineair. We noemen de afbeelding f_* ook wel *de afbeelding geïnduceerd door* f of ${}_R\mathrm{Hom}(M, f)$.

Stel nu dat $h : M \to M'$ een R-S-lineaire afbeelding is. Dan induceert h een S-T-lineaire afbeelding h^* gegeven door:

$$\begin{array}{rcl} {}_R\mathrm{Hom}(M, N) & \xleftarrow{h^*} & {}_R\mathrm{Hom}(M', N) \\ (M \xrightarrow{gh} N) & \longmapsto & (M' \xrightarrow{g} N). \end{array} \tag{1}$$

We noemen de afbeelding h^* ook wel ${}_R\mathrm{Hom}(h, N)$.

Met de terminologie van de categorieëntheorie zeggen we: ${}_R\mathrm{Hom}(M, -)$ is *covariant* en ${}_R\mathrm{Hom}(-, N)$ is *contravariant*. Op de argumentplaatsen mogen modulen of afbeeldingen worden ingevuld.

Zij f en f' R-T-lineaire afbeeldingen zodat

$$N \xrightarrow{f} N' \xrightarrow{f'} N''.$$

Dan

$${}_R\,\mathrm{hom}(M, N) \xrightarrow{f_*} {}_R\mathrm{Hom}(M, N') \xrightarrow{f'_*} {}_R\mathrm{Hom}(M, N'')$$

en er geldt dat $f'_* f_* = (f'f)_*$.

Zij h en h' R-S-lineaire afbeeldingen zodat

$$M \xrightarrow{h} M' \xrightarrow{h'} M''.$$

Dan

$$_R\mathrm{Hom}(M,N) \xleftarrow{h^*} {}_R\mathrm{Hom}(M',N) \xleftarrow{h'^*} {}_R\mathrm{Hom}(M'',N)$$

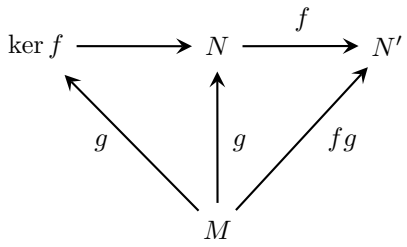
en er geldt dat $h^* h'^* = (h'h)^*$.

Dus $_R\mathrm{Hom}(M,N)$ is 'contra' in M en 'co' in N en is daarom een S-T-bimoduul. Ook geldt dus dat $_S\mathrm{Hom}(M,L)$ 'contra' is in M en 'co' in L. Daarom is $_S\mathrm{Hom}(M,L)$ een U-R-bimoduul.

Zij R een ring en M een R-moduul. We zullen laten zien: "$_R\mathrm{Hom}(M,-)$ transformeert kernen in kernen". Preciezer gezegd:

Lemma 6.1. *Als N en N' R-modulen zijn en de afbeelding $f : N \to N'$ R-lineair is, dan geldt dat $_R\mathrm{Hom}(M, \ker f) = \ker(_R\mathrm{Hom}(M,f)) = \ker f^*$.*

Bewijs. Ieder R-lineair homomorfisme g van M naar $\ker f$ is ook een R-lineair homomorfisme van M naar N, want $\ker f \subset N$. We hebben nu het volgende commutatieve diagram:



Er geldt: $g(M) \subset \ker f \Leftrightarrow fg = 0 \Leftrightarrow g \in \ker f_*$. Dus $_R\mathrm{Hom}(M, \ker f) = \ker f_*$. □

Men zegt: $_R\mathrm{Hom}(M,-)$ is *links-exact*, want als $0 \longrightarrow N''' \xrightarrow{f''} N \xrightarrow{f} N'$ exact is, dan is $0 \longrightarrow {}_R\mathrm{Hom}(M,N''') \xrightarrow{f''_*} {}_R\mathrm{Hom}(M,N) \xrightarrow{f_*} {}_R\mathrm{Hom}(M,N'')$ ook exact.

Verder geldt:

$$_R\mathrm{Hom}(M, N''' \oplus N') \cong {}_R\mathrm{Hom}(M,N''') \oplus {}_R\mathrm{Hom}(M,N').$$

De analoge bewering geldt ook voor $_R\mathrm{Hom}(-,N)$.

Omdat R zelf een R-R-bimoduul is, zijn zowel R als N links-R-modulen. Nu geldt dat de afbeelding

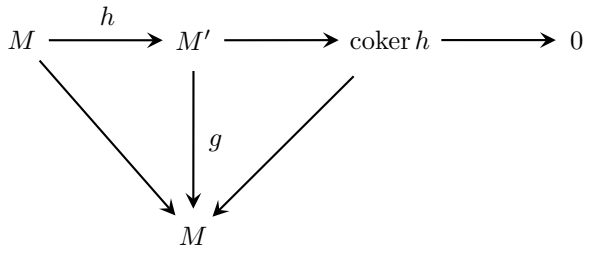
$$\begin{array}{rcl} {}_R\mathrm{Hom}(R,N) & {}_R\cong & N \\ f & \longmapsto & f(1) \end{array}$$

een R-isomorfisme is, omdat de afbeelding $N \to {}_R\mathrm{Hom}(R,N)$ gegeven door $x \mapsto (r \mapsto rx)$ de inverse is.

Zij R een ring en N een R-moduul. We gaan laten zien dat "${}_R\mathrm{Hom}(-,N)$ cokernen in cokernen transformeert". Dit maken we preciezer in het volgende lemma.

Lemma 6.2. *Als M en M' R-modulen zijn en de afbeelding $h : M \to M'$ R-lineair is, dan geldt dat ${}_R\mathrm{Hom}(\mathrm{coker}\, h, N) = \ker({}_R\mathrm{Hom}(h,N)) = \ker h^*$.*

Bewijs. Omdat $\mathrm{coker}\, h$ isomorf is met $M'/h(M)$, is de projectie-afbeelding een surjectieve afbeelding van M' naar $\mathrm{coker}\, h$. Laat nu $g : M' \to N$ een R-lineair homomorfisme zijn. Dan hebben we het volgende diagram:



Als nu g factoriseert via $\mathrm{coker}\, h$, d.w.z. dat het bovenstaande diagram commuteert, dan correspondeert g met een R-lineair homomorfisme $\mathrm{coker}\, h \to N$. Dit is equivalent met $gh = 0$, wat betekent dat $h^*(g) = 0$. □

Men zegt dat ${}_R\mathrm{Hom}(-,N)$ *links-exact* is, want als $M \xrightarrow{h} M' \xrightarrow{h'} M'' \to 0$ exact is, dan is $0 \to {}_R\mathrm{Hom}(M'',N) \xrightarrow{h'^*} {}_R\mathrm{Hom}(M',N) \xrightarrow{h^*} {}_R\mathrm{Hom}(M,N)$ ook exact.

Als we twee vrije R-modulen bekijken, zeg R^n en R^m, dan vinden we dat ${}_R\mathrm{Hom}(R^n,R^m)$ isomorf is met de verzameling van $m \times n$-matrices over R.

Zij S en T verzamelingen. De verzameling afbeeldingen van T naar S noteren we door $\mathrm{Afb}(T,S)$ of S^T of $\prod_{t\in T} S$. Deze notatie doet vermoeden dat $(S^T)^U = S^{T\times U}$, waarbij U ook een verzameling is. Dit is inderdaad het geval, want de afbeelding

$$\begin{array}{rcl} \mathrm{Afb}(T\times U, S) & \longrightarrow & \mathrm{Afb}(U, \mathrm{Afb}(T,S)) \\ f & \longmapsto & (u \mapsto (t \mapsto f(t,u))) \end{array}$$

is een bijectie.

Laat L, M en N abelse groepen zijn. We geven eerst een definitie.

Definitie 6.3. *Een afbeelding $f : L \times M \to N$ heet* bilineair *als $\forall x, x_1, x_2 \in L$: $\forall y, y_1, y_2 \in M$: $f(x, y_1 + y_2) = f(x,y_1) + f(x,y_2)$ en $f(x_1 + x_2, y) = f(x,y_1) + f(x,y_2)$.*

Er geldt:

$$\mathrm{Hom}(L, \mathrm{Hom}(M,N)) \subset \mathrm{Afb}(L, \mathrm{Hom}(M,N)) \subset \mathrm{Afb}(L, \mathrm{Afb}(M,N)) = \mathrm{Afb}(L\times M, N).$$

Als $f : L \times M \to N$ een afbeelding is, dan behoort het corresponderende element van $\mathrm{Afb}(L, \mathrm{Afb}(M,N))$ tot $\mathrm{Hom}(L, \mathrm{Hom}(M,N))$ dan en slechts dan als f bilineair is.

We noteren de verzameling van bilineaire afbeeldingen van $L \times M$ naar N door $\mathrm{Bil}(L \times M, N)$. De verzameling $\mathrm{Bil}(L \times M, N)$ is een groep. Er geldt dat:

$$\mathrm{Hom}(L, \mathrm{Hom}(M, N)) = \mathrm{Bil}(L \times M, N) = \mathrm{Hom}(L \otimes M, N);$$

we zullen spoedig zien wat $L \otimes M$ betekent.

Zij nu R een ring, L een rechts-R-moduul, M een links-R-moduul en N een abelse groep. We breiden de definitie van een bilineaire afbeeldingen uit tot R-bilineaire afbeeldingen.

Definitie 6.4. *Een afbeelding $f : L \times M \to N$ heet R-bilineair als ten eerste f bilineair is, en ten tweede $\forall r \in R : \forall x \in L : \forall y \in M : f(xr, y) = f(x, ry)$.*

Merk op dat $\mathbb{Z}$-bilineariteit hetzelfde is als bilineariteit.

Voorbeeld
De afbeelding $R \times R \to R$ gegeven door $(s, t) \mapsto st$ is R-bilineair.

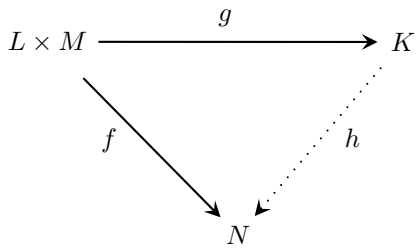
De afbeelding $R \times M \to M$ gegeven door $(s, m) \mapsto sm$ is R-bilineair.

De afbeelding $L \times R \to L$ gegeven door $(l, t) \mapsto lt$ is R-bilineair.

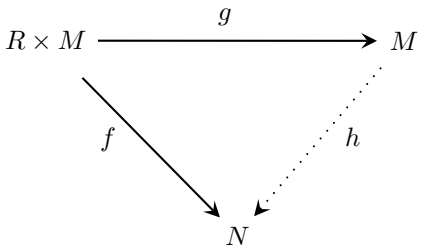
Definitie 6.5. *Zij K een abelse groep. Een R-bilineaire afbeelding $g : L \times M \to K$ heet* universeel *als voor elke abelse groep N de afbeelding*

$$\begin{array}{ccc} \mathrm{Hom}(K, N) & \longrightarrow & \mathrm{Bil}_R(L \times M, N) \\ h & \longmapsto & hg \end{array}$$

bijectief is. Met andere woorden: g heet universeel als voor elke abelse groep N en elke R-bilineaire afbeelding $f : L \times M \to N$ er een uniek groepshomomorfisme $h : K \to N$ is dat onderstaand diagram commutatief maakt.



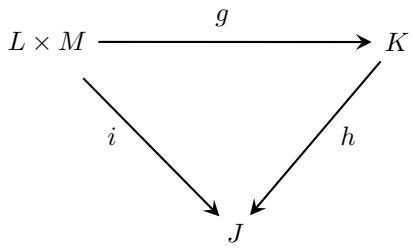
Voorbeeld
Alle drie de voorbeelden die we zojuist hebben gezien zijn universeel. We laten dit zien voor de afbeelding $R \times M \to M$ gegeven door $(s, m) \mapsto sm$. De vraag is of er een groepshomomorfisme $h : M \to N$ bestaat zodanig dat onderstaand diagram commutatief wordt.



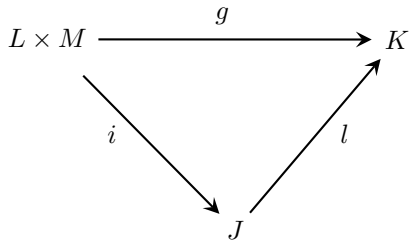
Als er een h is die voldoet, dan geldt voor deze h dat $f(s,m) = hg(s,m) = h(sm) = hg(1,sm) = f(1,sm)$. Dus als een dergelijk groepshomomorfisme h bestaat, dan is het gedefinieerd door $h(m) = f(1,m)$. De afbeelding die op deze manier gedefinieerd is, is inderdaad een groepshomomorfisme. Omdat $f(s,m) = f(1,sm) = h(sm)$ is nu g universeel.

Stelling 6.6. *Stel dat $g : L \times M \to K$ en $i : L \times M \to J$ R-bilineair en universeel zijn. Dan is er een uniek groepsisomorfisme $h : K \xrightarrow{\sim} J$.*

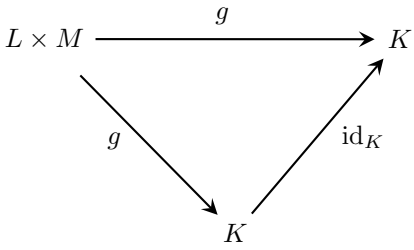
Bewijs. Vanwege de universaliteit van g bestaat er een groepshomomorfisme $h : K \to J$ dat onderstaand diagram commutatief maakt.



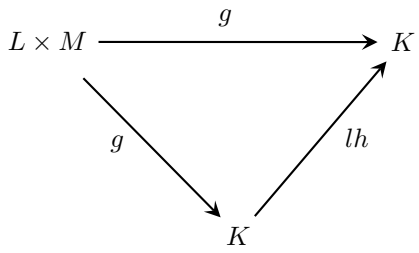
We moeten laten zien dat h bijectief is. Omdat ook i universeel is, bestaat er eveneens een groepshomomorfisme $l : J \to K$ dat het volgende diagram commutatief maakt:



We weten nu dat $i = hg$ en $g = li$. We willen laten zien dat $hl = \mathrm{id}_J$ en $lh = \mathrm{id}_K$. Daarom bekijken we het volgende commutatieve diagram:



Omdat $lhg = li = g$ commuteert ook het volgende diagram:



Uit de universaliteit van g volgt dat $lh = \mathrm{id}_K$. Op analoge wijze kunnen we bewijzen dat $hl = \mathrm{id}_J$. Dus l is de inverse van h, dus h is inderdaad een isomorfisme van K naar J. □

Definitie 6.7. *Als er een universele R-bilineaire afbeelding $g : L \times M \to K$ bestaat, dan definiëren we*

$$\begin{array}{rcl} L \otimes_R M & := & K \\ \cup & & \cup \\ x \otimes y & := & g(x,y). \end{array}$$

Merk op dat $(L \otimes_R M, - \otimes -)$ slechts op isomorfie na gedefinieerd zijn, als ze überhaupt gedefinieerd zijn.

Als zo'n paar K, g bestaat, dan is het op een uniek isomorfisme na uniek bepaald en dan schrijven we $L \otimes_R M$ in plaats van K en $x \otimes y$ in plaats van $g(x,y)$.

Voorbeeld
$R \otimes_R R \cong R$ met $x \otimes y \leftrightarrow xy$.

$R \otimes_R M \cong M$ met $r \otimes y \leftrightarrow ry$.

$L \otimes_R R \cong L$ met $x \otimes r \leftrightarrow xr$.

Het is zo dat "$\otimes$ met willekeurige directe sommen commuteert". Preciezer zien we dit in het volgende lemma.

Lemma 6.8. *Stel dat $(M_i)_{i \in I}$ een collectie R-modulen is en stel dat voor elke $i \in I$ het tensorproduct $L \otimes_R M_i$ bestaat. Dan bestaat ook $L \otimes_R (\bigoplus_{i \in I} M_i)$ en er geldt:*

$$\begin{array}{rcl} L \otimes_R (\bigoplus\limits_{i \in I} M_i) & \xrightarrow{\sim} & \bigoplus\limits_{i \in I} (L \otimes_R M_i) \\ x \otimes (y_i)_{i \in I} & \longmapsto & (x \otimes y_i)_{i \in I}. \end{array}$$

Bewijs. Controleer zelf dat de afbeelding

$$\begin{array}{rcl} L \times (\bigoplus\limits_{i \in I} M_i) & \longrightarrow & \bigoplus\limits_{i \in I} (L \otimes_R M_i) \\ (x, (y_i)_{i \in I}) & \longmapsto & (x \otimes y_i)_{i \in I} \end{array}$$

R-bilineair en universeel is. □

Stelling 6.9. *Als $L \otimes_R M$ bestaat, dan is hij voortgebracht door $\{x \otimes y | x \in L, y \in M\}$.*

Bewijs. Stel H is de ondergroep van $L \otimes_R M$ voortgebracht door $\{x \otimes y | x \in L, y \in M\}$.

Beschouw de canonieke projectie $\pi : L \otimes_R M \to (L \otimes_R M)/H$ en de nulafbeelding $0 : L \otimes_R M \to (L \otimes_R M)/H$. Dit zijn allebei groepshomomorfismen, en na samenstellen met $\otimes_R : L \times M \to L \otimes_R M$ vormen ze dezelfde bilineaire afbeelding $L \times M \to (L \otimes_R M)/H$, aangezien het beeld van $L \times M$ door π naar 0 gestuurd wordt. Uit universaliteit van $\otimes_R$ volgt nu dat $\pi = 0$, dus dat $H = L \otimes_R M$. □

Voorbeeld
Zij L een rechts-R-moduul. Dan hebben we:

$$\begin{array}{lll} L \otimes_R (R^n) & \cong (L \otimes_R R)^n \cong & L^n \\ x \otimes (r_i)_{i=1}^n & \longmapsto & (xr_i)_{i=1}^n. \end{array}$$

In het bijzonder geldt dus:

$$\begin{array}{rcl} (R^m) \otimes (R^n) & \cong & R^{mn} \\ (b_j)_{j=1}^m \otimes (a_i)_{i=1}^n & \longmapsto & (b_j a_i)_{1 \le i \le n, 1 \le j \le m}. \end{array}$$

Voorbeeld
Zij k een lichaam en V en W twee k-vectorruimten van eindige dimensie, zeg $V \cong k^m$ en $W \cong k^n$, met bases $\{e_1, \ldots, e_m\}$ en $\{f_1, \ldots, f_n\}$ respectievelijk. Dan is $V \otimes_k W$ een k- vectorruimte van dimensie mn met basis $(e_i \otimes f_j)_{1 \le i \le m, 1 \le j \le n}$.

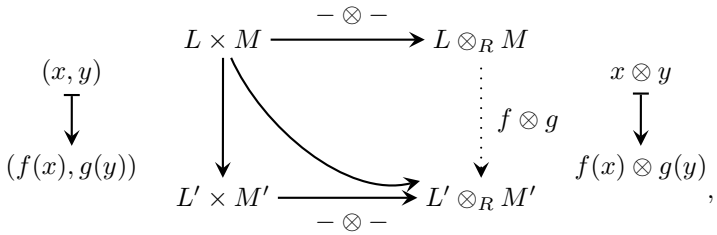
Zij R, S en T ringen. Zij L een S-R-bimoduul en M een R-T-bimoduul. Dan is $L \otimes_R M$ een S-T-bimoduul met $s(x \otimes y) = (sx) \otimes y$ en $(x \otimes y)t = x \otimes (yt)$.

Zij R een ring, L een rechts-R-moduul en M een links-R-moduul. Als R commutatief is, dan is $L \otimes_R M$ een R-moduul met $r(x \otimes y) = (rx) \otimes y = (xr) \otimes y = x \otimes (ry)$ en $(x \otimes y)r = x \otimes (yr)$, en $L \otimes_R M \cong M \otimes_R L$.

Zij R, S, T en U ringen en zij L een S-R-bimoduul, M een R-T-bimoduul en N een T-U-bimoduul. Dan geldt:

$$(L \otimes_R M) \otimes_T N_S \cong_U L \otimes_R (M \otimes_T N).$$

Stel dat $f : L \to L'$ een rechts-R-lineaire afbeelding is en $g : M \to M'$ een R-lineaire afbeelding. Dan commuteert het volgende diagram:



waarbij de afbeelding $L \times M \to L' \otimes_R M'$ via $L' \times M'$ bilineair is.

Als we nu bijvoorbeeld $L' = L$ nemen en voor $f : L \to L$ de identiteit id_L, dan vinden we de volgende afbeelding:

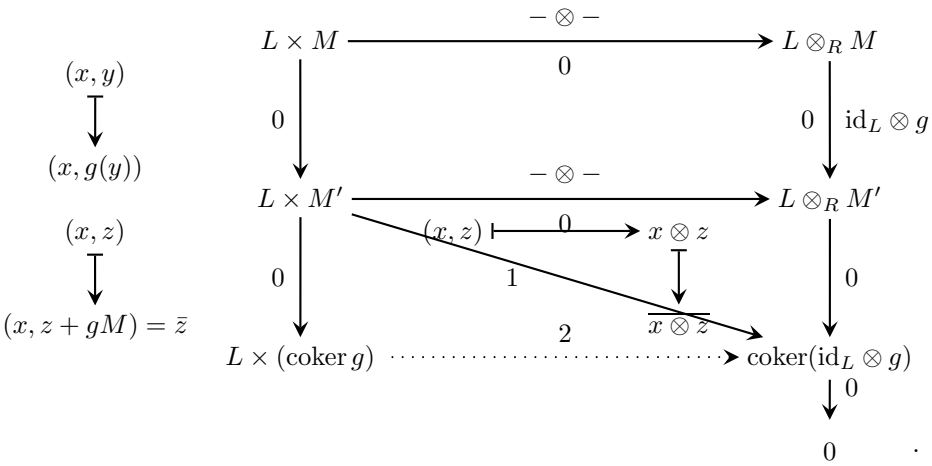
$$\begin{array}{rcl} L \otimes_R M & \xrightarrow{\mathrm{id}_L \otimes g} & L \otimes_R M' \\ x \otimes y & \longmapsto & x \otimes g(y). \end{array}$$

Er geldt: "$L \otimes_R -$ commuteert met cokernen". Preciezer zien we dat in de volgende stelling.

Stelling 6.10. *Als $g : M \to M'$ R-lineair is en $L \otimes_R M$ en $L \otimes_R M'$ allebei bestaan, dan bestaat ook $L \otimes_R (\operatorname{coker} g)$ en $L \otimes_R (\operatorname{coker} g) = \operatorname{coker}(\mathrm{id}_L \otimes g)$.*

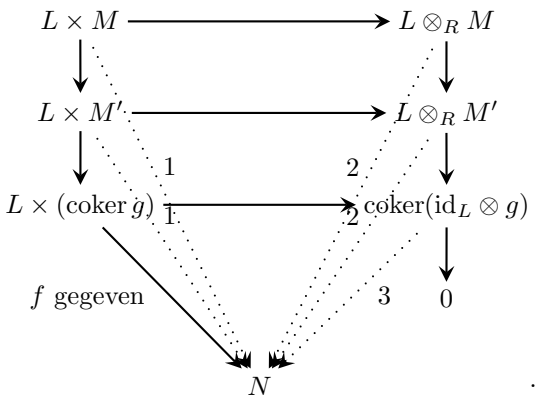
Anders gezegd: $L \otimes_R -$ is rechts-exact.

Bewijs. Diagrammenjagen! We hebben alle afbeeldingen waar een 0 bij staat al. De afbeelding met een 1 kunnen we eenvoudig maken door samenstelling. De afbeelding met een 2 ontstaat door $(x, \bar{z})$ af te beelden op $\overline{x \otimes z}$. Deze afbeelding is welgedefinieerd, want als $(x, \bar{z})$ en $(x, \overline{z'})$ dezelfde restklasse representeren, dan zijn $\overline{x \otimes z}$ en $\overline{x \otimes z'}$ gelijk, want $z' - z \in \operatorname{im} g$, dus $\overline{x \otimes (z' - z)} = 0$, want de rechterkolom is exact.



Zij N een abelse groep. Zij $f : L \times (\operatorname{coker} g) \to N$ gegeven. Dan zijn er bilineaire afbeeldingen $L \times M \to N$ en $L \times M' \to N$ die ontstaan door samenstelling (ze worden met 1 aangegeven in het diagram hieronder). De afbeelding $L \times M \to N$ die we op deze manier vinden is de nul-afbeelding, omdat de linkerkolom exact is in de tweede component.

Uit de universaliteit van deze twee afbeeldingen volgt dat er unieke afbeeldingen $L \otimes_R M \to N$ en $L \otimes_R M' \to N$ bestaan (deze worden met 2 aangegeven). Hieruit volgt dat er een afbeelding $\operatorname{coker}(\mathrm{id}_L \otimes g) \to N$ bestaat, want kies voor elk element van $\operatorname{coker}(\mathrm{id}_L \otimes g)$ een representant en beeldt die met de afbeelding $L \otimes_R M' \to N$ die we zojuist gevonden hebben af op N. Deze afbeelding is onafhankelijk van de keuze van de representant, want omdat de rechterkolom exact is, is $L \otimes_R M \to N$ de nul-afbeelding. Deze nieuwe afbeelding geven we aan met 3. Vanwege de uniciteit van de afbeelding $L \otimes_R M' \to N$ is ook de gevonden afbeelding 3 uniek.



Verder hebben we dat $L \otimes_R -$ rechts-exact is, want als $M \xrightarrow{g} M' \to M'' \to 0$ exact is, dan is $L \otimes_R M \to L \otimes_R M' \to L \otimes_R M'' \to 0$ ook exact. □

We hebben nog niet laten zien dat $L \otimes_R M$ bestaat. Dat doen we in de volgende stelling.

Stelling 6.11. *Het tensorproduct $L \otimes_R M$ bestaat.*

Bewijs. Kies een deelverzameling $S \subset M$ die M voortbrengt, d.w.z. een verzameling S waarvoor de R-lineaire afbeelding

$$\begin{aligned} R^{(S)} = \bigoplus_{s \in S} R &\longrightarrow M \\ (r_s)_{s \in S} &\longmapsto \sum_{s \in S} r_s s \end{aligned}$$

surjectief is. Kies een deelverzameling $T \subset \ker g$ die $\ker g$ voortbrengt, i.e. de analoge afbeelding $R^{(T)} \to \ker g$ is surjectief. Nu geldt dat $R^{(T)} \xrightarrow{h} R^{(S)} \to M = \operatorname{coker} h \to 0$ exact is. Zowel $L \otimes_R R^{(T)}$ als $L \otimes_R R^{(S)}$ bestaan, dus uit de vorige stelling volgt dat $L \otimes_R M$ bestaat. □

Voorbeeld
We laten zien dat $V_4 \otimes_{\mathbb{Z}} C_8 = V_4$. Het rijtje $\mathbb{Z} \xrightarrow{8} \mathbb{Z} \to C_8 \to 0$ is exact, dus

$$\begin{aligned} V_4 \otimes \mathbb{Z} &\xrightarrow{\mathrm{id}_{V_4} \otimes 8} V_4 \otimes \mathbb{Z} \longrightarrow V_4 \otimes C_8 \longrightarrow 0 \\ x \otimes y &\longmapsto 8(x \otimes y) \end{aligned}$$

is exact. We weten dat $V_4 \otimes \mathbb{Z} = V_4$ en dat $x \otimes y \mapsto 8(x \otimes y)$ de nulafbeelding is. Nu volgt dat $V_4 \otimes C_8 = V_4$.

Als we het tensorproduct nemen van V_4 met een andere abelse groep, krijgen we ook soms de triviale groep: $V_4 \otimes C_9 = 0$.

Definitie 6.12. *Een abelse groep G heet* deelbaar *als* $\forall x \in G, n \in \mathbb{Z} : \exists y \in G : ny = x$.

Definitie 6.13. *Een abelse groep heet* torsie *als* $\forall z \in G : \exists m \in \mathbb{Z} : mz = 0$.

Stelling 6.14. *Zij A een abelse groep die deelbaar is en B een abelse groep die torsie is, dan geldt $A \otimes_{\mathbb{Z}} B = 0$.*

Bewijs. Laat $x \in A, z \in B$ willekeurig gegeven. Kies $m \in \mathbb{Z}$ zodat $mz = 0$. Volgens de deelbaarheid van A bestaat er een $y \in A$ zodat $x = my$. Dan vinden we: $x \otimes z = (my) \otimes z = y \otimes (mz) = y \otimes 0 = 0$. □

Voorbeeld
$\mathbb{Q} \otimes C_{36} = 0$

$(\mathbb{Q}/\mathbb{Z}) \otimes (\mathbb{Q}/\mathbb{Z}) = 0$

$(\mathbb{Q}/\mathbb{Z}) \otimes (\mathbb{R}/\mathbb{Z}) = 0$

Zij L, M en N abelse groepen. Omdat $\mathrm{Hom}(L, \mathrm{Hom}(M, N))$ en $\mathrm{Hom}(L \otimes M, N)$ allebeid isomorf zijn met $\mathrm{Bil}(L \times M, N)$ geldt ook

$$\mathrm{Hom}(L, \mathrm{Hom}(M, N)) \cong \mathrm{Hom}(L \otimes M, N).$$

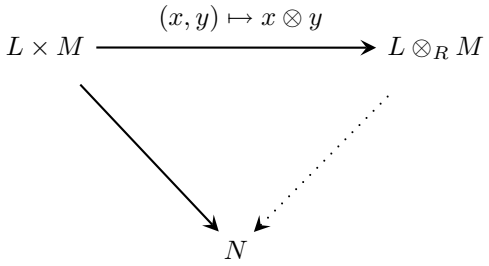
En we vinden:

$$\underbrace{{}_S\mathrm{Hom}(\underbrace{L}_{S-U}, \underbrace{{}_R\mathrm{Hom}(\underbrace{M}_{R-S}, \underbrace{N}_{R-T})}_{S-T})_U}_{U-T} \cong_T \underbrace{{}_R\mathrm{Hom}(\underbrace{\underbrace{M}_{R-S} \otimes_S \underbrace{L}_{S-U}}_{R-U}, \underbrace{N}_{R-T})}_{U-T} \tag{2}$$

en

$$\underbrace{\mathrm{Hom}(\underbrace{L}_{U-S}, \underbrace{\mathrm{Hom}_R(\underbrace{M}_{S-R}, \underbrace{N}_{T-R})}_{T-S})_T}_{T-U} \cong_U \underbrace{\mathrm{Hom}_R(\underbrace{\underbrace{L}_{U-S} \otimes_S \underbrace{M}_{S-R}}_{U-R}, \underbrace{N}_{T-R})}_{T-U}. \tag{3}$$

Zij R een ring, L een rechts-R-moduul en M een links-R-moduul. Dan hebben we het volgende commutatieve diagram:



Als M een R-T-bimoduul is en L een S-R-bimoduul, dan is $L \otimes_R M$ een S-T-bimoduul.

Zij nu k een lichaam en V en W k-vectorruimten met $\dim_k W = n < \infty$ en $\dim_k V = m < \infty$. Dan $\dim_k(V \otimes_k W) = nm$.

Zij R en R' twee ringen en $R \to R'$ een ringhomomorfisme. Zij M een R-moduul. Dan is $M' := \underbrace{R'}_{R'-R} \otimes_R \underbrace{M}_{R-\mathbb{Z}}$ een R'-moduul. We zeggen dat M' verkregen is uit M door *base extension*.

Als M vrij is over R, dan is M' ook vrij over R'.

Voorbeeld
Beschouw het ringhomomorfisme $\mathbb{R} \to \mathbb{C}$. Zij V een $\mathbb{R}$-vectorruimte die als $\mathbb{R}$-moduul isomorf is met $\mathbb{R}^n$. Zij $(e_i)_{i=1}^n$ een basis van V. Dan is $\mathbb{C} \otimes_{\mathbb{R}} V \cong \mathbb{C}^n$ als $\mathbb{C}$-moduul met basis $(1 \otimes e_i)_{i=1}^n$.

Lemma 6.15. *Zij nu $g_1 : R \to R_1$ en $g_2 : R \to R_2$ ringhomomorfismen zodat $g_1(R) \subset Z(R_1)$ en $g_2(R) \subset Z(R_2)$. Dan wordt $R_1 \otimes_R R_2$ een ring met $(s_1 \otimes s_2) \cdot (t_1 \otimes t_2) = (s_1 t_1) \otimes (s_2 t_2)$.*

Schets van het bewijs. We moeten nog laten zien dat we deze afbeelding inderdaad kunnen voortzetten. We moeten dus laten zien dat er inderdaad een afbeelding

$$(R_1 \otimes_R R_2) \times (R_1 \otimes_R R_2) \xrightarrow{\times} R_1 \otimes_R R_2$$

bestaat die

$$(s_1 \otimes s_2, t_1 \otimes t_2) \longmapsto (s_1 t_1) \otimes (s_2 t_2).$$

Stap 1. Definieer

$$\begin{array}{rcl} R_1 \times R_2 \times R_1 \times R_2 & \xrightarrow{f} & R_1 \otimes_R R_2 \\ (s_1, s_2, t_1, t_2) & \longmapsto & (s_1 t_1) \otimes (s_2 t_2). \end{array}$$

Stap 2. Controleer dat $\forall s_1 \in R_1 : \forall s_2 \in R_2$ de afbeelding

$$f(s_1, s_2, -, -) : R_1 \times R_2 \longrightarrow R_1 \otimes_R R_2$$

R-bilineair is. De universele eigenschap geeft dat er voor alle $(s_1, s_2) \in R_1 \times R_2$ een uniek homomorfisme

$$\begin{array}{rcl} h_{s_1,s_2} : R_1 \otimes_R R_2 & \longrightarrow & R_1 \otimes_R R_2 \\ t_1 \otimes t_2 & \longmapsto & (s_1 t_1) \otimes (s_2 t_2) \end{array}$$

bestaat.

Stap 3. Controleer dat de afbeelding

$$\begin{array}{rcl} R_1 \times R_2 & \longrightarrow & \mathrm{Hom}(R_1 \otimes_R R_2, R_1 \otimes_R R_2) \\ (s_1, s_2) & \longmapsto & h_{s_1,s_2} \end{array}$$

R-bilineair is. Dan krijg je

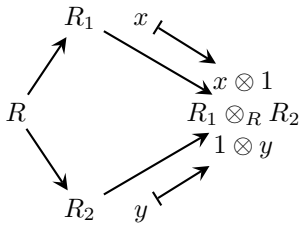
$$\begin{array}{rcl} g : R_1 \otimes_R R_2 & \longrightarrow & \mathrm{Hom}(R_1 \otimes_R R_2, R_1 \otimes_R R_2) \\ s_1 \otimes s_2 & \longmapsto & h_{s_1,s_2}. \end{array}$$

Stap 4. Definieer $\times$ door

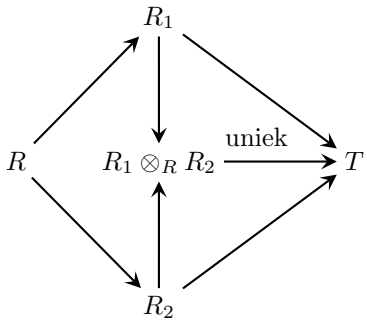
$$\times(a, b) = (g(a))(b).$$

□

We vinden het volgende commutatieve diagram van ringhomomorfismen.

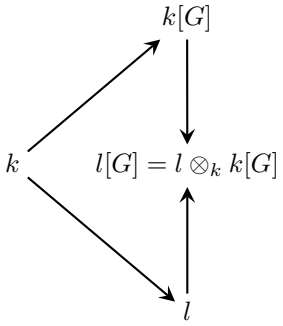


Zij nu R, R_1 en R_2 commutatieve ringen en $R \to R_1$ en $R \to R_2$ ringhomomorfismen. Zij T een ring en $R_1 \to T$ en $R_2 \to T$ ringhomomorfismen. Dan commuteert het volgende diagram.



Als $R \to R_1 \to T$ en $R \to R_2 \to T$ hetzelfde ringhomomorfisme $R \to T$ zijn, dan gaat het via het tensorproduct.

We kijken nu naar een geval dat relevant is voor de representatietheorie. Zij k een lichaam en l een uitbreidingslichaam van k. Voor R_1 nemen we de groepenring $k[G]$ en voor R_2 het uibreidingslichaam l. Dan commuteert het volgende diagram.



7 De Stelling van Jordan-Hölder en Grothendieck-groepen

De onderwerpen in deze paragraaf zijn relatief jong: ze stammen uit de negentiende en twintigste eeuw. De belangrijkste resultaten in deze paragraaf zijn gevonden door de volgende wiskundigen:

- Camille Jordan (1838–1921)
- Otto Hölder (1859–1937)
- Otto Schreier (1901–1929)
- Hans Zassenhaus (1912–1991)
- Alexander Grothendieck (1928)

Zij R een ring en M een R-moduul. We bekijken *ketens* in M.

Definitie 7.1. *Een* keten *in (of voor) M is een rij deelmodulen*

$$\{0\} = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_t = M,$$

waarbij $t \in \mathbb{Z}_{\geq 0}$. Het getal t heet nu de lengte *van de keten.*

Definitie 7.2. *Stel dat $(M_i)_{i=1}^t$ een keten voor M is, en $(N_j)_{j=1}^u$ voor N. Een* isomorfisme *van de eerste keten naar de tweede is een bijectie*

$$\rho : \{1, 2, \ldots, t\} \longrightarrow \{1, 2, \ldots, u\}$$

plus, voor elke $i \in \{1, 2, \ldots, t\}$ een R-isomorfisme

$$M_i/M_{i-1} \xrightarrow{\sim} N_{\rho(i)}/N_{\rho(i)-1}.$$

Het is duidelijk dat isomorfe ketens gelijke lengte moeten hebben.

Definitie 7.3. *Twee modulen M en N heten* Jordan-Hölder-isomorf *(of:* J.-H.-isomorf*), als ze isomorfe ketens hebben. Notatie: $M \cong_{JH} N$.*

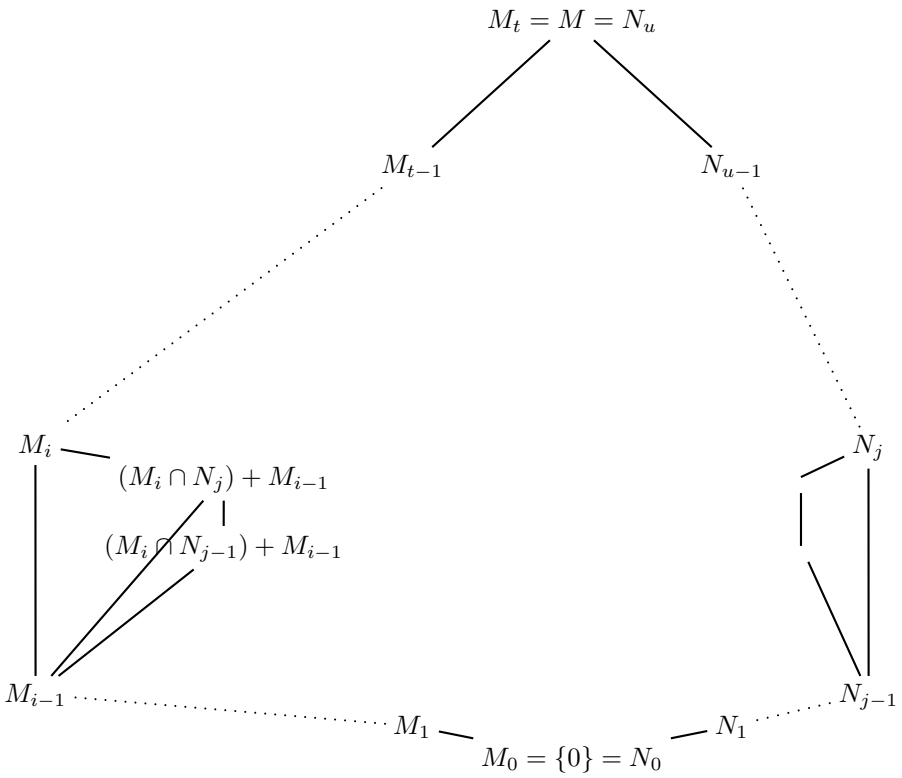
We kunnen ons nu afvragen of Jordan-Hölder-isomorfie een equivalentierelatie is. Het is eenvoudig in te zien dat Jordan-Hölder-isomorfie voldoet aan de eisen van symmetrie en reflexiviteit. De transitiviteit is het probleem. Stel namelijk dat een moduul M J.-H.-isomorf is met N en met L. Dat betekent dat er een keten voor M en een keten voor N bestaan die isomorf zijn, en ook bestaan er een keten voor M en een voor L die isomorf zijn. Maar omdat in deze beide gevallen de ketens voor M niet dezelfde hoeven te zijn, is het niet meteen duidelijk of ook N en L isomorfe ketens hebben.

Zij R een ring, M een R-moduul.

Definitie 7.4. *Een keten $(M_i)_{i=1}^t$ in M heet een* verfijning *van een keten $(M'_i)_{i=1}^{t'}$ in M als elk deelmoduul van M ten minste even vaak onder de M_i voorkomt als onder de M'_i.*

Stelling 7.5 (Verfijningsstelling van Schreier). *Elke twee ketens van M hebben isomorfe verfijningen.*

Bewijs. Stel dat we twee ketens in M hebben, zeg $(M_i)_{i=1}^t$ en $(N_j)_{j=1}^u$. Dan kunnen we de ketens op de volgende manier verfijnen (ga dit zelf na).

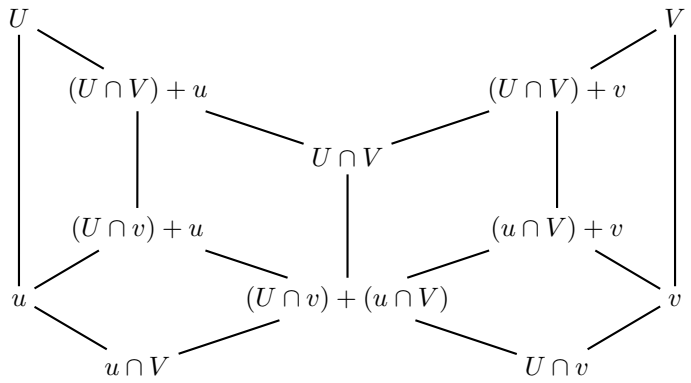


Beide ketens hebben *ut* stappen en ze zijn isomorf. Dat volgt uit het Vlinderlemma van Zassenhaus. □

Lemma 7.6 (Vlinderlemma van Zassenhaus). *Stel u, U, v en V zijn deelmodulen van M met $u \subset U$ en $v \subset V$. Dan geldt:*

$$((U \cap V) + u)/((U \cap v) + u) \cong_R ((U \cap V) + v)/((u \cap V) + v).$$

Bewijs. Het bewijs berust op het volgende diagram, dat het lemma ook zijn naam geeft.



De afbeelding $(U \cap V)/((U \cap v) + (u \cap V)) \to ((U \cap V) + u)/((U \cap v) + u)$ is een isomorfisme. De kern betsaat uit alle $x + y \in U \cap V$ met $x \in U \cap v$ en $y \in u \cap V$. Uit symmetrie-overwegingen volgt dat ook $(U \cap V)/((V \cap u) + (v \cap U)) \to ((U \cap V) + v)/((V \cap u) + v)$ een isomorfisme is. Hieruit volgt het lemma. □

In de context van groepen in plaats van modulen is de verfijningsstelling ook waar met kleine aanpassingen. We stellen dan als extra eis dat in een keten

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_t = G$$

iedere ondergroep G_{i-1} normaal moet zijn in G_i, en in de formulering van het Vlinderlemma moeten we eisen dat $u \subset U$ en $v \subset V$ ook normaal zijn. Het bewijs wordt in dit geval langer, omdat ook steeds de normaliteit bewezen dient te worden.

We kunnen nu antwoord geven op de vraag of Jordan-Hölder-isomorfie een equivalentierelatie is. Het antwoord is ja.

Lemma 7.7. *Jordan-Hölder-isomorfie is een equivalentierelatie.*

Bewijs. We hebben al gezien dat het alleen nodig is om te bewijzen dat Jordan-Hölder-isomorfie transitief is. Stel nu dat L en M J.-H.-isomorf zijn en dat de ketens $(M_i)_{i=1}^t$ in M en $(L_i)_{i=1}^t$ isomorf zijn. Stel dat M ook J.-H.-isomorf is met N en laat $(M'_j)_{j=1}^u$ in M en $(N_j)_{j=1}^u$ in N isomorfe ketens zijn. We gaan de twee ketens in M verfijnen op de manier van de Verfijningsstelling van Schreier. Iedere verfijning van de keten in M kunnen we gebruiken om de isomorfe keten te verfijnen, zodat de verfijning van $(M_i)_{i=1}^t$ isomorf blijft met de verfijning van $(L_i)_{i=1}^t$, en analoog voor M en N. Uiteindelijk vinden we een keten in M die een verfijning is van zowel $(M_i)_{i=1}^t$ als $(M'_j)_{j=1}^u$ en die isomorf is met een verfijning van $(L_i)_{i=1}^t$ en ook met een verfijning van $(N_j)_{j=1}^u$. Dus ook L en N zijn J.-H.-isomorf. □

Definitie 7.8. *Een moduul M heet* simpel *of* irreducibel *als het aantal deelmodulen van M precies twee is.*

Merk op dat dit betekent dat een simpel moduul M geen andere deelmodulen heeft dan 0 en M zelf, en dat M niet gelijk mag zijn aan 0.

Definitie 7.9. *Een keten $(M_i)_{i=1}^t$ van M heet een* compositieketen *als voor alle i met $1 \leq i \leq t$ het quotiënt M_i/M_{i-1} simpel is.*

Omdat een simpel moduul ongelijk aan 0 is, is een compositieketen alleen te verfijnen door deelmodulen te herhalen.

Definitie 7.10. *Een keten $(M_i)_{i=1}^t$ van M heet* echt *als $\forall i \in \{1, 2, \ldots, t\} : M_i \neq M_{i-1}$.*

Lemma 7.11. *Als $(M_i)_{i=1}^t$ en $(N_j)_{j=0}^u$ twee echte ketens van M zijn, dan hebben ze elk een verfijning zodanig dat*

1. *beide verfijningen isomorf zijn, en*
2. *elk van beide verfijningen óók een echte keten is.*

Bewijs. We kunnen beide ketens verfijnen op de manier van de Verfijningsstelling van Schreier. Dan vinden we twee isomorfe verfijningen

$$0 = M'_0 \subset M'_1 \subset \ldots \subset M'_s = M$$

en

$$0 = N'_0 \subset N'_1 \subset \ldots \subset N'_s = N.$$

Omdat de verfijningen isomorf zijn, komen in beide ketens alle quotiënten even vaak voor. Als we nu alle duplicaties verwijderen, houden we dus twee isomorfe ketens over die echt zijn. □

Lemma 7.12. *Zij $(M_i)_{i=1}^t$ een keten van M. Dan zijn equivalent:*

1. *$(M_1)_{i=1}^t$ is een compositieketen.*
2. *Voor alle $i \in \{1, 2, \ldots, t\}$ is M_i/M_{i-1} simpel.*
3. *De keten is echt, en de enige verfijning van de keten die ook echt is, is de keten zelf.*

Bewijs. Eerst bewijzen we $1 \Rightarrow 2 \Rightarrow 3$. Per definitie geldt $1 \Rightarrow 2$. Uit 1 is ook duidelijk dat de keten echt is. Stel nu dat er wel een verfijning bestaat die echt is, maar niet gelijk is aan de keten zelf. Dus stel dat voor een i een moduul M' bestaat met $M_{i-1} \subset M' \subset M_i$ zodat M' verschillend is van zowel M_{i-1} als M_i. Dan vinden we $0 \subset M'/M_{i-1} \subset M_i/M_{i-1}$, waarbij M'/M_{i-1} verschillend is van 0 en van M_i/M_{i-1}. Dit is in tegenspraak met het feit dat de quotiënten M_i/M_{i-1} allemaal simpel zijn.

De implicatie $3 \Rightarrow 1$ gaat hetzelfde, maar dan de andere kant op: als $(M_i)_{i=1}^t$ geen compositieketen is, bestaat er een quotient M_i/M_{i-1} dat niet simpel is, dus het heeft een echt deelmoduul M'/M_{i-1}. M' levert nu een verfijning van $(M_i)_{I=1}^t$ die echt is. □

Elke twee compositieketens van M zijn isomorf en hebben dus ook dezelfde lengte.

We bekijken nu de $\mathbb{Z}$-modulen, i.e. de abelse groepen.

Voorbeeld

$$0 \subset 30\mathbb{Z}/60\mathbb{Z} \subset 6\mathbb{Z}/60\mathbb{Z} \subset 2\mathbb{Z}/60\mathbb{Z} \subset \mathbb{Z}/60\mathbb{Z}$$

Alle simpele $\mathbb{Z}$-modulen zijn isomorf aan $\mathbb{Z}/p\mathbb{Z}$ voor een priemgetal p. De $\mathbb{Z}/p\mathbb{Z}$ zijn de enige simpele abelse groepen.

Stel A is een $\mathbb{Z}$-moduul. Dan zijn de volgende beweringen equivalent.

1. A heeft een compositieketen.
2. A is eindig.

Dit is als volgt in te zien. Het bestaan van een compositieketen

$$0 = A_0 \subset A_1 \subset \ldots \subset A_t = A$$

is equivalent met de simpliciteit van alle quotiënten A_i/A_{i-1}. Alle quotiënten zijn dus isomorf met $\mathbb{Z}/p\mathbb{Z}$ voor een priemgetal p, wat equivalent is met de bewering dat A eindig is.

Definitie 7.13. *We zeggen dat M* eindige lengte *heeft als M een compositieketen heeft.*

Nu zijn de volgende beweringen equivalent.

1. M heeft eindige lengte.
2. Er bestaat een geheel getal b zodanig dat elke echte keten van M lengte $\leq b$ heeft.

Dit is eenvoudig in te zien. Als elke echte keten van M lengte $\leq b$ heeft, dan stopt het verfijnen van $(M_i)_{i=1}^t$, dus vinden we een compositieketen. De andere implicatie volgt door voor b de lengte van een compositieketen te nemen.

Definitie 7.14. *Stel dat M een compositieketen heeft. Dan is de* lengte *van M gelijk aan t. Notatie:* $\text{length}(M)$ *of* $l(M)$.

Definitie 7.15. *Stel S is een simpel R-moduul en M is een R-moduul van eindige lengte, met compositieketen $(M_i)_{i=1}^{l(M)}$. Dan is de S-*lengte *van M gelijk aan $\#\{i : 0 < i \leq l(M), M_i/M_{i-1} \cong_R S\}$. Notatie: $l_S(M)$. We noemen S een* compositiefactor *van M als $l_S(M) \geq 1$.*

Het is duidelijk dat nu geldt:

$$l(M) = \sum_{S(\text{op isomorfie na})} l_S(M).$$

Voorbeeld
Beschouw het geval $R = \mathbb{Z}$. Dan zegt bovenstaande bewering dat als A een eindige abelse groep is, dan is $\#A = \prod_{p\text{priem}} p^{l_{\mathbb{Z}/p\mathbb{Z}}(A)}$. Anders gezegd: als

$$0 = A_0 \subset A_1 \subset \ldots \subset A_t = A$$

een compositieketen is, dan $\#A = \prod_{i=1}^t \#(A_i/A_{i-1})$.

Definitie 7.16. *Stel M is een R-moduul van eindige lengte, met compositieketen $(M_i)_{i=1}^{l(M)}$. 'De'* semi-simplificatie *van M is het R-moduul*

$$\bigoplus_{i=1}^{l(M)} (M_i/M_{i-1}).$$

De semi-simplificatie van M is onafhankelijk van de keuze van de compositieketen. We zullen zien dat de semi-simplificatie van M semi-simpel is, wat de naam doet vermoeden.

Zij R een ring.

Lemma 7.17. *Stel L en M zijn R-modulen en L is simpel. Dan is elk R-homomorfisme $f : L \to M$ òf nul òf injectief, en elk R-homomorfisme $g : M \to L$ is òf nul òf surjectief.*

Bewijs. $\ker f$ is een deelmoduul van L en daarom geldt dat $\ker f = L$ òf $\ker f = 0$. In het eerste geval geldt $f = 0$, in het tweede geval geldt dat f injectief is.

$g(M)$ is een submoduul van L, dus $g(M) = 0$ òf $g(M) = L$. In het eerste geval geldt $g = 0$, in het tweede geval geldt dat g surjectief is. □

Gevolgen:

1. Als L en L' simpel zijn, dan is elke R-lineaire afbeelding $L \to L'$ òf nul òf een isomorfisme.
2. Als L simpel is, dan is $\mathrm{End}_R(L)$ een delingsring ("Schur's lemma"). Bijvoorbeeld: als $L = \mathbb{Z}/p\mathbb{Z}$, dan is $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{F}_p$.
3. Als L en L' twee niet-isomorfe simpele R-modulen zijn, dan $\mathrm{Hom}_R(L, L') = 0$.

Definitie 7.18. *Als R een commutatieve ring is, dan is een* maximaal ideaal *van R een ideaal $\mathfrak{m} \subset R$ van R zodanig dat $\#\{I : I \text{ ideaal van } R, \mathfrak{m} \subset I \subset R\} = 2$. Een equivalente definitie is: een ideaal $\mathfrak{m} \subset R$ is maximaal dan en slechts dan als $R/\mathfrak{m}$ simpel is.*

Uit het lemma van Zorn volgt dat elke commutatieve ring die niet gelijk aan 0 is een maximaal ideaal heeft. Hiervoor is het belangrijk dat $1 \in R$.

Als een simpel moduul L over een commutatieve ring R isomorf is met $R/\mathfrak{m}$, dan

$$\begin{array}{rccc} \mathfrak{m} = \ker(R & \overset{\text{ringhomomorfisme}}{\longrightarrow} & \mathrm{End}_{\mathbb{Z}}(L)) \\ (r & \longmapsto & (x \mapsto rx)). \end{array}$$

Dus: $R/\mathfrak{m} \cong_R R/\mathfrak{m}' \Rightarrow \mathfrak{m} = \mathfrak{m}'$.

Zij R een ring, niet per se commutatief.

Definitie 7.19. *Een linksideaal I van R heet een* maximaal linksideaal *als $\#\{J : J \text{ is een linksideaal van } R, I \subset J \subset R\} = 2$. Een equivalente definitie is: een linksideaal I van R is maximaal dan en slechts dan als R/I simpel is als R-moduul.*

Uit het lemma van Zorn volgt dat elke ring die niet gelijk aan 0 is een maximaal linksideaal heeft.

Stelling 7.20. *Elk simpel R-moduul is van de vorm R/I met I een maximaal linksideaal.*

Bewijs. Stel L is simpel. Kies nu $x \in L$ ongelijk aan 0. Beeld R als volgt op L af:

$$\begin{array}{rcl} g : R & \longrightarrow & L \\ r & \longmapsto & rx. \end{array}$$

Dan is g R-lineair en $g \neq 0$. Nu volgt dus uit lemma 7.17 dat g surjectief is. Dus $L \cong_R R/\ker g$, waarbij $\ker g$ een maximaal linksideaal is, want $R/\ker g$ is simpel. $\square$

Zij k een lichaam en n een geheel getal groter dan 1. We nemen $R = M(n,k) = \{n \times n - \text{matrices met coëfficiënten in } k\}$ en $L = k^n$, waarbij we k^n opvatten als de verzameling kolomvectoren van n elementen uit k. Dan is L een R-moduul met $A \cdot v \in L$ voor $A \in R$ en $v \in L$. (Ga na.)

Nu geldt dat L simpel is. Dat kunnen we als volgt laten zien. Stel dat M een deelmoduul verschillend van 0 en L is zodat $0 \subset M \subset L$. Zij v een element van M dat ongelijk is aan 0. Uit de lineaire algebra is bekend dat als $v, w \in k^n$ met $v \neq 0$, dan is er een lineaire transformatie $k^n \to k^n$ met $v \mapsto w$. Dus $\forall w \in L : \exists A \in R : Av = w$. Dus $Rv = L$, dus $M = L$.

We zoeken nu een maximaal linksideaal $I \subset M(n,k) = R$ met $R/I \cong_R L$. Kies

$$x = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in L = k^n.$$

Dan kunnen we nemen:

$$\begin{aligned} I &= \left\{ A \in R : A \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} 0 & * & * & * & * \\ 0 & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & * & * & * & * \end{pmatrix} \in R \right\}. \end{aligned}$$

Door verschillende vectoren voor x te kiezen (neem ook

$$x = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ of } \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ etc.)}$$

vinden we n linksidealen I zodat $R/I \cong_R L$.

Zij R een ring en M een R-moduul.

Stelling 7.21. *Als M van eindige lengte is, dan is M eindig voortgebracht.*

Bewijs. Het bewijs gaat met inductie naar $l(M)$. Als $l(M) = 0$, dan M is 0 en we zijn klaar. Als $l(M) = t > 0$, neem dan een compositieketen $0 = M_0 \subset M_1 \subset \ldots \subset M_t = M$. Volgens de inductiehypothese is M_{t-1} eindig voortgebracht. Het quotiënt M_t/M_{t-1} is simpel, dus M_t/M_{t-1} is isomorf met $R/(\text{maximaal linksideaal})$, voortgebracht door een enkel element $x + M_{t-1}$. Dan wordt M dus voortgebracht door M_{t-1} samen met x. Dus M is eindig voortgebracht. $\square$

We zien dat het aantal voortbrengers begrensd wordt door $l(M)$.

Stelling 7.22. *Stel M is een R-moduul en $N \subset M$ is een deelmoduul. Dan zijn equivalent:*

1. *M is van eindige lengte.*
2. *N en N/M zijn beide van eindige lengte.*

(Met andere woorden: voor een kort exact rijtje $0 \to N \to M \to L \to 0$ geldt: M van eindige lengte $\Leftrightarrow$ N en L van eindige lengte.) Verder impliceren de bovenstaande beweringen dat $l(M) = l(N) + l(M/N)$ en dat voor alle simpele R-modulen S geldt dat $l_S(M) = l_S(N) + l_S(M/N)$.

Bewijs. 1 $\Rightarrow$ 2: We hebben $0 \subset N \subset M$. Als N echte ketens van willekeurige lengte heeft, dan heeft M dat ook. Door bovenstaande keten uit te delen naar N vinden we $0 \subset M/N$, waarbij N op 0 wordt afgebeeld en M surjectief naar M/N afbeeldt. Dus als M/N echte ketens van willekeurige lengte heeft, dan heeft M dat ook.

2 $\Rightarrow$ 1 en de laatste implicatie: Zij $0 = N_0 \subset N_1 \subset \ldots \subset N_u = N$ en $0 = L_0 \subset L_1 \subset \ldots \subset L_v = M/N$ compositieketens. Zij f de projectie-afbeelding $M \to M/N$, die uiteraard surjectief is. Dan is $0 = N_0 \subset N_1 \subset \ldots \subset N_u = N = f^{-1}L_0 \subset f^{-1}L_1 \subset f^{-1}L_v = M$ een compositieketen voor M. Dus $l(M) = u + v = l(N) + l(M/N)$. Omdat alle quotiënten onveranderd gebleven zijn, geldt ook $l_S(M) = l_S(N) + l_S(M/N)$. □

8 Additieve invarianten

Stel R is een ring en $\mathcal{C}$ is een klasse R-modulen met $0 \in \mathcal{C}$.

Voorbeeld
$\mathcal{C} = \{\text{alle } R\text{-modulen}\}$

$\mathcal{C} = \{\text{alle eindig voortgebrachte } R\text{-modulen}\}$

$\mathcal{C} = \{\text{alle } R\text{-modulen van eindige lengte}\}$

Definitie 8.1. *Zij A een additief geschreven abelse groep. Een functie $f : \mathcal{C} \to A$ heet* additief *als voor elke exacte rij $0 \to N \to M \to L \to 0$ met L, M, $N \in \mathcal{C}$ geldt dat $f(M) = f(N) + f(L)$. We noemen f ook wel een* additieve invariant.

Als we in de definitie $N = M = L = 0$ nemen, vinden we dat voor een additieve invariant f geldt dat $f(0) = 0$. Als we $L = 0$ nemen, vinden we dat $N \cong M \Rightarrow f(M) = f(N)$.

Voorbeeld
$R = \mathbb{Z}$, $\mathcal{C} = \{\text{eindige abelse groepen}\}$, $A = \mathbb{Q}^*_{>0}$, $f(M) = \#M$.

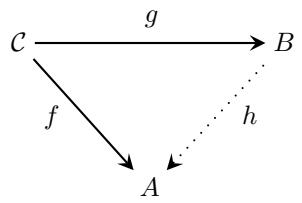
We noteren de verzameling additieve afbeeldingen $\mathcal{C} \to A$ als $\mathrm{Add}(\mathcal{C}, A)$.

Definitie 8.2. *Zij B een abelse groep. Een afbeelding $g : \mathcal{C} \to B$ heet* universeel additief *als g additief is en voor elke abelse groep A de afbeelding*

$$\begin{array}{ccc} \mathrm{Hom}(B, A) & \longrightarrow & \mathrm{Add}(\mathcal{C}, A) \\ h & \longmapsto & hg \end{array}$$

een bijectie is.

Met andere woorden: g heet universeel additief als g additief is en er voor elke abelse groep A en elke additieve afbeelding $f : \mathcal{C} \to A$ een uniek groepshomomorfisme $h : B \to A$ bestaat dat onderstaand diagram commutatief maakt.



Constructie van een universele additieve afbeelding voor gegeven R en $\mathcal{C}$:
$K(\mathcal{C}) = \mathbb{Z}^{(\mathcal{C})}/H$ met $\mathbb{Z}^{(\mathcal{C})} = \{(n_M)_{M\in\mathcal{C}} : n_M \in \mathbb{Z}, \#\{M : n_M \neq 0\} < \infty\}$. Voor $M \in \mathcal{C}$ definiëren we een vector $e_M \in \mathbb{Z}^{(\mathcal{C})}$ als volgt: e_M heeft een 1 in positie M en een 0 in alle andere posities. De e_M zijn basisvectoren voor $\mathbb{Z}^{(\mathcal{C})}$. We kunnen ook schrijven: $(n_M)_{M\in\mathcal{C}} = \sum_M^{<\infty} n_M e_M$. Voor H nemen we de ondergroep voortgebracht door $\{e_M - e_L - e_N : 0 \to L \to M \to N \to 0$ is een exacte rij in $\mathcal{C}\}$. In $\mathbb{Z}^{(\mathcal{C})}/H$ geldt $\overline{e_M} = \overline{e_L} + \overline{e_N}$.

Definitie 8.3. *De groep $K(\mathcal{C})$ die we hierboven geconstrueerd hebben heet de* Grothendieck groep *van $\mathcal{C}$.*

Notatie: voor $M \in \mathcal{C}$ is $[M]$ het element $\overline{e_M}$ van $K(\mathcal{C})$.

Definitie 8.4. *We noemen een element van $K(\mathcal{C})$* effectief *als het van de vorm $[M]$, $M \in \mathcal{C}$ is. Andere elementen heten* virtueel.

Stelling 8.5. *De afbeelding $\mathcal{C} \xrightarrow{[\,]} K(\mathcal{C})$ is universeel additief.*

Bewijs. Zij A een abelse groep. Merk op dat $\mathrm{Hom}(\mathbb{Z}^{(\mathcal{C})}, A) = \{$alle afbeeldingen $\mathcal{C} \to A\}$. Daarom geldt:

$$\begin{array}{rcl} \mathrm{Hom}(K(\mathcal{C}), A) & = & \mathrm{Hom}(\mathbb{Z}^{(\mathcal{C})}/H, A) \cong \{j \in \mathrm{Hom}(\mathbb{Z}^{(\mathcal{C})}, A) : j|_H = 0\} \\ & \cong & \{f : \mathcal{C} \to A : \forall 0 \to N \to M \to L \to 0 : f(M) = f(L) = f(N)\} \\ & = & \mathrm{Add}(\mathcal{C}, A). \end{array}$$

□

Lemma 8.6. *Als $\mathcal{C}$ gesloten is onder $\oplus$, dan is elk element van $K(\mathcal{C})$ van de vorm $[M] - [M']$ met $M, M' \in \mathcal{C}$.*

Bewijs. Het is duidelijk dat $\{[M] : M \in \mathcal{C}\}$ de groep $K(\mathcal{C})$ voortbrengt. Er geldt voor $M, M', N, N' \in \mathcal{C}$: $([M]-[M'])-([N]-[N']) = [M]+[N']-([M']+[N]) = [M\oplus$

$N'] - [M' \oplus N]$, want $0 \to M \to M \oplus N' \to N' \to 0$ en $0 \to M' \to M' \oplus N \to N \to 0$ zijn exact. Daarom is de deelverzameling $\{[M] - [M'] : M, M' \in \mathcal{C}\}$ een ondergroep van $K(\mathcal{C})$ die alle voortbrengers bevat, dus $\{[M] - [M'] : M, M' \in \mathcal{C}\} = K(\mathcal{C})$. □

Voorbeeld
Zij R een ring.

1. Zij $\mathcal{C} = \{\text{alle } R\text{-modulen}\}$, dan $K(\mathcal{C}) = 0$.

   Bewijs. Beschouw de volgende exacte rij:

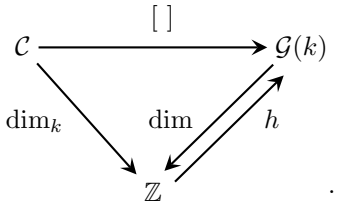
   $$0 \to M \xrightarrow{f} \bigoplus_{i=0}^{\infty} M \xrightarrow{g} \bigoplus_{i=0}^{\infty} M \to 0,$$

   met $f(x) = (x, 0, \ldots, 0)$ en $g(x_0, x_1, x_2, \ldots) = (x_1, x_2, \ldots)$. Dan $[\bigoplus_{i=0}^{\infty} M] = [M] + [\bigoplus_{i=0}^{\infty} M]$, dus $[M] = 0$. □

2. Zij $\mathcal{C} = \{\text{eindig voortgebrachte } R\text{-modulen}\}$. Notatie: $K(\mathcal{C}) = \mathcal{G}(R) = \mathcal{G}_{\text{fg}}(R)$.

   Stelling 8.7. *Als k een lichaam is, dan* $\dim : \mathcal{G}(k) \xrightarrow{\sim} \mathbb{Z}$ *is een isomorfisme.*

   Bewijs. Zij $\mathcal{C} = \{\text{eindig voortgebrachte } k\text{-modulen}\} = \{k\text{-vectorruimten van eindige dimensie}\}$. Dan hebben we het volgende diagram:

   .

   De afbeelding $\dim : \mathcal{G}(k) \to \mathbb{Z}$ bestaat en is uniek vanwege de universaliteit van $[\ ]$ (dat hebben we gezien in stelling 8.5). Deze afbeelding is gegeven door $[M] \longmapsto \dim_k(M)$. Dit is welgedefinieerd, want $M \cong N \Leftrightarrow \dim_k(M) = \dim_k(N)$. Deze afbeelding dim is bijectief, want we laten zien dat $n \mapsto n[k]$ de inverse van dim is. Er geldt dat $[k^a] + [k^b] = [k^{a+b}]$, dus met inductie vinden we dat $n[k] = [k^n]$. Zij nu $M \in \mathcal{C}$, met $\dim_k(M) = n$. Merk op dat $M \cong k^n$, dus geldt $[M] = [k^n]$. Nu geldt: $n \overset{h}{\longmapsto} n[k] = [k^n] = [M] \overset{\dim}{\longmapsto} n$ en $[M] \overset{\dim}{\longmapsto} \dim_k(M) = n \overset{h}{\longmapsto} [k^n] = [M]$. □

   Ook geldt: $\mathcal{G}(\mathbb{Z}) \cong \mathbb{Z}$.

   Bewijs. Iedere eindige abelse groep is isomorf met het product van cyclische groepen: $\bigoplus_{i=1}^{r} (\mathbb{Z}/n_i\mathbb{Z})$, met $n_i \in \mathbb{Z}_{\geq 0}$.

   Voor $n \in \mathbb{Z}_{>0}$ hebben we het exacte rijtje $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$. Hieruit volgt dat $[\mathbb{Z}/n\mathbb{Z}] = 0$. We hebben nu het volgende isomorfisme:

   $$[M] = \left[\bigoplus_{i=1}^{r} (\mathbb{Z}/n_i\mathbb{Z})\right] \longmapsto \#\{i : 1 \leq i \leq r, n_i = 0\} = \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} M).$$

   □

3. Zij $\mathcal{C} = \{$alle R-modulen van eindige lengte$\}$. We schrijven $K(\mathcal{C})$ dan ook wel als $\mathcal{G}_{\mathrm{fl}}(R)$. ('fl' staat voor 'finite length'.)

Stelling 8.8. *Er is een groepsisomorfisme*

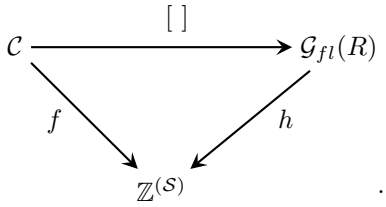
$$\begin{array}{rcl} \mathcal{G}_{fl}(R) & \xrightarrow{\sim} & \mathbb{Z}^{(\mathcal{S})} \\ [M] & \longmapsto & (l_S(M))_{S\in\mathcal{S}}, \end{array}$$

waarbij $\mathcal{S} = \{$*simpele* R*-modulen*$\}/\cong_R$.

Bewijs. Omdat $\forall S \in \mathcal{S} : l_S(M) = l_S(N) + l_S(L)$ als $0 \to L \to M \to N \to 0$ exact is, is

$$\begin{array}{rcl} f : \mathcal{C} & \longrightarrow & \mathbb{Z} \\ M & \longmapsto & (l_S(M))_{S\in\mathcal{S}} \end{array}$$

een additieve invariant. De universele eigenschap van $\mathcal{G}_{fl}(R)$ geeft nu een afbeelding $h : \mathcal{G}_{fl}(R) \to \mathbb{Z}^{(\mathcal{S})}$ en het volgende commutatieve diagram:



.

We zullen laten zien dat de afbeelding

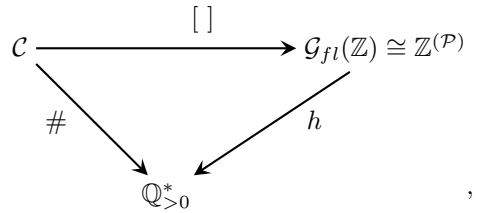
$$\begin{array}{rcl} j : \mathbb{Z}^{(\mathcal{S})} & \longrightarrow & \mathcal{G}_{fl}(R) \\ (n_S)_{S\in\mathcal{S}} & \longmapsto & \displaystyle\sum_{S\in\mathcal{S}} (n_S[S]) \end{array}$$

de inverse van h is. Ten eerste is j een rechtsinverse omdat geldt $hj[e_S] = h([S]) = e_S$. Andersom geldt $jh([M]) = j(\sum_{S\in\mathcal{S}} l_S(M)e_S) = \sum_{S\in\mathcal{S}} l_S(M)[S] = \sum_{i=1}^{t}[M_i/M_{i-1}]$, als $0 = M_0 \subset M_1 \subset \ldots \subset M_t = M$ een compositieketen van M is.

Voor $1 \le u \le t$ is de rij $0 \to M_{u-1} \to M_u \to M_u/M_{u-1} \to 0$ exact, dus geldt dat $[M_u] = [M_{u-1}] + [M_u/M_{u-1}]$. Met inductie naar u volgt nu dat $\sum_{i=1}^{t}[M_i/M_{i-1}] = [M]$, wat bewijst dat j een linksinverse van h is. □

Merk op dat onder dit isomorfisme de deelverzameling van *effectieve* elementen van $\mathcal{G}_{fl}(R)$ als beeld $\mathbb{Z}_{\ge 0}^{(\mathcal{S})}$ heeft.

Voorbeeld: $R = \mathbb{Z}$, $\mathcal{C} = \{$eindige abelse groepen$\}$. Zij $\mathcal{P}$ de verzameling priemgetallen $\{2, 3, 5, \ldots\}$. Dan hebben we het volgende commutatieve diagram:



,

waarin h, gegeven door $(n_p)_{p\in\mathcal{P}} \mapsto \prod_{p\in\mathcal{P}} p^{n_p}$, een isomorfisme is, volgens de eenduidige priemfactorontbinding.

Definitie 8.9. *Zij M een R-moduul van eindige lengte, met compositieketen $0 = M_0 \subset M_1 \subset \ldots \subset M_t = M$. Dan wordt de* semi-simplificatie M_{ss} *van M gegeven door $\bigoplus_{i=1}^{t} M_i/M_{i-1}$.*

Gevolg 8.10. *Stel M, N zijn R-modulen van eindige lengte. Dan geldt:*

$$\begin{aligned} [M] = [N] &\Leftrightarrow M \text{ en } N \text{ hebben isomorfe compositieketens} \\ &\Leftrightarrow M \cong_{JH} N \\ &\Leftrightarrow M_{\text{ss}} \cong N_{\text{ss}}. \end{aligned}$$

Voorbeeld
Zij $G = \langle\sigma\rangle$ met $\#G = 2$ en k een lichaam van karakteristiek ongelijk aan 2. We hebben eerder gezien dat elk $k[G]$-moduul V van de vorm $V_+ \oplus V_-$ is, waarbij V_+ en V_- beide k-vectorruimten zijn, met $\forall x \in V_+ : \sigma x = x$ en $\forall x \in V_- : \sigma x = -x$.

Als V simpel is, moet dus gelden dat $V = V_+$ of $V = V_-$.

Verder geldt voor elke $v \in V$, $v \neq 0$ dat kv een niet-triviaal deel-$k[G]$-moduul van V is, dus als V simpel is moet $\dim V = 1$ gelden.

We vinden nu: V simpel $\Leftrightarrow$ ($V = V_+$ of $V = V_-$) en $\dim V = 1$.

Conclusie: elk simpel $k[G]$-moduul is isomorf met k_+ of met k_-. Hier is $k_+ := k$, met $\sigma x = x$ voor alle $x \in k_+$, en $k_- := k$, met $\sigma x = -x$ voor alle $x \in k_-$. Ga zelf na dat $k_+ \ncong_{k[G]} k_-$.

Stelling 8.8 geeft nu het volgende isomorfisme:

$$\begin{aligned} \mathcal{G}_{\text{fl}}(k[G]) &\xrightarrow{\sim} \mathbb{Z} \oplus \mathbb{Z} \\ [V] &\longmapsto (\dim_k V_+, \dim_k V_-). \end{aligned}$$

Merk op: V is van eindige lengte over $k[G] \Leftrightarrow \dim_k V < \infty \Leftrightarrow \dim_k V_+ < \infty$ en $\dim_k V_- < \infty$.

Stelling 8.11. *Zij k een lichaam en R een ring die k als deelring bevat, met $k \subset Z(R)$ en $\dim_k R < \infty$. Zij M een R-moduul. Dan zijn equivalent:*

1. *M is eindig voortgebracht als R-moduul.*
2. *M is van eindige lengte als R-moduul*
3. *$\dim_k M < \infty$.*

Bovendien geldt $1 \leq \#\mathcal{S} < \infty$, waarbij $\mathcal{S} = \{$simpele R-modulen$\}/\cong_R$.

Enkele voorbeelden van ringen die aan de voorwaarden voldoen zijn $R = k$, R een eindige lichaamsuitbreiding van k, $R = k[G]$ met G een eindige groep en $R = M(n, k)$.

Bewijs. $(ii) \Rightarrow (i)$: Al eerder bewezen.

$(i) \Rightarrow (iii)$: M is eindig voortgebracht, dus er is een n zodat R^n surjectief afbeeldt op M. Er geldt dus dat $\dim_k(M) \leq \dim_k(R^n) = n \dim_k(R) < \infty$.

$(iii) \Rightarrow (ii)$: Elk deel-R-moduul van M is ook een deel k-moduul, dus elke R-keten van M is ook een k-keten. Dus de lengte van elke echte R-keten is kleiner dan of gelijk aan de lengte van een maximale k-keten. Deze is gelijk aan $\dim_k M$.

Merk op dat dit bewijs ook geeft dat $\text{length}_R(M) \leq \dim_k(M)$.

Bewijs van $1 \leq \#\mathcal{S} < \infty$:

R is eindig voortgebracht als R-moduul, dus R heeft eindige lengte als R-moduul. Als S een simpel moduul is, geldt dat $S = R/L$, met L een maximaal linksideaal van R. Er is een compositieketen van R van de vorm $0 \subset ... \subset L \subset R$, dus $l_S(R) \geq 1$. Dit betekent dat

$$l(R) = \sum_{S \in \mathcal{S}} l_S(R) \geq \#\mathcal{S},$$

en dus $1 \leq \#\mathcal{S} < \infty$.

Merk op dat dit bewijs zelfs geeft dat $\#\mathcal{S} \leq l(R) \leq \dim_k(R)$. □

Stelling 8.12. *Zij k en R als in de vorige stelling. Zij S een simpel R-moduul. Dan is $\text{End}_R(S)$ een delingsring die k in zijn centrum bevat, met $\dim_k(End_R(S)) < \infty$.*

Als bovendien k algebraïsch afgesloten is, geldt dat $\text{End}_R(S) = k$.

Bewijs. Zij $f \in \text{End}_R(S)$ ongelijk aan 0. Dan is $\ker(f) = 0$ en $\text{im}(f) = S$, want S is simpel en heeft dus geen deelmodulen ongelijk aan 0 en S. $\text{End}_R(S)$ is dus een delingsring.

S is simpel, dus van eindige lengte. Dit betekent dat $n := \dim_k(S) < \infty$, volgens stelling 8.11.

Er geldt dat $\text{End}_R(S) \subset \text{End}_k(S) \cong M(n,k)$. Zoals bekend is $\dim_k(M(n,k)) = n^2 < \infty$. $\text{End}_R(S)$ bevat k, en aangezien $k \subset Z(M(n,k))$ geldt ook dat $k \subset Z(\text{End}_R(S))$.

Stel nu dat k algebraïsch afgesloten is. We weten al dat $k \subset \text{End}_R(S)$, dus we hoeven slechts te bewijzen dat $k \supset \text{End}_R(S)$.

Kies $\alpha \in \text{End}_R(S)$. Definieer een ringhomorfisme

$$\begin{array}{ccc} \varphi : k[X] & \longrightarrow & \text{End}_R(S) \\ \sum a_i X^i & \longmapsto & \sum a_i \alpha^i. \end{array}$$

$k[X]$ is commutatief, dus het beeld van φ is een domein. Dit betekent dat $\ker \varphi$ een priemideaal van $k[X]$ is, dus $\ker \varphi = (X - a)$ voor een $a \in k$. (Merk op dat $\ker \varphi \neq 0$, omdat $\dim_k(\text{End}_R(S)) < \infty$ en $\dim_k(k[X]) = \infty$.)

Nu geldt dat $\varphi(X - a) = 0 = \alpha - a$, dus $\alpha = a$. □

Zij k een lichaam, G een eindige groep en $R = k[G]$. Notatie: $\mathcal{R}(G) = \mathcal{R}_k(G) = \mathcal{G}(k[G])$, de Grothendieckgroep van de $k[G]$-modulen van eindige k-dimensie.

Stelling 8.13. *Zij k een lichaam en G een eindige groep. Dan heeft $\mathcal{R}_k(G)$ een unieke ringstructuur met de gegeven optelling en vermenigvuldiging zodanig dat $[M][N] = [M \otimes_k N]$ voor elke tweetal eindig voortgebrachte $k[G]$-modulen M, N, waarbij $M \otimes_k N$ een $k[G]$-moduul wordt door $\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y)$ voor alle $\sigma \in G$, $x \in M$, $y \in N$. Deze ring is commutatief.*

Voorbeeld
Als $\#G = 2$ en k een lichaam van karakteristiek ongelijk aan 2, dan is $\mathcal{S} = \{k_+, k_-\}$ en $\mathcal{R}(G) = \mathbb{Z}[k_+] \oplus \mathbb{Z}[k_-]$.

Zij $\epsilon, \eta \in \{\pm 1\}$. We weten dat $k_\epsilon \otimes_k k_\eta = k$ als k-vectorruimten. Er geldt voor alle $x \in k_\epsilon$, $y \in k_\eta$ dat $\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y) = \epsilon x \otimes \eta y = \epsilon\eta(x \otimes y)$. Dus $[k_\epsilon][k_\eta] = [k_{\epsilon\eta}]$ en $\mathcal{R}(G) \cong \mathbb{Z}[\text{groep van orde 2}]$ (als ringen).

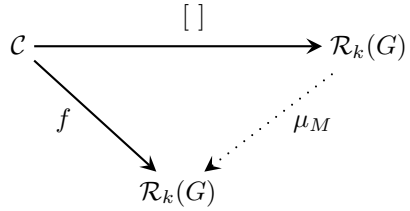
Bewijs. We moeten een vermenigvuldiging $\mathcal{R}_k(G) \times \mathcal{R}_k(G) \longrightarrow \mathcal{R}_k(G)$ definiëren die aan de eigenschappen uit de stelling voldoet.

Houd eerst M vast. Beschouw dan de afbeelding

$$\begin{array}{rcl} f : \mathcal{C} & \longrightarrow & \mathcal{R}_k(G) \\ N & \longmapsto & [M \otimes_k N]. \end{array}$$

Als $0 \to N_1 \to N_2 \to N_3 \to 0$ exact is, is $M \otimes_k N_1 \to M \otimes_k N_2 \to M \otimes_k N_3 \to 0$ ook exact. Omdat k een lichaam is, splitst het eerste exacte rijtje (volgens opgave A8.19). Ga na dat hieruit volgt dat de geïnduceerde afbeelding $M \otimes_k N_1 \to M \otimes_k N_2$ een injectie is, dus $0 \to M \otimes_k N_1 \to M \otimes_k N_2 \to M \otimes_k N_3 \to 0$ is exact. Alle afbeeldingen zijn ook $k[G]$-lineair, dus f is een additieve invariant.

De universele eigenschap van $\mathcal{R}_k(G)$ geeft nu een uniek groepshomomorfisme μ_M zodat $\mu_M([N]) = [M \otimes_k N]$.

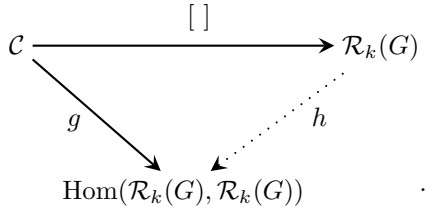


Beschouw nu de afbeelding

$$\begin{array}{rcl} g : \mathcal{C} & \longrightarrow & \mathrm{Hom}(\mathcal{R}_k(G), \mathcal{R}_k(G)) \\ M & \longmapsto & \mu_M. \end{array}$$

Ga zelf na dat dit ook een additieve invariant is. (Het bewijs is bijna hetzelfde als dat van de vorige additieve invariant.)

Universaliteit geeft nu een uniek groepshomomorfisme $h : \mathcal{R}_k(G) \longrightarrow \mathrm{Hom}(\mathcal{R}_k(G), \mathcal{R}_k(G))$, zodat het volgende diagram commutatief is:



Definieer nu de vermenigvuldiging op $\mathcal{R}_k(G)$ door $xy = h(x)(y)$ voor alle $x, y \in \mathcal{R}_k(G)$.

Deze afbeelding heeft per constructie de gewenste eigenschap $[M][N] = [M \otimes_k N]$, immers $[M][N] = h([M])[N] = \mu_M([N]) = [M \otimes_k N]$.

De distributieve wetten volgen uit de bilineariteit (ga deze zelf na). Associativiteit volgt uit $(L \otimes_k M) \otimes_k N \cong_{k[G]} L \otimes_k (M \otimes_k N)$.

Als eenheidselement fungeert $[k]$ voor het $k[G]$-moduul k met $\sigma x = x$ voor alle $\sigma \in G$, $x \in k$. Controleer zelf dat de afbeelding $k \otimes_k N \to N$ met $x \otimes y \mapsto xy$ een $k[G]$-lineair isomorfisme geeft.

Commutativiteit van de vermenigvuldiging volgt direct uit de commutativiteit van $- \otimes_k -$. □

Stelling 8.14. *Zij k een lichaam en G een eindige groep. Dan heeft $\mathcal{R}_k(G)$ een uniek ringautomorfisme $\overline{\ }$ waarvoor voor elk eindig voortgebracht $k[G]$-moduul M geldt dat $\overline{[M]} = [\mathrm{Hom}_k(M,k)]$, waarbij $\mathrm{Hom}_k(M,k)$ een $k[G]$-moduul is door $\sigma f(m) = f(\sigma^{-1}m)$ voor $\sigma \in G$, $f \in \mathrm{Hom}_k(M,k)$, $m \in M$. Er geldt dat dit ringautomorfisme twee keer toegepast de identiteit is.*

Merk op dat deze G-werking op $\mathrm{Hom}_k(M,k)$ als volgt is verkregen. Zoals bekend is $\mathrm{Hom}_k(M,k)$ een rechts-$k[G]$-moduul, en dus een links-$k[G]^{\mathrm{opp}}$-moduul. Het ringisomorfisme

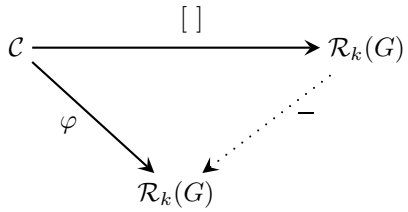
$$\begin{array}{rcl} k[G] & \longrightarrow & k[G]^{\mathrm{opp}} \\ \sum a_\sigma \sigma & \longmapsto & \sum a_\sigma \sigma^{-1} \end{array}$$

maakt nu van $\mathrm{Hom}_k(M,k)$ een links-$k[G]$-moduul.

Bewijs. We gebruiken de volgende notatie: $M^\dagger := \mathrm{Hom}(M,k)$.

Stel dat $0 \to M_1 \to M_2 \to M_3 \to 0$ een korte exacte rij van eindig voortgebrachte $k[G]$-modulen is. Uit de links-exactheid van $\mathrm{Hom}_k(-,k)$ en het splitsen van de gegeven exacte rij volgt dat $0 \to M_3^\dagger \to M_2^\dagger \to M_3^\dagger \to 0$ ook een exacte rijtje van $k[G]$-lineaire afbeeldingen is. Dan geldt dus dat $[M_2^\dagger] = [M_1^\dagger] + [M_3^\dagger]$. Dit betekent dat $\varphi : M \to [M^\dagger]$ een additieve invariant is.

Volgens de universele eigenschap is er nu een uniek *groepshomomorfisme* $\overline{\ }$: $\mathcal{R}_k(G) \to \mathcal{R}_k(G)$ zodanig dat $\forall M \in \mathcal{C} : \overline{[M]} = [M^\dagger]$.



De afbeelding

$$\begin{array}{rcl} M & \longrightarrow & M^{\dagger\dagger} = \mathrm{Hom}_k(\mathrm{Hom}_k(M,k),k) \\ x & \longmapsto & (f \mapsto f(x)) \end{array}$$

is een $k[G]$-lineair isomorfisme. Dit betekent dat $\overline{\overline{[M]}} = [M]$. Hieruit volgt dat $\overline{}$ zijn eigen inverse is, en dus in het bijzonder een (groeps)isomorfisme.

Om te bewijzen dat $\overline{}$ ook een ringisomorfisme is, is het voldoende de ringhomomorfisme-eigenschap voor voortbrengers van $\mathcal{R}_k(G)$ te bewijzen. We moeten dus laten zien dat $[M^\dagger][N^\dagger] = [(M \otimes_k N)^\dagger]$. We hebben gezien dat $[M^\dagger][N^\dagger] = [M^\dagger \otimes_k N^\dagger]$.

We construeren een homomorfisme

$$\begin{array}{rcl} \psi_{M,N} : \mathrm{Hom}_k(M,k) \otimes_k \mathrm{Hom}_k(N,k) & \longrightarrow & \mathrm{Hom}_k(M \otimes_k N, k) \\ f \otimes g & \longmapsto & (x \otimes y \mapsto f(x)g(y)). \end{array}$$

Het bestaan van zo'n ψ is te bewijzen door de universele eigenschappen van beide tensorproducten te gebruiken. Ga zelf na dat ψ een $k[G]$-lineaire afbeelding is.

Als $M = N = k$ is $\psi_{M,N}$ een isomorfisme. Controleer nu dat $\psi_{M,N}$ ook een isomorfisme is als M en N eindige directe sommen van k zijn. Dit bewijst dat $\psi_{M,N}$ een isomorfisme is voor eindig-dimensionale vectorruimten M en N, en dus voor $M, N \in \mathcal{C}$.

Het isomorfisme ψ geeft dus een isomorfisme tussen $M^\dagger \otimes_k N^\dagger$ en $(M \otimes_k N)^\dagger$. Dit betekent dat, zoals gewenst, $[M^\dagger \otimes_k N^\dagger] = [(M \otimes_k N)^\dagger]$. □

9 Semi-simpliciteit

Zij R een ring.

Definitie 9.1. *Een R-moduul M heet* semi-simpel *als elke exacte rij van R-modulen $0 \to L \to M \to N \to 0$ splitst.*

Propositie 9.2. *Stel M is semi-simpel.*

- *Als $0 \to L \to M \to N \to 0$ exact is, dan zijn L en N semi-simpel*
- *Als $M \neq 0$, dan heeft M een deelmoduul dat simpel is.*

Bewijs. Stel $0 \to L \xrightarrow{f} M \to N \to 0$ is exact. We zullen eerst bewijzen dat L dan semi-simpel is.

Stel $0 \to J \xrightarrow{h} L \to K \to 0$ is exact. Omdat zowel h en f injectief zijn, is $i := fh$ ook injectief en kunnen we het volgende commutatieve diagram met exacte rijen construeren:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \xrightarrow{h} & L & \longrightarrow & K & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_J} & & \downarrow{\scriptstyle f} & & & & \\ 0 & \longrightarrow & J & \xrightarrow{i} & M & \longrightarrow & M/J & \longrightarrow & 0. \end{array}$$

M is semi-simpel, dus de onderste exacte rij splitst, dus is er een R-lineaire afbeelding $j : M \to J$ zodat $ji = \mathrm{id}_J$. Definieer nu $k := jf$. Dan geldt dat $kh = jfh = ji = \mathrm{id}_J$, dus de bovenste rij splitst ook, en L is semi-simpel.

Omdat $0 \to L \to M \to N \to 0$ splitst, is $M \cong L \oplus N$, dus er is ook een splitsende exacte rij $0 \to N \to M \to L \to 0$. Hieruit volgt dat N ook semi-simpel is.

Kies nu $x \in M$, $x \neq 0$. Dan is $Rx \subset M$ een deelmoduul van R isomorf met R/I voor $I = \mathrm{Ann}(x)$. (Merk op dat $I \neq R$.) Zij L met $I \subset L \subset R$ een maximaal linksideaal. Dan is R/L simpel.

Beschouw het exacte rijtje $0 \to L/I \to R/I \to R/L \to 0$. Dit rijtje splitst, want M, en dus ook $Rx \cong R/I \subset M$ is semi-simpel. Dus geldt: $(L/I) \oplus (R/L) \cong R/I \cong Rx \subset M$, dus R/L is isomorf met een (simpel) deelmoduul van M. □

Stelling 9.3. *Zij R een ring en M een R-moduul. Dan zijn equivalent:*

1. *M is semi-simpel.*
2. *Er zijn een collectie $(S_i)_{i\in I}$ van simpele R-modulen en een isomorfisme $M \cong \bigoplus_{i\in I} S_i$.*
3. *Er zijn een collectie $(S_i)_{i\in I}$ van simpele R-modulen en een surjectieve R-lineaire afbeelding $\bigoplus_{i\in I} S_i \twoheadrightarrow M$.*

Voorbeeld
Zij $R = \mathbb{Z}$. Dan geldt: M is semi-simpel $\Leftrightarrow M \cong \bigoplus_{i\in I} \mathbb{Z}/p_i\mathbb{Z}$ met p_i priem.

Bewijs. (1) $\Rightarrow$ (3): Neem $\mathcal{T} = \{\text{simpele deelmodulen van } M\}$. Beschouw de afbeelding

$$\begin{array}{rcl} f : \displaystyle\bigoplus_{S\in\mathcal{T}} S & \longrightarrow & M \\ (x_S)_{S\in\mathcal{T}} & \longmapsto & \displaystyle\sum_{S\in\mathcal{T}} x_S. \end{array}$$

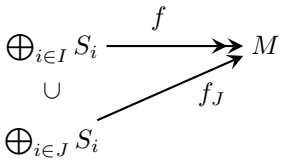
Definieer N als het beeld van f. Dan is er een $K \subset M$ zodat $M = N \oplus K$, omdat M semi-simpel is.

Als $K = 0$ is f de gevraagde surjectie, dus neem aan dat $K \neq 0$. K is semi-simpel, dus heeft K volgens propositie 9.2 een simpel deelmoduul U. Omdat $U \subset M$, geldt dat $U \in \mathcal{T}$. Maar dat betekent dat $U \subset N$, wat in tegenspraak is met $N \cap K = 0$.

(3) $\Rightarrow$ (2):

Zij $f : \bigoplus_{i\in I} S_i \longrightarrow\!\!\!\!\!\rightarrow M$ als in de stelling.

Definieer voor een deelverzameling $J \subset I$ de door f geïnduceerde afbeelding $f_J : \bigoplus_{i\in J} S_i \to M$.



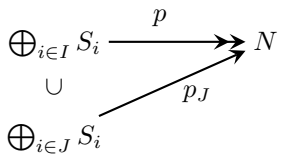
Kies nu (met het lemma van Zorn) een maximale deelverzameling J uit alle deelverzamelingen $J' \subset I$ waarvoor $f_{J'}$ injectief is. We zullen bewijzen dat f_J ook surjectief is.

Als $I = J$ zijn we klaar. Dus stel dat $I \neq J$. Zij $h \in I$, $h \notin J$. De maximaliteit van J impliceert dat $f_{(J\cup\{h\})}$ niet injectief is. Dus, de afbeelding $S_h \overset{f_{\{h\}}}{\to} M \to M/(\mathrm{im}(f_J))$ is niet injectief. Omdat S_h simpel is, moet dit dus de nul-afbeelding zijn. Dit betekent dat het beeld van S_h volledig bevat is in het beeld van f_J.

Hieruit volgt dat voor alle $i \in I$ het beeld van $f_{\{i\}}$ in M bevat is in $\mathrm{im}(f_J)$, en dus het gehele beeld van f.

(2) $\Rightarrow$ (1): Stel de rij $0 \to L \to \bigoplus_{i\in I} S_i \overset{p}{\to} N \to 0$ is kort exact.

De methode uit het bewijs van (3) $\Rightarrow$ (2) geeft bij deze surjectie p een deelverzameling J en een afbeelding p_J zodat $p_J : \bigoplus_{i\in J} S_i \to N$ een isomorfisme is.



Het homomorfisme $N \overset{p_J^{-1}}{\to} \bigoplus_{i\in J} S_i \hookrightarrow \bigoplus_{i\in I} S_i$ geeft nu een splitsing van de exacte rij. □

Definitie 9.4. *Een ring R heet* semi-simpel *als elk links-R-moduul semi-simpel is.*

Propositie 9.5. *De volgende beweringen zijn equivalent:*

1. *R is semi-simpel.*
2. *R is als links-R-moduul semi-simpel.*
3. *Elke korte exacte rij van R-modulen splitst.*

Bewijs. (3) $\Leftrightarrow$ (1): Per definitie.

(1) $\Rightarrow$ (2): Triviaal.

(2) $\Rightarrow$ (1): Zij M een R-moduul. Dan is er een verzameling I zodat $R^{(I)} \twoheadrightarrow M$. R is semi-simpel, dus volgens stelling 9.3 is $R^{(I)}$ semi-simpel en dan is volgens propositie 9.2 M semi-simpel. □

Voorbeeld
Zij $R = D$ een delingsring. Als $x \in D$, $x \neq 0$, dan $Dx = D$, dus D heeft precies 2 deelmodulen: 0 en D. Dus D is simpel als links-D-moduul. In het bijzonder is D semi-simpel. Elk simpel D-moduul is isomorf met $D/(\text{maximaal linksideaal}) = D$.

Elk D-moduul is semi-simpel en dus een directe som van kopieën van D.

Lemma 9.6. *Er geldt:* $D^{(I)} \cong D^{(J)} \Leftrightarrow \#I = \#J$.

Bewijs. ($\Leftarrow$): Triviaal.

($\Rightarrow$): Als I eindig is, dan is de D-lengte van $D^{(I)}$ gelijk aan $\#I$. Dan heeft $D^{(J)}$ dus ook eindige lengte, en is $\#J = l_D(D^{(J)}) = l_D(D^{(I)}) = \#I$.

Als I oneindig is, dan moet J dus ook oneindig zijn. Zij f een isomorfisme van $D^{(I)} \xrightarrow{\sim} D^{(J)}$, en $(e_i)_{i\in I}$ de standaard-basis voor $D^{(I)}$.

Definieer $J_i := \{j : \text{de } j\text{-de coördinaat van } f(e_i) \neq 0\} \subset J$. Omdat f surjectief is, is $J = \bigcup_{i\in I} J_i$.

Dus: $\#J \leq \sum_{i\in I} \#J_i \leq \#I \cdot \#Z = \#I$. Vanwege symmetrie geldt ook $\#J \leq \#I$, en dus $\#I = \#J$. □

Stelling 9.7 (Maschke). *Stel k is een lichaam en G een eindige groep met* char $k \nmid \#G$ *(bijvoorbeeld als* char $k = 0$*). Dan is $k[G]$ semi-simpel.*

Bewijs. Stel $0 \to L \to M \xrightarrow{p} N \to 0$ is een korte exacte rij van $k[G]$-modulen. Als we deze rij als een rij van k-modulen beschouwen, splitst hij omdat k semi-simpel is. Er is dus een k-lineaire afbeelding $q : N \to M$ zodat $pq = \mathrm{id}_N$.

Definieer $r : N \to M$ door

$$r = \frac{1}{\#G} \sum_{\tau\in G} \tau q \tau^{-1} \qquad (\text{in } \mathrm{Hom}_k(N, M)).$$

Hiervoor geldt dat

$$pr = \frac{1}{\#G} \sum_{\tau\in G} p\tau q\tau^{-1} = \frac{1}{\#G} \sum_{\tau\in G} \mathrm{id}_N = \mathrm{id}_N,$$

omdat p een $k[G]$-lineaire afbeelding is.

Ook geldt voor $\sigma \in G$ dat

$$\sigma r \sigma^{-1} = \frac{1}{\#G} \sum_{\tau\in G} p\sigma\tau q(\sigma\tau)^{-1} = r,$$

dus r is $k[G]$-lineair. Dit betekent dat r een splitsing van de rij geeft. □

Propositie 9.8. *Stel $R \cong \bigoplus_{i\in I} S_i$ als links-R-modulen, met S_i simpel voor elke $i \in I$. Dan is I eindig en elk simpel R-moduul is isomorf met één van de S_i.*

Bewijs. Zij $f : R \to \bigoplus_{i\in I} S_i$ een links-R-moduulisomorfisme. Zij $f(1) = (a_i)_{i\in I} \in \bigoplus_{i\in I} S_i$. Definieer $J := \{i \in I : a_i \neq 0\}$, een *eindige* deelverzameling van I. Nu geldt dat $f(1) \in \bigoplus_{i\in J} S_i$, dus $Rf(1) \subset \bigoplus_{i\in J} S_i$. Er geldt dat $Rf(1) = f(R1) = f(R) = \bigoplus_{i\in I} S_i$, want f is R-lineair en surjectief. Uit dit alles volgt dat $\bigoplus_{i\in I} S_i \subset \bigoplus_{i\in J} S_i \subset \bigoplus_{i\in I} S_i$, dus $I = J$ en I is eindig.

Nu geldt $R \cong_R S_1 \oplus S_2 \oplus \ldots \oplus S_n$ voor een $n \in \mathbb{Z}$. R heeft een compositieketen waarin alleen de S_i als quotiënten optreden, dus R is van eindige lengte.

Zij S een simpel R-moduul, dan is $S \cong R/L$ voor een maximaal linksideaal $L \subset R$. We hebben $0 \subset L \subset R$ en L is van eindige lengte, dus L heeft een compositieketen. We vinden op deze manier dus nog een compositieketen van R. Deze keten is Jordan-Hölder-isomorf met de compositieketen waarin alleen de S_i als quotiënten voorkomen. Dus $S \cong S_i$ voor een i. □

Gevolg 9.9. *Als R semi-simpel is en de S_i als in propositie 9.8, dan is elk R-moduul isomorf met een R-moduul van de vorm $\bigoplus_{i\in I} S_i^{(V_i)}$ voor zekere verzamelingen V_i.*

Voorbeeld
Neem D een delingsring, $n \in \mathbb{Z}_{>0}$ en $R = M(n, D)$. Dan gelden de volgende beweringen:

1. $S = D^n$ is een simpel R-moduul. (We vatten D^n op als de verzameling kolomvectoren met n elementen uit D.)
2. $R = S^n$ als links-R-moduul, R is semi-simpel, S is op isomorfie na het enige simpele R-moduul en elk R-moduul is isomorf met $S^{(V)}$ voor een verzameling V.
3. De afbeelding $\varphi : D^{\mathrm{opp}} \xrightarrow{\sim} {}_R\mathrm{End}(S)$ gegeven door $d \mapsto (x \mapsto xd)$ is een ringisomorfisme.

Bewijs. 1. Beschouw D^n als rechts-D-moduul. Dan $R = \mathrm{End}_D(D^n)$. Als nu $x \in D^n$, $x \neq 0$, dan $xD \cong_D D$, waarbij $xd \leftrightarrow d$, dus

$$\begin{array}{rcl} D^n = (xD) \oplus (\text{complement}) & \xrightarrow{f} & D \\ (xd, \ldots) & \longmapsto & d \end{array}$$

is surjectief. De samenstelling van f met de inclusie $f_i : D \to D^n$, $d \mapsto de_i$ (waarbij e_i de i-de standaard-basisvector is) levert voor het element $x \in xD$ het volgende op: $x = (x, 0) \xmapsto{f} 1 \longmapsto e_i$. Deze samengestelde afbeelding is een D-lineair endormorfisme van D^n, dus is een element van R, zeg r_i. Dus voor elke $i = 1, \ldots, n$ is er een $r_i \in R$ met $r_i x = e_i$. Dus $e_1, \ldots, e_n \in Rx$, dus $D^n \subset Rx \subset D^n$. Dus $Rx = D^n$, dus D^n is simpel als R-moduul.

2. Het bewijs van $R = S^n$ gaat precies hetzelfde als voor lichamen. R is dus duidelijk semi-simpel. De rest van de bewering volgt uit propositie 9.8.

3. De afbeelding $f : D \to {}_R\mathrm{End}(S)$ gegeven door $d \mapsto (x \mapsto xd)$ is welgedefinieerd (want $(Ax)d = A(xd)$ voor alle $A \in R$ en $d \in D$). Verder zien we dat voor alle $d_1, d_2 \in D$ geldt dat $d_1 + d_2 \mapsto (x \mapsto x(d_1 + d_2)) = (x \mapsto xd_1 + xd_2) = (x \mapsto xd_1) + (x \mapsto xd_2)$, dus voor alle $d_1, d_2 \in D$ geldt dat $f(d_1 + d_2) = f(d_1) + f(d_2)$. Dus f is een groepshomomorfisme.

Vanwege de associativiteit van D geldt voor alle $d_1, d_2 \in D$ dat $(x \mapsto x(d_1 d_2)) = (x \mapsto (xd_1)d_2)$, dus voor alle $d_1, d_2 \in D$ geldt $f(d_1 d_2) = f(d_1) \circ f(d_2)$. Het is duidelijk dat $f(1) = \mathrm{id}$.

Er volgt dat f een anti-ringhomomorfisme is, dus $f : D^{\mathrm{opp}} \to {}_R\mathrm{End}(S)$ is een ringhomomorfisme op D^{opp}.

We willen nog laten zien dat f bijectief is. Stel dat $\delta : S \to S$ een R-lineair endomorfisme is. Dan zoeken we een $d \in D$ met $f(d) = \delta$, d.w.z. $\forall x \in S : \delta(x) = xd$. Omdat δ R-lineair is, geldt voor alle $r \in R$ en $x \in S$ dat $\delta(rx) = r\delta(x)$. Dus voor elke $r \in R$ beeldt δ de verzameling rS binnen rS af. Pas dit toe met r de matrix met een 1 op plaats (i, i) en verder overal een 0. Dan vinden we:

$$rS = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ D \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e_i D.$$

Dus $\delta(e_i) = e_i d_i$ voor een $d_i \in D$. Nu geldt dus:

$$\delta \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 d_1 \\ a_2 d_2 \\ \vdots \\ a_n d_n \end{pmatrix}.$$

Neem nu

$$r = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix}.$$

Dan vinden we dat

$$rS = \left\{ \begin{pmatrix} a \\ a \\ \vdots \\ a \end{pmatrix} : a \in D \right\}.$$

Dus

$$\delta \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ a \\ \vdots \\ a \end{pmatrix}$$

voor een $a \in D$. Aan de andere kant weten we al dat

$$\delta \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}.$$

Hieruit volgt nu dat $a = d_1 = d_2 = d_3 = \ldots = d_n$. Dus voor alle $x \in S$ geldt dat $\delta(x) = xd$ voor een $d \in D$. Dus f is surjectief.

Het is eenvoudig te zien dat f ook injectief is, want de kern van f is een tweezijdig ideaal in de delingsring D, dus gelijk aan 0.

□

Definieer $D' = ({}_R\mathrm{End}(S))^{\mathrm{opp}}$. Merk op dat $D^{\mathrm{opp}} \cong (D')^{\mathrm{opp}}$. Nu induceert φ een isomorfisme $R \to \mathrm{End}_{D'}(S) \cong M(n, D')$ (ga dit zelf na).

Gevolg 9.10. *Zij $n \in \mathbb{Z}_{>0}$ en k een lichaam. Dan geldt $Z(M(n,k)) = k$.*

Bewijs. $\supset$: Duidelijk.

$\subset$: Als $r \in Z(M(n,k))$, dan is $S = k^n \xrightarrow{r} k^n$; $x \mapsto rx$ $M(n,k)$-lineair, namelijk: als $rs = sr$ voor $s \in M(n,k)$, dan $r(sx) = s(rx)$. Dus $r \in {}_R\mathrm{End}(S) = k$. □

Stelling 9.11. *Laat $t \in \mathbb{Z}_{\geq 0}$, $D_1, D_2, \ldots, D_t$ delingsringen en $R = \prod_{i=1}^t M(n_i, D_i)$. Dan gelden de volgende beweringen. R is semi-simpel. Voor elke $i \in \{1, \ldots, t\}$ is $S_i = D_i^{n_i}$ een simpel R-moduul en $R \cong \bigoplus_{i=1}^t S_i^{n_i}$ als R-moduul. Elk simpel R-moduul is isomorf met S_i voor een unieke $i \in \{1, 2, \ldots, t\}$. Verder geldt $D_i^{\mathrm{opp}} \cong {}_R\mathrm{End}(S_i)$.*

Bewijs. We weten dat $R = R_1 \times R_2 \times \ldots \times R_t$, waarbij $R_i = M(n_i, D_i)$. We hebben in het voorbeeld gezien dat $S_i = D_i^{n_i}$ voor alle $i \in \{1, 2, \ldots, t\}$ een simpel R_i-moduul is en dat ${}_{R_i}R_i \cong S_i^{n_i}$. Dus geldt dat ${}_R R \cong \bigoplus_{i=1}^t S_i^{n_i}$. Uit het voorbeeld volgt ook dat elk simpel R-moduul isomorf is met S_i voor een unieke $i \in \{1, 2, \ldots, t\}$ en dat $D_i^{\mathrm{opp}} \cong {}_R\mathrm{End}(S_i)$. □

Stelling 9.12. *Stel R is een semi-simpele ring. Dan is R van de vorm $\prod_{i=1}^t M(n_i, D_i)$ met t, (n_i) en (D_i) als in stelling 9.11 en bovendien zijn t, (n_i) en (D_i) uniek bepaald door R op volgorde en isomorfie na.*

In het bewijs van deze stelling gebruiken we de volgende lemma's.

Lemma 9.13. *Zij R een ring. Dan zijn R en $({}_R\mathrm{End}(R))^{\mathrm{opp}}$ isomorf als ringen.*

Bewijs. De afbeelding $R \to ({}_R\mathrm{End}(R))^{\mathrm{opp}}$ gegeven door $a \mapsto (x \mapsto xa)$ is een ringhomomorfisme met inverse $f \mapsto f(1)$. Ga dit zelf na. □

Lemma 9.14. *Zij R een ring, $M_1, M_2, \ldots, M_m$ en $N_1, N_2, \ldots, N_n$ R-modulen en zij $M = \bigoplus_{i=1}^m M_i$ en $N = \bigoplus_{j=1}^n N_j$. Dan: ${}_R\mathrm{Hom}(M, N) \cong \bigoplus_{i,j} {}_R\mathrm{Hom}(M_i, N_j)$. (Hierbij loopt i over $1, \ldots, m$ en j over $1, \ldots, n$.)*

Bewijs. Duidelijk. □

Bewijs van stelling 9.12. We weten dat ${}_R\mathrm{Hom}(S_i, S_j) = 0$ als $S_i \ncong S_j$. Verder geldt dat ${}_R\mathrm{End}(S_i) = D_i$ een delingsring is.

Stel dat $S_1, S_2, \ldots, S_t$ alle simpele R-modulen zijn op isomorfie na en onderling niet isomorf. Kies $n_1, \ldots, n_t$ zo dat ${}_R R \cong \bigoplus_{i=1}^t S_i^{n_i}$. Dan geldt:

$$\begin{aligned} {}_R\mathrm{End}(R) &= {}_R\mathrm{End}(\bigoplus_{i=1}^t S_i^{n_i}) = \prod_{i-1}^t {}_R\mathrm{End}(S_i^{n_i}) = \prod_{i=1}^t \prod_{\substack{1\le j\le n_i,\\ 1\le k\le n_i}} {}_R\mathrm{Hom}(S_i, S_i) \\ &= \prod_{i=1}^t \prod_{j,k=1}^{n_i} D_i^{\mathrm{opp}} = \prod_{i=1}^t M(n_i, D_i^{\mathrm{opp}}). \end{aligned}$$

Een eenvoudige berekening laat zien dat als je de identificatie $\prod_{j,k} D_i \xrightarrow{\sim} M(n_i, D_i^{\mathrm{opp}})$ goed kiest, dan is de resulterende afbeelding ${}_R\mathrm{End}(R) \to \prod_{i-1}^t M(n_i, D_i^{\mathrm{opp}})$ een *ring*isomorfisme.

Nu geldt: $R \cong ({}_R\mathrm{End}(R))^{\mathrm{opp}} \cong \prod_{i=1}^t M(n_i, D_i^{\mathrm{opp}})^{\mathrm{opp}} = \prod_{i=1}^t M(n_i, D_i)$. Deze laatste gelijkheid geldt omdat voor $n \in \mathbb{Z}_{>0}$ en een delingsring D geldt dat $M(n, D)^{\mathrm{opp}} \to M(n, D^{\mathrm{opp}})$ gegeven door $A \mapsto A^T$ een isomorfisme is. □

Merk op dat $n_i = \mathrm{length}_{S_i} R$. Voor alle $i \in \{1, \ldots, t\}$ geldt dat S_i een links-D_i^{opp}-moduul is dus een rechts-D_i-moduul, en in feite een R-D_i-bimoduul, want $(rs)d = r(sd)$ voor $r \in R$, $s \in S_i$ en $d \in D_i$.

Stelling 9.15. *Stel R is een semi-simpele ring, $k \subset Z(R)$ een deelring die een lichaam is, en neem aan dat $[R : k] = \dim_k(R) < \infty$. Dan geldt $R \cong \prod_{i=1}^t M(n_i, D_i)$ met $t \in \mathbb{Z}_{>0}$, $n_i \in \mathbb{Z}_{>0}$ en D_i een delingsring met $k \subset Z(D_i)$ en $[D_i : k] < \infty$. Bovendien geldt $\sum_{i=1}^t n_i^2 [D_i : k] = [R : k]$. Als $k = \bar{k}$, dan geldt $D_i = k$ voor alle $i \in \{1, \ldots, t\}$, en $\sum_{i=1}^t n_i^2 = [R : k]$.*

Bewijs. Zij $S_1, S_2, \ldots, S_t$ als tevoren. Dan $\dim_k(S_i) < \infty$. Volgens stelling 9.12 geldt dat $R \cong \prod_{i=1}^t M(n_i, D_i)$ met $n_i = \mathrm{length}_{S_i} R$ en $D_i = ({}_R\mathrm{End}(S_i))^{\mathrm{opp}} \subset (M(\dim_k(S_i), k))^{\mathrm{opp}}$, dus $k \subset Z(D_i)$.

De gelijkheid $\sum_{i=1}^t n_i^2 [D_i : k] = [R : k]$ is eenvoudig te bewijzen door de dimensies in de gelijkheid $R \cong \prod_{i=1}^t M(n_i, D_i)$ te vergelijken.

Als $k = \bar{k}$, dan geldt dat $D_i = k$ (Stelling 8.12). □

Merk op dat in het geval $k = \bar{k}$ geldt dat $S_i \cong D_i^{n_i} = k^{n_i}$ en dat dus $n_i = \dim_k(S_i)$.

Voorbeeld
$R = k[G]$ met G een groep met char $k \nmid \#G < \infty$. Dan $[R : k] = \#G$. Als $k = \bar{k}$, dan $\sum_{i=1}^t n_i^2 = \#G$.

Voorbeeld
$k = \mathbb{C}$, $G = S_3$, dus $\#G = 6$.

Dan geldt $\mathbb{C}[S_3] \cong \prod_{i=1}^t M(n_i, \mathbb{C})$ als ringen. Uit stelling 9.15 volgt dat $n_1^2 + n_2^2 + \ldots + n_t^2 = 6$. Nu zijn er dus twee mogelijkheden: òf $t = 6$, $n_1 = n_2 = \ldots = n_6 = 1$, òf $t = 3$, $n_1 = n_2 = 1$, $n_3 = 2$. Stel dat het eerste geval geldt, dan volgt dat $M(1, \mathbb{C}) = \mathbb{C}$ en $\mathbb{C}[S_3] \cong \mathbb{C}^6$, dus $\mathbb{C}[S_3]$ is commutatief: tegenspraak. Dus we zitten in het tweede geval: $t = 3$, $n_1 = n_2 = 1$ en $n_3 = 2$. We vinden dat

$\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times M(2,\mathbb{C})$. Dus op isomorfie na zijn er precies drie simpele $\mathbb{C}[S_3]$-modulen, twee van $\mathbb{C}$-dimensie 1 en één van $\mathbb{C}$-dimensie 2. Wat zijn deze simpele $\mathbb{C}[S_3]$-modulen?

- $S_0 = \mathbb{C}$, $\sigma x = x$ voor alle $x \in \mathbb{C}$, $\sigma \in S_3$
- $S_1 = \mathbb{C}$, $\sigma x = \varepsilon(\sigma)x$ voor alle $x \in \mathbb{C}$, $\sigma \in S_3$ en met $\varepsilon : S_3 \to \{\pm 1\}$ de tekenafbeelding.
- We bekijken $\mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3$, $\sigma(e_i) = e_{\sigma(i)}$ voor alle $\sigma \in S_3$. Dus $\sigma(e_1 + e_2 + e_3) = e_1 + e_2 + e_3$ voor alle $\sigma \in S_3$. Nu nemen we $S_2 = \{(x_1, x_2, x_3) \in \mathbb{C}^3 : x_1 + x_2 + x_3 = 0\}$. Dan geldt $\dim_{\mathbb{C}}(S_0) = 2$. Omdat $\mathbb{C}[S_3]$ semi-simpel is, is S_2 in elk geval een directe som van semi-simpele modulen. Dus òf S_2 is simpel, òf S_2 is een directe som van één-dimensionale modulen, dus we hebben de volgende mogelijkheden: $S_2 \cong S_0 \oplus S_0$ of $S_0 \oplus S_1$ of $S_1 \oplus S_1$. Op alle drie de modulen werkt A_3 als de identiteit. Maar A_3 werkt niet triviaal op S_2. Dus S_2 is semi-simpel.

Als k een lichaam is en G een groep, dan is de afbeelding

$$\begin{array}{rcl} \mathrm{Hom}(G, k^*) & \longrightarrow & \{k[G]\text{-modulen van } k\text{-dimensie } 1\}/\cong_{k[G]} \\ \chi & \longmapsto & k_\chi = (k \text{ met } G\text{-actie } \sigma(x) = \chi(\sigma)x, \text{ voor } \sigma \in G \text{ en } x \in k) \end{array}$$

een bijectie, want de afbeelding $S \mapsto (\chi : G \to \mathrm{Aut}_k(S) \cong k^*)$ is de inverse. $\mathrm{Hom}(G, k^*)$ is een groep. De corresponderende groepsstructuur aan de rechterkant wordt gegeven door $\otimes$. Er geldt nu dus dat $k[G] \cong \prod_{i=1}^{t} M(n_i, k)$, met $\#\{i : n_i = 1\} = \#\mathrm{Hom}(G, k^*)$.

Voorbeeld
Zij $k = \bar{k}$, char $k = 0$ en G een eindige abelse groep. Dan geldt dat $k[G] \cong \prod_{i=1}^{t} M(n_i, k)$, dus $\prod_{i=1}^{t} M(n_i, k)$ is commutatief, dus alle n_i zijn gelijk aan 1. We weten dat $\sum_{i=1}^{t} n_i^2 = \#G$, dus $t = \#G = \#\mathrm{Hom}(G, k^*)$.

Als $G = V_4 = \{1, \sigma, \tau, \sigma\tau\}$, dan bestaan er vier homomorfismen $G \to k^*$, gegeven door:

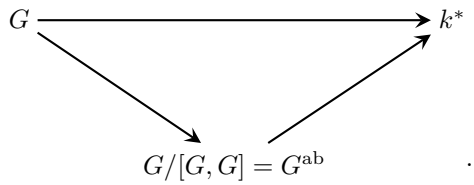
	1	σ	τ	$\sigma\tau$
	1	1	1	1
	1	-1	1	-1
	1	1	-1	-1
	1	-1	-1	1

.

Er bestaan dus precies vier simpele $k[V_4]$-modulen, allemaal van dimensie 1.

Stelling 9.16. *Zij $k = \bar{k}$,* char $k = 0$ *en $\#G < \infty$. Dan geldt: $\#\{i : n_i = 1\} = \#\mathrm{Hom}(G, k^*) = \#G/[G, G]$.*

Bewijs. We hebben het volgende diagram:



Ieder homomorfisme $G \to k^*$ gaat via $[G,G]$, want k^* is abels, dus alle commutatoren gaan naar 1. Dus $\mathrm{Hom}(G^{\mathrm{ab}}, k^*) \xrightarrow{\sim} \mathrm{Hom}(G, k^*)$. Nu volgt dat $t = \#G/[G,G]$ (zie het voorbeeld hierboven). □

Voorbeeld
$\mathbb{C}[D_4]$, $D_4 = \langle \rho, \sigma \rangle$ met $\sigma\rho\sigma^{-1} = \rho^{-1}$ en $\sigma^2 = \rho^4 = 1$. Dan $\#D_4 = 8$. Dus $\sum_{i=1}^{t} n_i^2 = 8$, $\#\{i : n_i = 1\} = \#D_4/[D_4, D_4] = 4$, want $[D_4, D_4] = \langle \rho^2 \rangle$. We hebben dus $n_1 = n_2 = n_3 = n_4 = 1$, $n_5 = 2$ en $t = 5$. D_4 beeldt surjectief af op $D_4^{\mathrm{ab}} \cong V_4$, dus de 1-dimensionale representaties komen van de representaties van V_4. Verder geeft k^2 waarop ρ en σ werken als

$$\rho = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

een 2-dimensionale representatie. Merk op dat ρ^2 met -1 vermenigvuldigt, dus ρ^2 werkt niet triviaal. Dus deze representatie is irreducibel.

Stelling 9.17. *Stel k is een algebraïsch afgesloten lichaam en G een eindige groep met* char $k \nmid \#G$. *Dan is het aantal isomorfieklassen van simpele $k[G]$-modulen gelijk aan het aantal conjugatieklassen van G.*

Bewijs. $k[G] \cong \prod_{i=1}^{t} M(n_i, k)$, dus $Z(k[G]) \cong Z(\prod_{i=1}^{t} M(n_i, k)) = \prod_{i=1}^{t} Z(M(n_i, k)) = \prod_{i=1}^{t} k$. Stel $a \in Z(k[G])$, $a = \sum_{\sigma \in G} a_\sigma \sigma$ met $a_\sigma \in k$. Dan geldt:

$$\begin{aligned}
a \in Z(k[G]) &\Leftrightarrow \forall b \in k[G] : ab = ba \\
&\Leftrightarrow \forall \tau \in G : a = \tau a \tau^{-1} \\
&\Leftrightarrow \forall \tau \in G : \sum_{\sigma \in G} a_\sigma \sigma = \sum_{\rho \in G} a_{\tau^{-1}\rho\tau} \rho \\
&\Leftrightarrow \forall \sigma, \tau \in G : a_\sigma = a_{\tau^{-1}\sigma\tau} \\
&\Leftrightarrow a \text{ is van de vorm } \sum_{C \in G/\sim} a_C (\sum_{\sigma \in C} \sigma),
\end{aligned}$$

waarbij $\sim$ conjugatie is. Dus $\{\sum_{\sigma \in C} \sigma : C \in G/\sim\}$ is een k-basis voor $Z(k[G])$. Als we nu dimensies vergelijken in $Z(k[G]) \cong \prod_{i=1}^{t} k$, vinden we dat $\#(G/\sim) = t$. □

Voorbeeld

- $G = S_3$, $n_1 = n_2 = 1$, $n_3 = 2$, $t = 3$
- G abels, $t = \#G$
- $G = D_4$, $t = 5$, de conjugatieklassen zijn: $\{1\}$, $\{\rho, \rho^{-1}\}$, $\{\sigma, \sigma\rho^2\}$, $\{\sigma\rho, \sigma\rho^3\}$ en $\{\rho^2\}$.

10 Sporen en karakters

In deze paragraaf is k een algebraïsch afgesloten lichaam van karakteristiek 0 en G een eindige groep.

Definitie 10.1. *We noemen de Grothendieckgroep van de eindig voortgebrachte $k[G]$-modulen de* representatiering $\mathcal{R}(G) = \mathcal{R}_k(G)$ *van G.*

Definitie 10.2. *Zij M een eindig voortgebracht $k[G]$-moduul met k-basis $\{e_1, \ldots, e_m\}$. Definieer voor een $\sigma \in G$ de matrix $A_\sigma = (a_{ij})$, waarbij a_{ij} gegeven worden door $\sigma e_i = \sum_{j=1}^m a_{ij} e_j$. Het bij M behorende* karakter *is de functie*

$$\begin{aligned} \chi_M = \mathrm{Tr}_M : G &\longrightarrow k \\ \sigma &\longmapsto \mathrm{Tr}(A_\sigma). \end{aligned}$$

In het bijzonder heet $\chi_M(1)$ de *graad* (of de *dimensie*) van het karakter χ_M. Merk verder op dat $\chi_{M\oplus N} = \chi_M + \chi_N$ (ga dit zelf na).

Voorbeeld
Als $\chi : G \to k^*$ een groepshomomorfisme is, geeft dit een 1-dimensionaal $k[G]$-moduul door $k_\chi = k$ als k-vectorruimte en $\sigma x = \chi(\sigma)x$ voor $\sigma \in G$, $x \in k_\chi$. Hiervoor geldt dat $\chi_{k_\chi} = \chi$.

Merk op dat groepshomomorfismen $G \to k^*$ *ook* karakters genoemd worden. Definitie 10.2 is een algemenere definitie.

Definitie 10.3. *Een functie $f : G \to k$ heet* centraal *als $\forall \sigma, \tau \in G : f(\sigma\tau) = f(\tau\sigma)$, of, equivalent, als $\forall \sigma, \rho \in G : f(\sigma\rho\sigma^{-1}) = f(\rho)$, of, equivalent, als f constant is op elke conjugatieklasse van G.*

De vectorruimte van centrale functies wordt aangegeven met $k^{G/\sim} \subset k^G$. Hier is $G/\sim$ (ook wel aangegeven met Γ) de verzameling conjugatieklassen van G.

Propositie 10.4. *Karakters zijn centraal.*

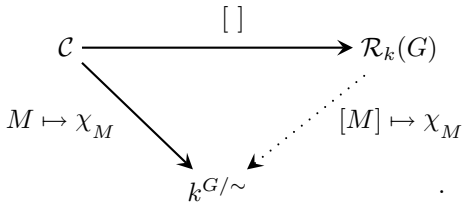
Bewijs. Zij Tr_M een karakter. Dan is voor alle $\sigma, \tau \in G$: $\mathrm{Tr}_M(\sigma\tau) = \mathrm{Tr}_M(\tau\sigma)$. Dit volgt uit de uit lineaire algebra bekende eigenschap $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ voor matrices A en B. □

De afbeelding

$$\begin{aligned} \mathcal{C} := \{\text{e.v. } k[G]\text{-modulen}\} &\longrightarrow k^{G/\sim} \\ M &\longmapsto \chi_M \end{aligned}$$

is additief. Immers, als $0 \to M \to L \to N \to 0$ exact is, dan splitst het rijtje en is L isomorf met $M \oplus N$. Dan geldt dus dat $\chi_L = \chi_M + \chi_N$.

De universele eigenschap van de representatiering van G geeft nu een uniek groepshomomorfisme $k^{G/\sim} \to \mathcal{R}(G)$ dat $[M]$ afbeeldt op χ_M:



Lemma 10.5. *Er geldt* $\chi_{M\otimes_k N} = \chi_M\chi_N$*, waarbij* $\chi_M\chi_N$ *gedefinieerd is door* $(\chi_M\chi_N)(\sigma) = \chi_M(\sigma)\chi_N(\sigma)$ *voor* $\sigma \in G$*.*

Bewijs. Opgave. □

Als $M \cong \bigoplus_S S^{n_S}$, dan is $\chi_M = \sum_S n_S\chi_S$. Het beschrijven van χ_S voor alle simpele $k[G]$-modulen S stelt ons dus in staat om χ_M voor alle $k[G]$-modulen te beschrijven.

Definitie 10.6. *De* karaktertafel *van* G *is de matrix*

$$\left[\chi_S(\sigma)\right]_{\substack{S\in\mathcal{S}\\ \sigma\in G/\sim}}.$$

Hier loopt S *over* $\mathcal{S} = \{$*simpele* $k[G]$*-modulen*$\}/\cong$*.*

Voorbeeld
We gaan de karaktertafel van $G = S_3$ bepalen. We weten al dat $G/\sim = \{1, (1\ 2), (1\ 2\ 3)\}$, $\mathcal{S} = \{1, \varepsilon, S_2\}$. Hier zijn de simpele $k[G]$-modulen 1 en ε 1-dimensionale k-vectorruimten waarop G werkt als de identiteit en de teken-afbeelding, respectievelijk. S_2 is het 2-dimensionale simpele $k[G]$-moduul.

Voor alle $\sigma \in G$ geldt dat $\chi_1(\sigma) = 1$. Ook weten we dat voor $S \in \mathcal{S} : \chi_S(1) = \dim_k(S)$. De overige waarden in de karaktertafel zijn eenvoudig te berekenen.

$S\backslash\sigma$	1	(1 2)	(1 2 3)
1	1	1	1
ε	1	-1	1
S_2	2	0	-1

Stelling 10.7. *De matrix* $\left[\chi_S(\sigma)\right]_{\substack{S\in\mathcal{S}\\ \sigma\in G/\sim}}$ *is inverteerbaar.*

Bewijs. We hebben al eerder gezien dat $k[G] \cong \prod_{S\in\mathcal{S}} \mathrm{End}_k(S)$. Dit betekent dat er een isomorfisme $\varphi : Z(k[G]) \xrightarrow{\sim} \prod_{S\in\mathcal{S}} k$ is. Ook is al bewezen dat dan $\{\sum_{\sigma\in C}\sigma : C \in G/\sim\}$ een k-basis voor $Z(k[G])$ is. Zij e_C de C-de basisvector, dus $e_C := \sum_{\sigma\in C}\sigma$ voor $C \in G/\sim$.

De S-de component van $\varphi(e_C)$ is $\alpha \in k$ als e_C op S werkt via vermenigvuldiging met α. Dan geldt:

$$\begin{aligned}
\alpha &= \frac{1}{\dim_k(S)}\mathrm{Tr}(\text{actie van } e_C \text{ op } S)\\
&= \frac{1}{\dim_k(S)}\sum_{\sigma\in C}\chi_S(\sigma)\\
&= \frac{\#C}{\dim_k(S)}\chi_S(\sigma) \quad \text{voor } \sigma \text{ in } C.
\end{aligned}$$

De afbeelding φ wordt op de gegeven bases gegeven door de matrix

$$\left[\frac{\#[\sigma]}{\dim_k(S)}\chi_S(\sigma)\right]_{\substack{S\in\mathcal{S}\\ \sigma\in G/\sim.}}$$

Deze matrix is inverteerbaar omdat φ een isomorfisme is. Omdat $\#[\sigma] \neq 0$ geldt nu dat ook $\left[\chi_S(\sigma)\right]_{\substack{S\in\mathcal{S}\\ \sigma\in G/\sim}}$ inverteerbaar is. □

Gevolg 10.8. *Het ringhomomorfisme*

$$\begin{array}{rcl}\psi : \mathcal{R}(G) & \longrightarrow & k^{G/\sim}\\ [M] & \longmapsto & \chi_M\end{array}$$

is injectief en induceert een ringisomorfisme $\psi' : \mathcal{R}(G)\otimes_{\mathbb{Z}} k \xrightarrow{\sim} k^{G/\sim}$.

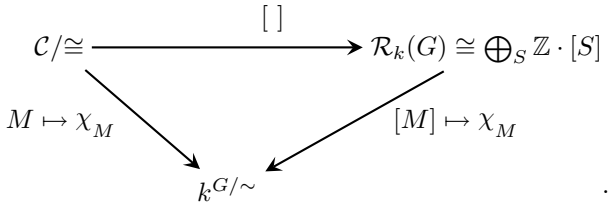
Bewijs. Zoals bekend is $\mathcal{R}(G) \cong \bigoplus_S \mathbb{Z}\cdot[S]$. Zij nu $[M] = \sum_S n_S\cdot[S] \in \mathcal{R}(G)$. Dan is $\psi([M]) = \sum_S n_S\chi_S$. Volgens stelling 10.7 zijn χ_S (voor $S \in \mathcal{S}$) lineair onafhankelijk over k. Dus, als $\sum_S n_S\chi_S = 0$ zijn alle n_S gelijk aan 0 (merk op dat hier nodig is dat char $k = 0$). Dit betekent dat ψ injectief is.

Omdat $\{[S] : S \in \mathcal{S}\}$ een $\mathbb{Z}$-basis voor $\mathcal{R}(G)$ is, is $\{[S]\otimes 1 : S \in \mathcal{S}\}$ een k-basis voor $\mathcal{R}/G\otimes_{\mathbb{Z}} k$. De karaktertafel van G geeft de matrixrepresentatie voor ψ' en is inverteerbaar. Hieruit volgt dat ψ' een isomorfisme is. □

Gevolg 10.9. *Elke centrale functie $f : G \to k$ is een unieke k-lineaire combinatie van de χ_S, waarbij S loopt over $\mathcal{S}$.*

Definitie 10.10. *Als $S \in \mathcal{S}$ heet χ_S een* irreducibel *karakter. De verzameling van irreducibele karakters van G schrijven we $X(G)$. Merk op dat $X(G) \cong \mathcal{S}$.*

Beschouw het volgende commutatieve diagram:



.

We beelden $k[G] \in \mathcal{C}$ op twee manieren via dit diagram af naar $k^{G/\sim}$.

Omdat $k[G] \cong_{k[G]} \prod_S \mathrm{End}_k(S)$, is $k[G] \cong \bigoplus_S S^{\dim_k S}$ als $k[G]$-moduul. Dus $[k[G]] = \sum_S(\dim_k S)[S]$. Hieruit volgt dat $\chi_{k[G]} = \sum_{\chi\in X(G)} \chi(1)\chi$.

De matrix die de afbeelding $k[G] \to k[G]$ gegeven door linksvermenigvuldiging met σ uitdrukt op de basis van alle $\tau \in G$ is $[m_{\rho,\tau}]_{\rho,\tau}$, met $m_{\rho,\tau} = 1$ als $\rho = \sigma\tau$ en anders $m_{\rho,\tau} = 0$. Het spoor van deze matrix is $\#G$ als $\sigma = 1$ en anders 0. Dit geeft ons dat

$$\chi_{k[G]}(\sigma) = \begin{cases}\#G \text{ als } \sigma = 1\\ 0 \text{ als } \sigma \neq 1.\end{cases}$$

Het gevolg hiervan is dat voor alle $\sigma \in G$ geldt dat

$$\sum_{\chi \in X(G)} \chi(1)\chi(\sigma) = \begin{cases} \#G \text{ als } \sigma = 1 \\ 0 \text{ als } \sigma \neq 1. \end{cases}$$

Voorbeeld
Zij $G = D_4 = \langle \rho, \sigma : \sigma^2 = \rho^4 = 1, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle$. We hebben al gezien dat $D_4^{\text{ab}} = D_4/\langle \rho^2 \rangle = V_4$. In een eerder voorbeeld hebben we ook de simpele $k[D_4]$-modulen bepaald: vier 1-dimensionale simpele modulen (S_0, S_1, S_2, S_3) en één 2-dimensionaal simpel moduul (S_4).

	1	σ	ρ	$\sigma\rho$	ρ^2
S_0	1	1	1	1	1
S_1	1	1	-1	-1	1
S_2	1	-1	1	-1	1
S_3	1	-1	-1	1	1
S_4	2	0	0	0	-2

Stelling 10.11. *Zij M een eindig voortgebracht $k[G]$-moduul en $\sigma \in G$. Dan is $\chi_M(\sigma)$ een som van $\dim_k(M)$ eenheidswortels waarvan de ordes $\text{orde}(\sigma)$ delen.*

Bewijs. Beschouw eerst het geval dat G abels is en M simpel. Dan is $\dim_k(M) = 1$, zodat $M = k_\chi$ voor een groepshomomorfisme $\chi : G \to k^*$. G is eindig, dus er is een m zodat $\sigma^m = 1$. Voor deze m geldt ook dat $\chi_M(\sigma)^m = 1$, dus $\chi_M(\sigma)$ is een eenheidswortel waarvan de orde m deelt.

Bekijk vervolgens het geval dat G abels is, maar M niet noodzakelijk simpel. Dan is $M = \bigoplus_{i=1}^t S_i$ met S_i simpel en $t = \dim_k(M)$. Dan is $\chi_M(\sigma) = \sum_{i=1}^t \chi_{S_i}(\sigma)$. Pas nu het eerste geval toe op $\chi_{S_i}(\sigma)$.

Het algemene geval volgt hieruit. Immers, beschouw M als $k[\langle\sigma\rangle]$-moduul. De sporen blijven dan onveranderd. □

Vanaf nu is $k = \mathbb{C}$ en G een eindige groep.

Stelling 10.12. *Zij M een eindig voortgebracht $k[G]$-moduul en $\sigma \in G$. Dan is $\chi_{M^\dagger}(\sigma) = \overline{\chi_M(\sigma)}$, waarbij $\overline{\ }$ complexe conjugatie is.*

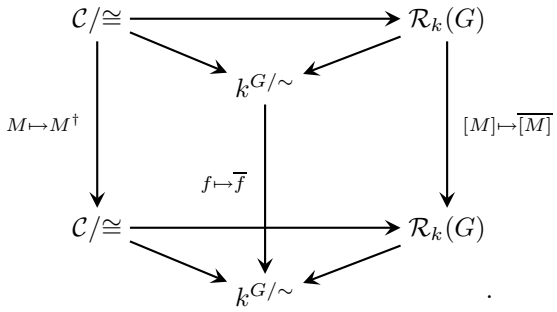
Bewijs. Als in het bewijs van stelling 10.11 reduceren we tot het geval waar G abels is en M simpel. Dan is weer $M = k_\chi$ voor een groepshomomorfisme $\chi : G \to k^*$.

Zij $f \in M^\dagger$. Dan $(\sigma f)(x) = f(\chi(\sigma)^{-1}x) = \chi(\sigma)^{-1}f(x)$ voor $x \in M$. Dus $\sigma f = \chi(\sigma)^{-1}f$ en $(k_\chi)^\dagger = k_{\chi^{-1}}$. Omdat $\chi_M(\sigma)$ een eenheidswortel is, geldt nu $\chi_{M^\dagger}(\sigma) = \chi_M(\sigma)^{-1} = \overline{\chi_M(\sigma)}$. □

Conclusie: als we

$$\begin{array}{rccl} \overline{\ } : k^{G/\sim} & \longrightarrow & k^{G/\sim} \\ f & \longmapsto & (\sigma \mapsto \overline{f(\sigma)}) \end{array}$$

definiëren, dan is $\overline{\ }$ een ringhomomorfisme van orde 2 en commuteert het volgende diagram:



Voorbeeld
Zij $G = C_3 \rtimes C_4$, waarbij $C_3 = \langle\tau\rangle$, $C_4 = \langle\sigma\rangle$ en $\sigma\tau\sigma^{-1} = \tau^{-1}$. De conjugatieklassen van G zijn $\{1\}$, $\{\tau, \tau^2\}$, $\{\sigma, \sigma\tau, \sigma\tau^2\}$, $\{\sigma^2\}$, $\{\sigma^2\tau\}$, $\{\sigma^3, \sigma^3\tau, \sigma^3\tau^2\}$.

Opmerking: het aantal elementen van de conjugatieklasse van $x \in G$ is gelijk aan $\#G/\#C_G(x)$. Hier is $C_G(x) := \{y \in G : xy = yx\}$ de *centralisator* van x.

$G^{\mathrm{ab}} = \langle\sigma\rangle$. Dus, we moeten $\#G = 12$ schrijven als som van zes kwadraten, waarvan vier enen: $12 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2 + 2^2$. Er zijn dus vier 1-dimensionale simpele modulen en twee 2-dimensionale. Omdat $G/\langle\sigma^2\rangle \cong C_3 \rtimes C_2 \cong S_3$, zijn de simpele S_3-modulen ook simpele G-modulen.

	1	τ	σ	σ^2	$\sigma^2\tau$	σ^3
	1	1	1	1	1	1
	1	1	i	-1	-1	$-i$
	1	1	-1	1	1	-1
	1	1	$-i$	-1	-1	i
	2	-1	0	2	-1	0
	2	-1	0	-2	1	0

Voor een paar $k[G]$-modulen M, N is $\mathrm{Hom}_{k[G]}(M, N)$ een k-vectorruimte. Dit induceert een bilineaire afbeelding

$$\begin{array}{rcl} \mathcal{R}(G) \times \mathcal{R}(G) & \longrightarrow & \mathbb{Z} \\ ([M], [N]) & \longmapsto & \dim_k \mathrm{Hom}_{k[G]}(M, N). \end{array}$$

Van de k-lineaire homomorfismen $\mathrm{Hom}_k(M, N)$ kunnen we een $k[G]$-moduul maken door $\sigma \in G$ te laten werken op $f \in \mathrm{Hom}_k(M, N)$ door $(\sigma f) : x \mapsto \sigma(f(\sigma^{-1}x))$. Dit geeft een afbeelding

$$\begin{array}{rcl} \mathcal{C}/\cong \times \mathcal{C}/\cong & \longrightarrow & \mathcal{C}/\cong \\ (M, N) & \longmapsto & \mathrm{Hom}_k(M, N). \end{array}$$

Lemma 10.13. *Zij R een commutatieve ring en M en N twee R-modulen. Neem aan dat M eindig voortgebracht en vrij is, dus $M \cong_R R^n$. Dan is de afbeelding*

$$\begin{array}{rcl} \mathrm{Hom}_k(M, R) \otimes_R N & \longrightarrow & \mathrm{Hom}_R(M, N) \\ f \otimes y & \longmapsto & (x \mapsto f(x)y) \end{array}$$

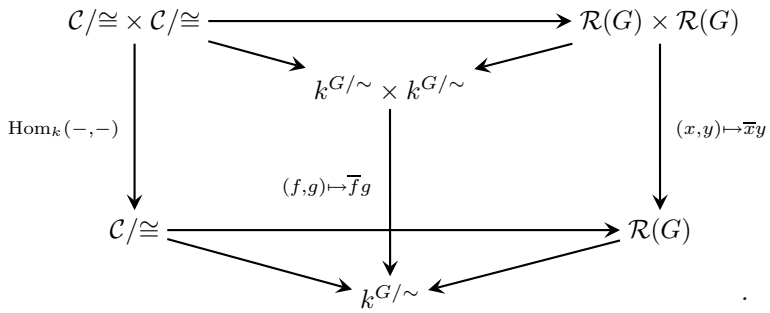
een isomorfisme van R-modulen.

Bewijs. Opgave. □

Gevolg 10.14. *Als M en N twee eindig voortgebrachte $k[G]$-modulen zijn, dan is* $\mathrm{Hom}_k(M,N) \cong_{k[G]} M^\dagger \otimes_k N$.

Bewijs. Het lemma geeft een k-lineair isomorfisme. Ga zelf na dat dit de G-actie respecteert. □

Gevolg 10.15. *Het volgende diagram commuteert:*



Lemma 10.16. *Als we van k een $k[G]$-moduul maken door G triviaal op k te laten werken, dan is*

$$\begin{array}{rcl} \mathrm{Hom}_k(k,N) & \longrightarrow & N \\ f & \longmapsto & f(1) \end{array}$$

een $k[G]$-lineair isomorfisme en

$$\begin{array}{rcl} \mathrm{Hom}_{k[G]}(k,N) & \longrightarrow & N^G = \{y \in N : \forall \sigma \in G : \sigma y = y\} \\ f & \longmapsto & f(1) \end{array}$$

een k-lineair isomorfisme. Ook is $\dim_k N^G = \frac{1}{\#G} \sum_{\sigma \in G} \chi_N(\sigma)$.

Bewijs. Ga zelf na dat de gegeven afbeeldingen welgedefinieerde isomorfismen zijn.

Definieer $\varphi = \sum_{\sigma \in G} (\#G)^{-1} \sigma \in k[G]$. Dan geldt voor alle $\tau \in G$ dat $\tau\varphi = \varphi$. Ga zelf na dat φ een exacte rij van k-modulen $0 \to \ker\varphi \to N \xrightarrow{\varphi} N^G \to 0$ induceert en dat de inclusie $N^G \subset N$ een splitsing van deze rij geeft.

Dit betekent dat $N \cong_k N^G \oplus \ker\varphi$. Omdat φ als de identiteit werkt op N^G en als 0 op $\ker\varphi$, is het spoor van de actie van φ op N gelijk aan $\dim_k N^G$. Uit de definitie van φ volgt dat het spoor van de actie van φ op N ook gelijk is aan $\frac{1}{\#G} \sum_{\sigma \in G} \chi_N(\sigma)$. □

Stelling 10.17. *Als M, N eindig voortgebrachte $k[G]$-modulen zijn, dan is*

$$\dim_k \mathrm{Hom}_{k[G]}(M,N) = \frac{1}{\#G} \sum_{\sigma \in G} \chi_M(\sigma)\overline{\chi_N(\sigma)}.$$

Bewijs. Uit lemma 10.16 volgt dat

$$(\mathrm{Hom}_k(M,N))^G = \{f \in \mathrm{Hom}_k(M,N) : \forall \sigma \in G : \sigma f = f\} = \mathrm{Hom}_{k[G]}(M,N).$$

Hieruit volgt dat

$$\dim_k \mathrm{Hom}_{k[G]}(M,N) = \frac{1}{\#G}\sum_{\sigma\in G}\chi_{\mathrm{Hom}_k(M,N)}(\sigma) = \frac{1}{\#G}\sum_{\sigma\in G}\overline{\chi_M(\sigma)}\chi_N(\sigma).$$

□

We definiëren $\langle [M],[N]\rangle = \frac{1}{\#G}\sum_{\sigma\in G}\chi_M(\sigma)\overline{\chi_N(\sigma)}$. Uit stelling 10.17 volgt dat we nu de bilineaire afbeelding van $\mathcal{R}(G)\times\mathcal{R}(G)\to\mathbb{Z}$ kunnen herformuleren als

$$\begin{array}{rcl}\mathcal{R}(G)\times\mathcal{R}(G) & \longrightarrow & \mathbb{Z}\\ ([M],[N]) & \longmapsto & \dim_k \mathrm{Hom}_{k[G]}(M,N) = \langle [M],[N]\rangle.\end{array}$$

Als we voor $f,g\in k^{G/\sim}$ analoog $\langle f,g\rangle = \frac{1}{\#G}\sum_{\sigma\in G} f(\sigma)\overline{g(\sigma)}$ definiëren, krijgen we het volgende commutatieve diagram:

$$\begin{array}{ccc}\mathcal{R}(G)\times\mathcal{R}(G) & \xrightarrow{\langle -,-\rangle} & \mathbb{Z}\\ \downarrow & & \downarrow\\ k^{G/\sim}\times k^{G/\sim} & \xrightarrow[\langle -,-\rangle]{} & k.\end{array}$$

Merk op dat als S, S' simpele modulen zijn, $\langle [S],[S']\rangle$ gelijk is aan 1 als $[S]=[S']$, en 0 anders. Eveneens geldt voor irreducibele karakters χ, ψ dat $\langle\chi,\psi\rangle$ gelijk is aan 1 als $\chi=\psi$, en 0 anders.

Als $M=\sum_{S\in\mathcal{S}} n_S[S]$ met $n_S\in\mathbb{Z}$, $n_S\geq 0$, dan is $\langle [M],[M]\rangle = \sum_S n_S^2$. Dus: als M een eindig voortgebracht $k[G]$-moduul is, is M irreducibel dan en slechts dan als $\langle [M],[M]\rangle = 1$, of, equivalent, als $\langle\chi_M,\chi_M\rangle = 1$.

Lemma 10.18. *Zij $f\in k^{G/\sim}$. Er is een eindig voortgebracht $k[G]$-moduul M met $f=\chi_M$ dan en slechts dan als $\forall\chi\in X(G):\langle f,\chi\rangle\in\mathbb{Z}_{\geq 0}$.*

Bewijs. Schrijf $f=\sum_{\chi\in X(G)} a_\chi\chi$, met $a_\chi\in k$. Dan geldt voor alle $\psi\in X(G)$ dat $\langle f,\psi\rangle = \sum_\chi a_\chi\langle\chi,\psi\rangle = a_\psi$.

Stel nu dat $\forall\psi\in X(G):\langle f,\psi\rangle\in\mathbb{Z}_{\geq 0}$. Definieer $M:=\bigoplus_{S\in\mathcal{S}} S^{\langle f,\chi_S\rangle}$. Dan geldt dat $\chi_M=\sum_S\langle f,\chi_S\rangle\chi_S = f$.

Omgekeerd, als $M=\bigoplus_S S^{n_S}$, dan is $\chi_M=\sum_S n_S\chi_S=\sum_S\langle f,\chi_S\rangle\chi_S$. □

Stelling 10.19. *Voor $\sigma,\tau\in G$ geldt:*

$$\sum_{\chi\in X(G)}\chi(\sigma)\overline{\chi(\tau)} = \begin{cases}\frac{\#G}{\#[\sigma]} = \#C_G(\sigma) & \text{als } \sigma\sim\tau\\ 0 \quad \text{als } \sigma\not\sim\tau.\end{cases}$$

Bewijs. Definieer $A=[\chi(\sigma)]_{\substack{\chi\in X(G)\\ \sigma\in G/\sim}}$ en $B=[\chi(\sigma)\sqrt{\#[\sigma]}]_{\substack{\chi\in X(G)\\ \sigma\in G/\sim}}$

Dan is

$$B\overline{B^T} = \left[\sum_{\sigma\in G/\sim} \#[\sigma]\chi(\sigma)\overline{\psi(\sigma)}\right]_{\chi,\psi\in X(G)} = \#G\cdot I,$$

omdat alle elementen buiten de diagonaal nul zijn en de elementen op de diagonaal $\#[\sigma]$.

Merk op dat een gevolg hiervan is dat $|\det A|^2 = \prod_{\sigma\in G/\sim} \frac{\#G}{\#[\sigma]} = \prod_\sigma \#C_G(\sigma)$.

We weten dus nu dat $B^{-1} = \frac{1}{\#G}\overline{B^T}$, en dus dat $B^T\overline{B} = \#G\cdot I$.

Dus:

$$\begin{aligned} \#G\cdot I = B^T\overline{B} &= \left[\sum_{\chi\in X(G)} \sqrt{\#[\sigma]\#[\tau]}\chi(\sigma)\overline{\chi(\tau)}\right]_{\sigma,\tau\in G/\sim} \\ &= \left[\sqrt{\#[\sigma]\#[\tau]}\sum_{\chi\in X(G)} \chi(\sigma)\overline{\chi(\tau)}\right]_{\sigma,\tau\in G/\sim.} \end{aligned}$$

De elementen op de diagonaal zijn $\#[\sigma]$ en alle elementen buiten de diagonaal zijn 0. Hieruit volgt de stelling. □

11 Geheelheid en de stelling van Burnside

Lemma 11.1. *Stel A is een commutatieve ring, M is een eindig voortgebracht A-moduul en $\varepsilon \in \mathrm{End}_A(M)$. Dan is er een monisch polynoom $f \in A[X]$ zodat $f(\varepsilon) = 0$ (dat wil zeggen, als $f = \sum a_i X^i$, dan $\sum a_i\varepsilon^i(m) = 0$ voor alle $m \in M$).*

Bewijs. Maak van M een $A[X]$-moduul door $(\sum b_i X^i)\cdot m = \sum b_i\varepsilon^i(m)$ voor $\sum b_i X^i \in A[X]$ en $m \in M$. (Ga zelf na dat dit inderdaad een $A[X]$-moduulstructuur geeft.)

Schrijf $M = \sum_{i=1}^n Am_i$ voor $m_1, \ldots, m_n \in M$.

Bewering: $\forall l \in \{0, 1, \ldots, n\}\exists f \in A[X]$ monisch : $\forall m \in M\exists g_1, \ldots, g_l \in A[X]$: $\deg g_i < \deg f$ en $f\cdot m = \sum g_i m_i$.

Bewijs van de bewering: Als $l = n$, neem $f = X$. Dan is $X\cdot m = \varepsilon(m) = \sum b_i m_i$. Neem dus $g_i = b_i$.

Stel de bewering is waar voor $l > 0$. We bewijzen dat hij ook waar is voor $l - 1$.

Er bestaan f en h_i zodanig dat $f\cdot m_l = \sum_{i=1}^l h_i\cdot m_i$ met $h_i \in A[X]$ en $\deg h_i < \deg f$.

Dus: $(f - h_l)\cdot m_l = \sum_{i=1}^{l-1} h_i\cdot m_i$. Merk op dat $f - h_l$ een monisch polynoom van dezelfde graad als f is.

Zij nu $m \in M$ willekeurig. We weten dat er g_i bestaan zodat $f\cdot m = \sum_{i=1}^l g_i\cdot m_i$.

Dan geldt:

$$\begin{aligned}(f-h_l)f\cdot m &= \left(\sum_{i=1}^{l-1}(f-h_l)g_i\cdot m_i\right)+g_l(f-h_l)\cdot m_l\\ &= \left(\sum_{i=1}^{l-1}(f-h_l)g_i\cdot m_i\right)+\left(\sum_{i=1}^{l-1}g_lh_i\cdot m_i\right)\\ &= \sum_{i=1}^{l-1}((f-h_l)g_i+g_lh_i)\cdot m_i.\end{aligned}$$

Voor $f' := (f-h_l)f$ en $g_i' := (f-h_l)g_i + g_lh_i$ geldt nu de bewering voor $l-1$.

Hieruit volgt uiteindelijk dat de bewering geldt voor $l=0$ en hieruit volgt direct het lemma. □

Definitie 11.2. *Een R-moduul M heet* trouw *als $\forall r\in R, r\neq 0 \exists m\in M : rm\neq 0$, of, met andere woorden, als de afbeelding $R\to \mathrm{End}_{\mathbb{Z}}(M)$ gegeven door $r\mapsto (m\mapsto rm)$ injectief is.*

Stelling 11.3. *Stel $A\subset B$ zijn commutatieve ringen en $\alpha\in B$. Dan zijn de volgende eigenschappen equivalent:*

1. *Er bestaat een monisch polynoom $f\in A[X]$ met $f(\alpha)=0$.*
2. *De deelring $A[\alpha]\subset B$ is eindig voortgebracht als A-moduul.*
3. *Er is een deelring $C\subset B$ met $A\subset C$, $\alpha\in C$ en C eindig voortgebracht als A-moduul.*
4. *Er is een trouw $A[\alpha]$-moduul M dat eindig voortgebracht is als A-moduul.*

Definitie: *Als deze eigenschappen waar zijn, heet α* geheel *over A.*

Bewijs. (1) $\Rightarrow$ (2): Stel $f = X^n + \sum_{i=0}^{n-1} a_iX^i \in A[X]$ voldoet aan $f(\alpha)=0$. Definieer $C := \sum_{i=0}^{n-1}\alpha^iA$. Dan is $\alpha^n\in C\subset A[\alpha]$. Merk op dat C een eindig voortgebracht A-moduul is.

Omdat $\alpha-\alpha^j\in C$ voor $0\leq j\leq n-1$, geldt $\alpha C\subset C$. Dus voor alle $j\geq 0$ geldt dat $\alpha^jC\subset C$, dus $A[\alpha]C\subset C$ en $A[\alpha]=C$. In het bijzonder is $A[\alpha]$ dus eindig voortgebracht als A-moduul.

(2) $\Rightarrow$ (3): Neem $C=A[\alpha]$.

(3) $\Rightarrow$ (4): Neem $M=C$. $A[\alpha]\subset C$, dus C is een $A[\alpha]$-moduul. Zij $r\in A[\alpha]$, $r\neq 0$. Dan is $1r\neq 0$, dus M is trouw.

(4) $\Rightarrow$ (1): Pas lemma 11.1 toe op $\varepsilon : m\mapsto \alpha m$. Dan is er een monisch polynoom $f\in A[X]$ zodanig dat $(m\mapsto f(\alpha)m)=0$. Omdat M trouw is, geldt nu dat $f(\alpha)=0$. □

Zij $A\subset B$ commutatieve ringen.

Definitie 11.4. *B is* geheel *over A als elk element van B geheel is over A.*

Definitie 11.5. *A heet* geheel afgesloten *in B als geen enkele $\alpha \in B \setminus A$ geheel is over A.*

Stelling 11.6. *Zij A een ontbindingsring. Dan is A geheel afgesloten.*

Bewijs. Stel $\alpha \in Q(A)$ is geheel over A. Schrijf $a = \frac{u}{v}$ met $u, v \in A$ zodanig dat u en v geen priemfactor gemeen hebben.

Kies $a_i \in A$ zodanig dat $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Dan is $a_{n-1}u^{n-1}v + a_{n-2}^{n-2}v^2 + \ldots + a_0 v^n = -u^n$. Dus $v|u^n$. Hieruit volgt dat $v \in A^*$ en $\alpha \in A$. □

Lemma 11.7. *Als $A \subset C$ ringen zijn zodat C eindig voortgebracht is als A-moduul, en M is een eindig voortgebracht C-moduul, dan is ook M eindig voortgebracht als A-moduul.*

Bewijs. Omdat C eindig voortgebracht is als A-moduul, bestaan er een $n \in \mathbb{Z}_{>0}$ en een surjectief A-lineair homomorfisme $A^n \to C$. Zo bestaan er ook een $m \in \mathbb{Z}_{>0}$ en een surjectief C-lineair homomorfisme $C^m \to M$. Dus bestaat er ook een surjectief A-lineair homomorfisme $A^{nm} \to C^m \to M$. □

Stelling 11.8. *Stel $A \subset B$ zijn commutatieve ringen. Dan is de gehele afsluiting van A in B een deelring van B die A omvat en die geheel afgesloten is in B.*

Bewijs. Definieer $D := \{\alpha \in B : \alpha \text{ is geheel over } A\}$, de gehele afsluiting van A in B. Het is duidelijk dat $A \subset D$.

We willen bewijzen dat als $\alpha, \beta \in D$, dan ook $\alpha\beta$, $\alpha - \beta \in D$. Zij α en β willekeurig gegeven elementen van D. Omdat α geheel is over A, geldt dat $A[\alpha]$ een eindig voortgebracht A-moduul is. Omdat β geheel is over A is β ook geheel over $A[\alpha]$, dus $A[\alpha][\beta] = A[\alpha, \beta]$ is een eindig voortgebracht $A[\alpha]$-moduul. Nu gebruiken we lemma 11.7 met $C = A[\alpha]$, $M = A[\alpha, \beta]$ en we vinden dat $A[\alpha, \beta]$ ook eindig voortgebracht is als A-moduul. Het is duidelijk dat $\alpha\beta$ en $\alpha - \beta$ bevat zijn in $A[\alpha, \beta]$. Uit stelling 11.3, deel 3 volgt nu dat $\alpha\beta$ en $\alpha - \beta$ geheel zijn over A, dus bevat zijn in D.

Er rest nog te bewijzen: als $\beta \in B$ geheel is over D, dan $\beta \in D$. Zij $\beta \in B$ een willekeurig gegeven element dat geheel is over D. Dan bestaat er een polynoom $g = X^t + \alpha_{t-1}X^{t-1} + \ldots + \alpha_1 X + \alpha_0 \in D[X]$ dat monisch is en waarvoor geldt dat $g(\beta) = 0$. We hebben nu de volgende keten van ringen: $A \subset A[\alpha_0] \subset A[\alpha_0, \alpha_1] \subset \ldots \subset A[\alpha_0, \alpha_1, \ldots, \alpha_{t-1}] =: D'$. Elke ring ongelijk aan A in deze keten is eindig voortgebracht als moduul over de vorige, want de nieuwe α_i is geheel over A en dus ook over $A[\alpha_0, \ldots, \alpha_{i-1}]$. Lemma 11.7 impliceert nu dat D' eindig voortgebracht is als A-moduul. Omdat β geheel is over D is β geheel over D', dus $D'[\beta]$ is eindig voortgebracht als D'-moduul. Pas nu weer stelling 11.3, deel 3 toe (met $C = D'[\beta]$) en we vinden dat β geheel is over A. □

Notatie: We noteren de gehele afsluiting van $\mathbb{Z}$ in $\mathbb{C}$ door $\overline{\mathbb{Z}}$. Stel dat $a, b \in \mathbb{C}$. We schrijven $b|a$ ("b deelt a") als $a \in \overline{\mathbb{Z}}b$.

Merk op dat $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Als $c|b$ en $b|a$, dan geldt ook $c|a$. Als $b|a_1$ en $b|a_2$, dan geldt ook $b|a_1 \pm a_2$.

Zij G een eindige groep.

Stelling 11.9. *Als M een eindig voortgebracht $\mathbb{C}[G]$-moduul is, dan geldt $\chi_M(\sigma) \in \overline{\mathbb{Z}}$ voor alle $\sigma \in G$.*

Bewijs. Zij $n = \dim_{\mathbb{C}} M$. Dan is $\chi_M(\sigma)$ een som van n eenheidswortels. Elke eenheidswortel is een nulpunt van een polynoom van de vorm $X^m - 1$, dus elke eenheidswortel behoort tot $\overline{\mathbb{Z}}$. Er volgt dus dat $\chi_M(\sigma) \in \overline{\mathbb{Z}}$. □

Voorbeeld
$i \in \overline{\mathbb{Z}}$, want i is een eenheidswortel.

$\frac{i}{2} \notin \overline{\mathbb{Z}}$, want als $\frac{i}{2}$ bevat zou zijn in $\overline{\mathbb{Z}}$, dan zou ook $(-i)\frac{i}{2} = \frac{1}{2} \in \overline{\mathbb{Z}}$ en dat is niet het geval omdat $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

Voorbeeld
Als $\alpha \in \mathbb{C}$ algebraïsch is over $\mathbb{Q}$, dan geldt: $\alpha \in \overline{\mathbb{Z}} \Leftrightarrow f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[X]$.

Bewijs. $\Leftarrow$: Duidelijk. $\Rightarrow$: Opgave. □

Lemma 11.10. *Stel $t \in \mathbb{Z}_{>0}$ en $\eta_1, \ldots, \eta_t \in \mathbb{C}$ zijn eenheidswortels. Schrijf $s = \eta_1 + \ldots + \eta_t$ en neem aan $s \neq 0$. Dan zijn de volgende uitspraken equivalent:*

1. *$t|s$.*
2. *Alle η_i zijn gelijk aan elkaar.*
3. *$|s| = t$.*
4. *$|s| \geq t$.*

Bewijs. (2) $\Rightarrow$ (1): Triviaal: $\frac{s}{t} = \eta_1 \in \overline{\mathbb{Z}}$.

(4) $\Rightarrow$ (3) $\Rightarrow$ (2): Als $a, b \in \mathbb{C}$ dan geldt $|a + b| \leq |a| + |b|$, en gelijkheid geldt dan en slechts dan als $\mathbb{R}_{>0} \cdot a = \mathbb{R}_{>0} \cdot b$ (d.w.z.: de vector van 0 tot a loopt in dezelfde richting als de vector van 0 tot b). Dan geldt dus ook voor $a_1, \ldots, a_t \in \mathbb{C}^*$ dat $|\sum_{i=1}^t a_i| \leq \sum_{i=1}^t |a_i|$, en gelijkheid geldt dan en slechts dan als alle vectoren van 0 tot a_i dezelfde richting hebben.

We passen dit toe met $a_i = \eta_i$. Voor $i = 1, \ldots, t$ is η_i een eenheidswortel, dus $|\eta_i| = 1$. Nu volgt dat $|s| = |\sum_{i=1}^t \eta_i| \leq \sum_{i=1}^t |\eta_i| = t$, en $|s| = t$ dan en slechts dan als alle vectoren van 0 tot η_i gelijk zijn, dus als alle η_i gelijk zijn.

Bewering (4) zegt dat $|s| \geq t$, dus we vinden dat $|s| = t$ (bewering (3)) en dus $\eta_1 = \ldots = \eta_t$ (bewering (2)).

(1) $\Rightarrow$ (4): Het "bewijs" dat het meest voor de hand zou liggen is fout (en dus geen bewijs). Dit "bewijs" zou er als volgt uitzien: als $t|s$ dan $\frac{s}{t} \in \overline{\mathbb{Z}}$, *dus* $\left|\frac{s}{t}\right| \geq 1$ en daarom $|s| \geq t$. De fout zit in het cursief gedrukte *dus*, want niet elk element van $\overline{\mathbb{Z}}$ ongelijk aan 0 heeft absolute waarde ≥ 1. Ook sommen van eenheidswortels hoeven niet absolute waarde ≥ 1 te hebben (het is bijvoorbeeld duidelijk te zien dat $|\zeta_5 + \zeta_5^4| < 1$, waarbij $\zeta_5 = e^{\frac{2\pi}{5}}$).

Definieer $K = \mathbb{Q}(\eta_1, \ldots, \eta_t)$. Het is duidelijk dat $s = \sum_{i=1}^{t} \eta_i \in K$. K is Galois over $\mathbb{Q}$ met Galois-groep $\mathrm{Gal}(K/\mathbb{Q})$. Voor $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ geldt: $\sigma(s) = \sum_{i=1}^{t} \sigma(\eta_i)$, waarbij $\sigma(\eta_i)$ voor alle i weer een eenheidswortel is, dus $0 < |\sigma(s)| \leq t$.

Omdat $\frac{s}{t}$ geheel is over $\mathbb{Z}$, is $\sigma(\frac{s}{t}) = \frac{\sigma(s)}{t}$ ook geheel over $\mathbb{Z}$. Er geldt nu: $\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \frac{\sigma(s)}{t} \in \overline{\mathbb{Z}}$. Ook weten we dat $\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \frac{\sigma(s)}{t} \in \mathbb{Q}$, want voor alle $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ geldt dat $\tau\left(\prod_\sigma \frac{\sigma(s)}{t}\right) = \prod_\sigma \frac{\sigma(s)}{t}$. Omdat $s \neq 0$ is ook $\sigma(s) \neq 0$ en we vinden dat $0 \neq \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \frac{\sigma(s)}{t} \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Dus $\left|\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \frac{\sigma(s)}{t}\right| \geq 1$. Er geldt dus dat $\left|\frac{s}{t}\right| = \prod_{\sigma \neq 1} \left|\frac{t}{\sigma(s)}\right| \geq 1$. □

Stelling 11.11. *Stel G is een eindige groep, M is een eindig voortgebracht $\mathbb{C}[G]$-moduul en $\sigma \in G$. We zeggen dat een element $\tau \in G$* als een scalar *op M werkt als $\exists c \in \mathbb{C} : \forall x \in M : \sigma(x) = cx$. De volgende equivalenties gelden:*

1. *σ werkt triviaal op $M \iff \chi_M(\sigma) = \dim_{\mathbb{C}} M$.*
2. *σ werkt als een scalar op $M \iff |\chi_M(\sigma)| = \dim_{\mathbb{C}} M$; als $M \neq 0$ is dit equivalent met: $\dim_{\mathbb{C}} M | \chi_M(\sigma)$.*

Bewijs. We mogen aannemen dat $G = \langle\sigma\rangle$, dus in het bijzonder mogen we aannemen dat G abels is. Nu geldt dus dat M een directe som is van één-dimensionale $\mathbb{C}[G]$-modulen, σ werkt als de matrix

$$\begin{pmatrix} \eta_1 & 0 & \ldots & 0 \\ 0 & \eta_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \eta_t \end{pmatrix},$$

waarbij $\eta_1, \ldots, \eta_t$ eenheidswortels zijn en $t = \dim_{\mathbb{C}} M$.

1. $\Rightarrow$: Triviaal.

$\Leftarrow$: Uit $\chi_M(\sigma) = \dim_{\mathbb{C}} M$ volgt dat $\eta_1 + \ldots + \eta_t = t$. Lemma 11.10 vertelt ons nu dat $\eta_1 = \ldots = \eta_t = 1$, dus σ werkt als de identiteitsmatrix, dus triviaal. (Merk op: *(1)* klopt ook als $M = 0$.)

2. Merk op dat de eerste equivalentie geldt als $M = 0$. Neem nu aan dat $M \neq 0$. $\Rightarrow$: Als σ als c werkt, dan is c een eenheidswortel. Dus $\chi_M(\sigma) = ct$, dus $|\chi_M(c)| = |ct| = t$.

$\Leftarrow$: $|\eta_1 + \ldots + \eta_t| = t$. Lemma 11.10 geeft dat alle η_i gelijk zijn, zeg c. Dan werkt σ als c.

Het bewijs van de laatste equivalentie gaat hetzelfde, met bewering 1 uit lemma 11.10. □

Definieer $N := \ker(G \to \mathrm{Aut}_{\mathbb{C}} M)$, de verzameling elementen van G die triviaal op M werken, en $H := \ker(G \to (\mathrm{Aut}_{\mathbb{C}} M)/\mathbb{C}^*)$, de verzameling elementen van G die als een scalar op M werken. De situatie ziet er nu als volgt uit: $N \subset H \subset G$, en N en H zijn allebei normaal in G.

Definitie 11.12. *Voor een $\mathbb{C}[G]$-moduul M en $u \in \mathbb{C}[G]$ is $\chi_M(u)$ het spoor van de actie van u op M; dus $\chi_M : \mathbb{C}[G] \to \mathbb{C}$ is $\mathbb{C}$-lineair.*

Lemma 11.13. *Stel dat $A \subset B_1$ en $A \subset B_2$ commutatieve ringen zijn en bed A in $B_1 \times B_2$ in door $a \mapsto (a, a)$. Dan geldt: een element $(b_1, b_2) \in B_1 \times B_2$ is geheel over A dan en slechts dan als b_1 en b_2 geheel zijn over A.*

Bewijs. Ga dit zelf na. □

Stelling 11.14. *Zij G een eindige groep en $u \in Z(\mathbb{C}[G])$. Dan geldt:*

$$\begin{aligned} u \in \overline{\mathbb{Z}}[G] &\implies u \text{ is geheel over } \mathbb{Z} \\ &\iff \text{voor alle } \chi \in X(G) \text{ geldt } \chi(1)|\chi(u). \end{aligned}$$

Bewijs. $\Rightarrow$: Definieer $B := \overline{\mathbb{Z}}[G] \cap Z(\mathbb{C}[G]) = \bigoplus_{C \in G/\sim} \overline{\mathbb{Z}} \sum_{\sigma \in G} \sigma$. B is eindig voortgebracht als $\overline{\mathbb{Z}}$-moduul dus elk element van B is geheel over $\overline{\mathbb{Z}}$. Omdat $\overline{\mathbb{Z}}$ geheel is over $\mathbb{Z}$, is B ook geheel over $\mathbb{Z}$.

$\Leftarrow$: De gehele afsluiting van $\mathbb{Z}$ in $Z(\mathbb{C}[G])$ is isomorf met de gehele afsluiting van $\mathbb{Z}$ in $\prod_\chi \mathbb{C}$ volgens het isomorfisme gegeven door $u \mapsto \left(\frac{\chi(u)}{\chi(1)}\right)_{\chi \in X(G)}$. Volgens lemma 11.13 is de gehele afsluiting van $\mathbb{Z}$ in $\prod_\chi \mathbb{C}$ gelijk aan $\prod_\chi \overline{\mathbb{Z}}$. Dus we vinden: u is geheel over $\mathbb{Z} \Leftrightarrow \forall \chi \in X(G) : \frac{\chi(u)}{\chi(1)} \in \overline{\mathbb{Z}}$. □

Stelling 11.15. *Voor elke $\chi \in X(G)$ geldt $\chi(1)|\#G$.*

Bewijs. Neem $u = \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma \in \mathbb{C}[G]$. Er geldt dat $\chi(\sigma^{-1}) = \chi(\tau^{-1})$ als $\sigma \sim \tau$, dus $u \in Z(\mathbb{C}[G])$. Omdat alle $\chi(\sigma^{-1}) \in \overline{\mathbb{Z}}$ geldt $u \in \overline{\mathbb{Z}}[G]$. Uit stelling 11.14 volgt nu dat $\chi(1)|\chi(u)$. Verder weten we dat $\chi(u) = \sum_{\sigma \in G} \chi(\sigma)\overline{\chi(\sigma)}$. Omdat χ een irreducibel karakter is, weten we dat $\frac{1}{\#G} \sum_{\sigma \in G} \chi(\sigma)\overline{\chi(\sigma)} = 1$, dus $\sum_{\sigma \in G} \chi(\sigma)\overline{\chi(\sigma)} = \#G$. We vinden dat $\chi(1)|\#G$. □

Stelling 11.16. *Voor elke $\chi \in X(G)$ en elke $\sigma \in G$ geldt $\chi(1)|\#[\sigma]\chi(\sigma)$. (Met $[\sigma]$ bedoelen we de conjugatieklasse van σ.)*

Bewijs. Neem $u = \sum_{\substack{\tau \in G \\ \tau \sim \sigma}} \tau \in \mathbb{C}[G]$. Er geldt dat $u \in Z(\mathbb{C}[G])$ en $u \in \overline{\mathbb{Z}}[G]$. Uit stelling 11.14 volgt nu dat $\chi(1)|\chi(u) = \#[\sigma]\chi(\sigma)$. □

Stelling 11.17. *Stel $\chi \in X(G)$ en $\sigma \in G$ voldoen aan $\gcd(\chi(1), \#[\sigma]) = 1$. Dan geldt òf $\chi(\sigma) = 0$ òf σ werkt als een scalar op het bij χ behorende simpele $\mathbb{C}[G]$-moduul S. In het laatste geval werkt $\sigma\tau^{-1}$ als de identiteit op S voor elke $\tau \in G$ die geconjugeerd is met σ.*

Bewijs. Schrijf $\chi = \chi_S$. Dan is $\chi(1) = \dim_{\mathbb{C}} S = t$. Er geldt dat $\chi(1)|\#[\sigma]\chi(\sigma)$ en $\chi(1)|\chi(1)\chi(\sigma)$. Omdat $\gcd(\chi(1), \#[\sigma]) = 1$ bestaan er gehele getallen l en m zodanig dat $l\#[\sigma] + m\chi(1) = 1$. We weten nu dat $\chi(1)|l\#[\sigma]\chi(\sigma)$ en $\chi(1)|m\chi(1)\chi(\sigma)$. Dus $\chi(1)|l\#[\sigma]\chi(\sigma) + m\chi(1)\chi(\sigma) = \chi(\sigma)$. Dus $t = \chi(1)|\chi(\sigma)$. Uit lemma 11.10 volgt dat òf $\chi(\sigma) = 0$ òf $\chi(\sigma) = t\eta$, voor een eenheidswortel η. In het laatste geval werkt σ als η. Als τ geconjugeerd is met σ werkt ook τ als η, dus $\sigma\tau^{-1}$ werkt als 1. □

Stelling 11.18 (Burnside). *Stel G is een eindige groep en $\sigma \in G$ is zo dat $\#[\sigma] = p^m$, met p priem en $m \in \mathbb{Z}_{>0}$. Dan is de ondergroep $N = \langle \sigma\tau^{-1} : \tau \in [\sigma] \rangle$ een normaaldeler van G met $\{1\} \subset N \subset G$, met N niet gelijk aan $\{1\}$ of G.*

Bewijs. Als $\rho \in G$ dan geldt:

$$\rho\sigma\tau^{-1}\rho^{-1} = \rho\sigma\rho^{-1}\sigma^{-1}\sigma(\rho\tau\rho^{-1})^{-1} = (\sigma(\rho\sigma\rho^{-1})^{-1})^{-1}\sigma(\rho\tau\rho^{-1})^{-1} \in N.$$

Dus N is een normale ondergroep en $N \neq \{1\}$ omdat $\#[\sigma] > 1$. Er geldt $\sigma \neq 1$, dus $\sum_{\chi \in X(G)} \chi(1)\chi(\sigma) = 0$. Dan $\sum_{\substack{\chi \in X(G) \\ \chi \neq 1}} \chi(1)\chi(\sigma) = -1$. Dus p is geen deler van $\sum_{\substack{\chi \in X(G) \\ \chi \neq 1}} \chi(1)\chi(\sigma)$. Kies $\chi \neq 1$ met $p \nmid \chi(1)\chi(\sigma)$. Er bestaat een simpel $\mathbb{C}[G]$-moduul S zodanig dat $\chi = \chi_S$. Omdat $\chi \neq 1$ werkt χ niet triviaal op S. Er geldt $p \nmid \chi(1)$, dus $\gcd(\chi(1), \#[\sigma]) = 1$. Uit $p \nmid \chi(1)\chi(\sigma)$ volgt dat $\chi(\sigma) \neq 0$, dus stelling 11.17 impliceert dat $\sigma\tau^{-1}$ als 1 werkt op S voor alle $\tau \in [\sigma]$. Dus N werkt *wel* triviaal op S. Dus $N \neq G$. □

Stelling 11.19 ("Stelling van Burnside" of "p^aq^b-Stelling"). *Als G een eindige groep is en het aantal priemgetallen dat $\#G$ deelt is ten hoogste twee, dan is G oplosbaar.*

Bewijs. We hebben al gezien dat deze stelling een gevolg is van stelling 11.18. □

12 De restrictie-afbeelding en de stelling van Frobenius

Stel G_1 en G_2 zijn groepen. Zij $\varphi : G_1 \to G_2$ een groepshomomorfisme. Dan is er een geïnduceerd ringhomomorfisme

$$\begin{array}{ccc} \mathbb{C}[G_1] & \longrightarrow & \mathbb{C}[G_2] \\ \displaystyle\sum_{\sigma \in G_1}^{<\infty} a_\sigma \sigma & \longmapsto & \displaystyle\sum_{\sigma \in G_1}^{<\infty} a_\sigma \varphi(\sigma) = \sum_{\tau \in G_2} \left(\sum_{\sigma \in \varphi^{-1}(\tau)} a_\sigma \right) \tau. \end{array}$$

(Ga zelf na dat dit een ringhomomorfisme is.)

Elk $\mathbb{C}[G_2]$-moduul M wordt nu een $\mathbb{C}[G_1]$-moduul door de samenstelling $G_1 \xrightarrow{\varphi} G_2 \longrightarrow \mathrm{Aut}_{\mathbb{C}} M$, of, equivalent, $rx = \varphi(r)x$ voor $r \in \mathbb{C}[G_1]$, $x \in M$ en φ het geïnduceerde ringhomomorfisme. Als er verwarring mogelijk is, noteren we het zo ontstane $\mathbb{C}[G_1]$-moduul als $\varphi^* M$.

Vanaf nu nemen we aan dat de groepen G_1 en G_2 eindig zijn.

We hebben de volgende inbeddingen:

$$\{\text{e.v. } \mathbb{C}[G_2]\text{-modulen}\}/\cong_{\mathbb{C}[G_2]} \hookrightarrow \mathcal{R}_{\mathbb{C}}(G_2) \hookrightarrow \mathcal{R}_{\mathbb{C}}(G_2) \otimes_{\mathbb{Z}} \mathbb{C} \cong \mathbb{C}^{G_2/\sim}$$

$$\{\text{e.v. } \mathbb{C}[G_1]\text{-modulen}\}/\cong_{\mathbb{C}[G_1]} \hookrightarrow \mathcal{R}_{\mathbb{C}}(G_1) \hookrightarrow \mathcal{R}_{\mathbb{C}}(G_1) \otimes_{\mathbb{Z}} \mathbb{C} \cong \mathbb{C}^{G_1/\sim}.$$

We zullen van links naar rechts door φ geïnduceerde verticale afbeeldingen construeren.

Ons groepshomomorfisme $\varphi : G_1 \to G_2$ induceert een afbeelding

$$\begin{array}{rcl} \varphi^* : \{\text{e.v. } \mathbb{C}[G_2]\text{-modulen}\}/\cong_{\mathbb{C}[G_2]} & \longrightarrow & \{\text{e.v. } \mathbb{C}[G_1]\text{-modulen}\}/\cong_{\mathbb{C}[G_1]} \\ M & \longmapsto & \varphi^* M. \end{array}$$

Als $0 \to L \to M \to N \to 0$ een korte exacte rij van eindig voortgebrachte $k[G_2]$-modulen is, is $0 \to \varphi^* L \to \varphi^* M \to \varphi^* N \to 0$ een korte exacte rij van eindig voortgebrachte $k[G_1]$-modulen. Dus, $M \mapsto [\varphi^* M] \in \mathcal{R}_{\mathbb{C}}(G_1)$ is additief en er is een uniek *groeps*homomorfisme $\varphi^* : \mathcal{R}_{\mathbb{C}}(G_2) \to \mathcal{R}_{\mathbb{C}}(G_1)$ zodat $[M] \mapsto [\varphi^* M]$.

Zij $g \in \mathbb{C}^{G_2/\sim}$, dan is g een afbeelding $G_2/\sim \to \mathbb{C}$. Het homomorfisme $\varphi : G_1 \to G_2$ induceert een afbeelding $\varphi/\sim : G_1/\sim \to G_2/\sim$. We vinden nu een afbeelding

$$\begin{array}{rcl} (\varphi/\sim)^* : \mathbb{C}^{G_2/\sim} & \longrightarrow & \mathbb{C}^{G_1/\sim} \\ g & \longmapsto & g \circ (\varphi/\sim). \end{array}$$

We hebben nu de volgende verticale afbeeldingen:

$$\begin{array}{ccccccc} \{\text{e.v. } \mathbb{C}[G_2]\text{-modulen}\}/\cong_{\mathbb{C}[G_2]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_2) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_2) \otimes_{\mathbb{Z}} \mathbb{C} & \cong & \mathbb{C}^{G_2/\sim} \\ \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^* \otimes \mathrm{id}} & & \downarrow{\scriptstyle (\varphi/\sim)^*} \\ \{\text{e.v. } \mathbb{C}[G_1]\text{-modulen}\}/\cong_{\mathbb{C}[G_1]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_1) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_1) \otimes_{\mathbb{Z}} \mathbb{C} & \cong & \mathbb{C}^{G_1/\sim}. \end{array}$$

Het is duidelijk te zien dat de linker twee vierkanten commutatief zijn.

Lemma 12.1. *Het rechter vierkant*

$$\begin{array}{ccc} \mathcal{R}_{\mathbb{C}}(G_2) \otimes_{\mathbb{Z}} \mathbb{C} & \xrightarrow[\psi_1]{\sim} & \mathbb{C}^{G_2/\sim} \\ \downarrow{\scriptstyle \varphi^* \otimes \mathrm{id}} & & \downarrow{\scriptstyle (\varphi/\sim)^*} \\ \mathcal{R}_{\mathbb{C}}(G_1) \otimes_{\mathbb{Z}} \mathbb{C} & \xrightarrow[\psi_2]{\sim} & \mathbb{C}^{G_1/\sim} \end{array}$$

is commutatief.

Bewijs. Omdat $\chi_{\varphi^* M}(\sigma) = \chi_M(\varphi(\sigma))$ geldt dat $\chi_{\varphi^* M} = \chi_M \circ \varphi$. Dus, $\psi_1(\varphi^* \otimes \mathrm{id}_{\mathbb{C}})$ en $(\varphi/\sim)^* \circ \psi_2$ vallen samen op alle elementen van de vorm $[M] \otimes 1$. Deze elementen spannen $\mathcal{R}_{\mathbb{C}}(G_2)$ als $\mathbb{C}$-vectorruimte op. Omdat de afbeeldingen $\mathbb{C}$-lineair zijn, zijn $\psi_1(\varphi^* \otimes \mathrm{id}_{\mathbb{C}})$ en $(\varphi/\sim)^* \circ \psi_2$ gelijk op heel $\mathcal{R}_{\mathbb{C}}(G_2)$. □

Stelling 12.2. *De afbeeldingen $\varphi^* : \mathcal{R}_{\mathbb{C}}(G_2) \to \mathcal{R}_{\mathbb{C}}(G_1)$, $\varphi^* \otimes \mathrm{id} : \mathcal{R}_{\mathbb{C}}(G_2) \otimes_{\mathbb{Z}} \mathbb{C} \to \mathcal{R}_{\mathbb{C}}(G_1) \otimes_{\mathbb{Z}} \mathbb{C}$ en $(\varphi/\sim)^* : \mathbb{C}^{G_2/\sim} \to \mathbb{C}^{G_1/\sim}$ zijn ringhomomorfismen.*

Bewijs. We zullen dit alleen bewijzen voor de eerste en de laatste afbeelding.

Voor de eerste afbeelding is het voldoende aan te tonen dat als M en N eindig voortgebrachte $\mathbb{C}[G_2]$-modulen zijn, geldt dat $\varphi^*(M \otimes_{\mathbb{C}} N) \cong \varphi^* M \otimes_C \varphi^* N$ als $\mathbb{C}[G_1]$-modulen. Enerzijds is $\varphi^*(M \otimes_{\mathbb{C}} N)$ gelijk aan $M \otimes_C N$ waarop G_1 werkt door $\sigma(x \otimes y) = \varphi(\sigma)(x \otimes y) = (\varphi(\sigma)x) \otimes (\varphi(\sigma)y)$. Anderzijds is $\varphi^* M \otimes_C \varphi^* N$ gelijk aan $M \otimes_{\mathbb{C}} N$ waarop G_1 werkt door $\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y) = (\varphi(\sigma)x) \otimes (\varphi(\sigma)y)$.

Algemeen geldt: als X en Y verzamelingen zijn, en $\lambda : X \to Y$ is een afbeelding, dan is de afbeelding

$$\begin{array}{rcl} \lambda^* : \mathbb{C}^Y & \longrightarrow & \mathbb{C}^X \\ f & \longmapsto & f \circ \lambda \end{array}$$

een ringhomomorfisme. Hier is $\mathbb{C}^Y$ een ring door $(fg)(y) = f(y)g(y)$ voor $f, g \in \mathbb{C}^Y$ en $y \in Y$. Controleer zelf dat dit waar is. Als we dit toepassen op $X = G_1/\!\sim$, $Y = G_2/\!\sim$, $\lambda = (\varphi/\!\sim)$, volgt dat $(\varphi/\!\sim)^*$ een ringhomomorfisme is. □

Zoals we eerder gezien hebben, kunnen we op $\mathcal{R}_{\mathbb{C}}(G_i)$, $\mathcal{R}_{\mathbb{C}}(G_i) \otimes_{\mathbb{Z}} \mathbb{C}$ en $\mathbb{C}^{G_i/\sim}$ een involutie $\overline{\ }$ definiëren.

$$\begin{array}{ccccccc} \{\text{e.v. } \mathbb{C}[G]\text{-modulen}\}/\!\cong_{\mathbb{C}[G]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G) \otimes_{\mathbb{Z}} \mathbb{C} & \cong & \mathbb{C}^{G/\sim} \\ \downarrow{\scriptstyle M \mapsto M^\dagger} & & \downarrow{\scriptstyle [M] \mapsto \overline{[M]}} & & \downarrow{\scriptstyle (x \otimes c) \mapsto (x^\dagger \otimes \bar{c})} & & \downarrow{\scriptstyle f \mapsto \overline{\ } \circ f} \\ \{\text{e.v. } \mathbb{C}[G]\text{-modulen}\}/\!\cong_{\mathbb{C}[G]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G) \otimes_{\mathbb{Z}} \mathbb{C} & \cong & \mathbb{C}^{G/\sim}. \end{array}$$

Stelling 12.3. *De drie ringhomomorfismen φ^*, $\varphi^* \otimes \mathrm{id}_C$ en $(\varphi/\!\sim)^*$ commuteren met de involutie $\overline{\ }$.*

Bewijs. We bewijzen dit alleen voor $(\varphi/\!\sim)^*$.

Algemeen geldt: als X en Y verzamelingen zijn en $\lambda : X \to Y$ een afbeelding, dan commuteert het volgende diagram:

$$\begin{array}{ccc} \mathbb{C}^Y & \xrightarrow{f \mapsto \overline{\ } \circ f} & \mathbb{C}^Y \\ {\scriptstyle \lambda^*}\downarrow & & \downarrow{\scriptstyle \lambda^*} \\ \mathbb{C}^X & \xrightarrow{f \mapsto \overline{\ } \circ f} & \mathbb{C}^X \end{array}$$

Immers, $\overline{\ } \circ (f \circ \lambda) = (\overline{\ } \circ f) \circ \lambda$.

Pas dit toe op $X = G_1/\!\sim$, $Y = G_2/\!\sim$, $\lambda = (\varphi/\!\sim)$. □

Merk op dat hieruit volgt dat deze drie ringhomomorfismen ook de afbeelding $(M, N) \mapsto \mathrm{Hom}_{\mathbb{C}}(M, N)$ respecteren. Immers, $\mathrm{Hom}_{\mathbb{C}}(M, N) \cong M^\dagger \otimes_C N$.

We hebben ook eerder het volgende commutatieve diagram geconstrueerd:

$$\begin{array}{ccccccc} (\{\text{e.v. } \mathbb{C}[G]\text{-modulen}\}/\!\cong_{\mathbb{C}[G]})^2 & \hookrightarrow & (\mathcal{R}_{\mathbb{C}}(G))^2 & \hookrightarrow & (\mathcal{R}_{\mathbb{C}}(G) \otimes_{\mathbb{Z}} \mathbb{C})^2 & \cong & (\mathbb{C}^{G/\sim})^2 \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi'} & & \downarrow & & \downarrow{\scriptstyle \langle -,- \rangle} \\ \mathbb{Z}_{\geq 0} & \subset & \mathbb{Z} & \subset & \mathbb{C} & = & \mathbb{C} \end{array}$$

De verticale afbeeldingen zijn hier, van links naar rechts:

$$\begin{array}{rcl} \psi : (M, N) & \mapsto & \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(M, N) \\ \psi' : ([M], [N]) & \mapsto & \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(M, N) \\ (x \otimes c, y \otimes d) & \mapsto & \psi'(x, y) c \bar{d} \\ (f, g) & \mapsto & \langle f, g \rangle \end{array}$$

Stelling 12.4. *Stel φ is* surjectief. *Dan respecteren φ^*, $\varphi^* \otimes \mathrm{id}_{\mathbb{C}}$ en $(\varphi/\!\sim)^*$ het inproduct uit het bovenstaande diagram. Dat wil zeggen, bijvoorbeeld,*

$$\forall x, y \in \mathcal{R}_{\mathbb{C}}(G_2) : \psi'(x, y) = \psi'(\varphi^* x, \varphi^* y)$$
$$\forall f, g \in \mathbb{C}^{G_2/\sim} : \langle f, g\rangle = \langle (\varphi/\!\sim)^*(f), (\varphi/\!\sim)^*(g)\rangle.$$

Bewijs. We zullen alleen bewijzen dat voor M, N eindig voortgebrachte $\mathbb{C}[G_2]$ modulen $\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G_2]}(M, N) = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G_1]}(\varphi^* M, \varphi^* N)$.

In het algemeen geldt dat $\mathrm{Hom}_{\mathbb{C}[G_2]}(M, N) \subset \mathrm{Hom}_{\mathbb{C}[G_1]}(\varphi^* M, \varphi^* N)$. Omdat φ surjectief is, is ook de door φ geïnduceerde afbeelding $\mathbb{C}[G_1] \mapsto \mathbb{C}[G_2]$ surjectief. Controleer zelf dat hieruit volgt dat elke $\mathbb{C}[G_1]$-lineaire afbeelding ook $\mathbb{C}[G_2]$-lineair is. Dus geldt dat $\mathrm{Hom}_{\mathbb{C}[G_2]}(M, N) = \mathrm{Hom}_{\mathbb{C}[G_1]}(\varphi^* M, \varphi^* N)$. In het bijzonder zijn de dimensies gelijk. □

Zij G een eindige groep en H een ondergroep van G. De inclusie-afbeelding $H \to G$ noemen we i. De normale notatie voor i^* is Res of Res^G_H en we noemen i^* de *restrictie-afbeelding*. Op deze situatie passen we toe wat we hierboven al gezien hebben. We krijgen dan het volgende commutatieve diagram:

$$\begin{array}{ccccccc}
\{\text{e.v. } \mathbb{C}[H]\text{-modulen}\}/\!\cong_{\mathbb{C}[H]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(H) & \subset & \mathcal{R}_{\mathbb{C}}(H) \otimes_{\mathbb{Z}} \mathbb{C} & \cong & \mathbb{C}^{H/\sim} \\
\uparrow{\scriptstyle i^*} & & \uparrow{\scriptstyle i^*} & & \uparrow{\scriptstyle i^* \otimes \mathrm{id}} & & \uparrow{\scriptstyle (i/\sim)^*} \\
\{\text{e.v. } \mathbb{C}[G]\text{-modulen}\}/\!\cong_{\mathbb{C}[G]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G) & \subset & \mathcal{R}_{\mathbb{C}}(G) \otimes_{\mathbb{Z}} \mathbb{C} & \cong & \mathbb{C}^{G/\sim}.
\end{array}$$

We zullen nu de stelling van Frobenius gaan bewijzen. Hierbij zullen we gebruik gaan maken van het bovenstaande diagram.

Stelling 12.5 (Stelling van Frobenius). *Stel G is een groep die transitief werkt op een eindige verzameling X. Schrijf $n_\sigma = \#\{x \in X : \sigma x = x\}$ voor $\sigma \in G$. Neem aan dat voor alle $\sigma \in G$, $\sigma \neq 1$, geldt dat $n_\sigma \leq 1$. Dan is $N = \{1\} \cup \{\sigma \in G : n_\sigma = 0\}$ een normale ondergroep van G met $\#N = \#X$.*

Voorbeeld
Neem een eindig lichaam $\mathbb{F}_q$ en een ondergroep $H \subset \mathbb{F}_q^*$, neem $X = \mathbb{F}_q$ en $G = \{\sigma : X \to X : \exists a \in H, b \in \mathbb{F}_q : \forall x \in \mathbb{F}_q : \sigma x = ax + b\}$.

Er geldt dat $\sigma 0 = b$ en $\sigma 1 = a$, dus $\#G = q \cdot \#H$, dus $\#G | (q-1)q$.

Om de n_σ berekenen, moeten we bepalen hoeveel oplossingen de gelijkheid $\sigma x = ax + b = x$ heeft voor $a \in H$ en $b \in \mathbb{F}_q$. Deze gelijkheid is equivalent met $(a-1)x = x$. We zien nu dat

$$n_\sigma = \begin{cases} 1 & \text{als } a \neq 1 \\ 0 & \text{als } a = 1, b = 0 \\ q & \text{als } \sigma = 1 \end{cases}.$$

Voor het geval $\#X = 1$ kloppen alle beweringen in de stelling (ga dit zelf na). Neem vanaf nu aan dat $\#X = n > 1$. Stel $\sigma \in \ker \varphi$, waarbij φ de afbeelding $G \to \mathrm{Sym} X = S_n$ is, gegeven door $\tau \mapsto (x \mapsto \tau x)$. Dan geldt dat $n_\sigma = \#X > 1$, dus $\sigma = 1$. Dus φ is injectief en G is isomorf met een ondergroep van de S_n, dus G is eindig.

Kies nu $y \in X$ vast en schrijf $H = \{\sigma \in G : \sigma y = y\}$, de stabilisator van y. Dan is de afbeelding $\tau H \mapsto \tau y$ een isomorfisme $G/H \xrightarrow{\sim} X$. Als $\tau, \rho \in G$ en $\tau H \neq \rho H$, dan

$\tau y \neq \rho y$, dus $\tau H \tau^{-1} \cap \rho H \rho^{-1} = \{\sigma \in G : \sigma\tau y = \tau y\} \cap \{\sigma \in G : \sigma\rho y = \rho y\} = \{1\}$. Dit is equivalent met de volgende bewering: als $\tau \in G$, $\tau \notin H$, dan $\tau H \tau^{-1} \cap H = \{1\}$. Dat deze bewering uit de vorige volgt, is duidelijk wanneer we $\rho = 1$ nemen. Dat de vorige bewering uit deze bewering volgt is duidelijk wanneer we opmerken dat $\tau H \neq \rho H \Leftrightarrow \rho^{-1}\tau H \neq H$. Als we de tweede bewering nu toepassen, vinden we dat $(\rho^{-1}\tau)H(\tau^{-1}\rho) \cap H = \{1\}$, dus $\tau H \tau^{-1} \cap \rho H \rho^{-1} = \{1\}$.

Er geldt dus: $G \setminus \{1\} = (N \setminus \{1\}) \sqcup \coprod_{\tau H \in G/H}((\tau H \tau^{-1}) \setminus \{1\})$. Schrijf $h = \#H$. Dan $\#G = \#(G/H) \cdot \#H = nh$. Uit dit alles volgt dat $nh - 1 = \#N - 1 + n(h-1)$, dus $nh = \#N + n(h-1)$, dus $\#N = n = \#X$.

Na deze opmerkingen kunnen we een herformulering geven van de Stelling van Frobenius.

Stelling 12.6 (Stelling van Frobenius, herformulering). *Stel G is een eindige groep en H is een ondergroep van G van index $n > 1$. Neem aan dat voor alle $\tau \in G$ met $\tau \notin H$ geldt: $\tau H \tau^{-1} \cap H = \{1\}$. Definieer $N = (G \setminus \bigcup_{\tau H \in G/H}(\tau H \tau^{-1})) \cup \{1\}$. Dan is N een normale ondergroep van G met $\#N = n$.*

Motivatie van het bewijs.
Neem even aan dat N normaal is. Dan $\#G/N = h$ en de afbeelding $H \to G/N$ die ontstaat door de inclusie-afbeelding $H \to G$ en de projectie-afbeelding $G \to G/N$ samen te stellen is injectief, want $H \cap N = \{1\}$. Hieruit volgt dat $H \cong G/N$. Er bestaat dus een groepshomomorfisme $\varphi : G \to H$ met $\varphi|_H = \mathrm{id}_H$, oftewel $\varphi i = \mathrm{id}_H$. Het idee van het bewijs is nu: construeer verticale afbeeldingen (in het bovenstaande diagram) die eenzijdig inversen van de gegeven verticale afbeeldingen zijn, gaande van rechts naar links.

Bewijs. Stel $\sigma \in H$, $\sigma \neq 1$. Dan $\#[\sigma]_H = \frac{\#H}{\#C_H(\sigma)}$. Ook geldt: $\#[\sigma]_G = \frac{\#G}{\#C_G(\sigma)}$. Hierbij is $C_H(\sigma) = \{\tau \in H : \sigma\tau = \tau\sigma\}$ de centralisator van σ in H. De centralisator $C_G(\sigma)$ is analoog gedefinieerd.

Stel $\rho \in C_G(\sigma)$. Dan $\rho\sigma\rho^{-1} = \sigma \in H \cap \rho H \rho^{-1}$, dus $H \cap \rho H \rho^{-1} \neq \{1\}$, dus $\rho \in H$. Dus $C_G(\sigma) = C_H(\sigma)$. Hieruit volgt dat $\#[\sigma]_G = \#[\sigma]_H \cdot n$. We zien dus dat $[\sigma]_G = \coprod_{\tau H \in G/H} \tau[\sigma]_H \tau^{-1}$ en $[\sigma]_G \cap H = [\sigma]_H$. We zien dat i een bijectie $(H \setminus \{1\})/\sim \to (G \setminus N)/\sim$ induceert.

Definieer nu de afbeelding $\psi : G/\sim \to H/\sim$ door

$$\psi([\sigma]_G) = \begin{cases} [\sigma]_H = [\sigma]_G \cap H & \text{als } \sigma \in H \setminus \{1\} \\ [1]_H & \text{voor } \sigma \in N \end{cases}.$$

Merk op dat $\psi \circ (i/\sim) = \mathrm{id}_{H/\sim}$.

Definieer $\psi^* : \mathbb{C}^{H/\sim} \to \mathbb{C}^{G/\sim}$ door $\psi^*(f) = f \circ \psi$. Het is duidelijk dat ψ^* een ringhomomorfisme is met $i^*\psi^* = \mathrm{id}_{\mathbb{C}^{H/\sim}}$.

Definieer nu de afbeelding $\mathcal{R}_{\mathbb{C}}(H) \otimes_{\mathbb{Z}} \mathbb{C} \to \mathcal{R}_{\mathbb{C}}(G) \otimes_{\mathbb{Z}} \mathbb{C}$ door in het diagram rechts-omlaag-links te lopen, d.w.z. definieer de afbeelding door het isomorfisme $\mathcal{R}_{\mathbb{C}}(G) \otimes_{\mathbb{Z}} \mathbb{C} \xrightarrow{\sim} \mathbb{C}^{G/\sim}$, de afbeelding $\psi : G/\sim \to H/\sim$ en het isomorfisme $\mathbb{C}^{H/\sim} \xrightarrow{\sim} \mathcal{R}_{\mathbb{C}}(H) \otimes_{\mathbb{Z}} \mathbb{C}$ samen te stellen.

We gaan nu een aantal eigenschappen van de afbeelding ψ^* bewijzen.

Eigenschap 1: $\psi^* : \mathbb{C}^{H/\sim} \to \mathbb{C}^{G/\sim}$ bewaart inproducten, d.w.z. voor alle $f, g \in \mathbb{C}^{H/\sim}$ geldt $\langle f, g\rangle_H = \langle \psi^* f, \psi^* g\rangle_G$.

Bewijs.

$$\begin{aligned}\langle \psi^* f, \psi^* g\rangle_G &= \frac{1}{\#G}\sum_{\sigma\in G} \psi^* f(\sigma)\overline{\psi^* g(\sigma)} = \frac{1}{\#G}\sum_{[\sigma]_G\in G/\sim} \#[\sigma]_G f(\psi([\sigma]_G))\overline{g(\psi([\sigma]_G))} \\ &= \frac{1}{\#G}\sum_{C\in H/\sim}\left(\sum_{\substack{[\sigma]_G\in G/\sim \\ \psi([\sigma]_G)=C}} \#[\sigma]_G\right) f(C)\overline{g(C)}.\end{aligned}$$

Er geldt dat

$$\sum_{\substack{[\sigma]_G\in G/\sim \\ \psi([\sigma]_G)=C}} \#[\sigma]_G = \begin{cases} n\cdot \#C & \text{als } C \neq \{1\} \\ \sum_{\substack{[\tau]_G\in G/\sim \\ \tau\in N}} \#[\tau]_G = \#N = n = n\cdot \#C & \text{als } C = 1 \end{cases}.$$

We vinden dus:

$$\langle \psi^* f, \psi^* g\rangle_G = \frac{n}{\#G}\sum_{C\in H/\sim} \#C f(C)\overline{g(C)} = \frac{1}{\#H}\sum_{\sigma\in H} f(\sigma)\overline{g(\sigma)} = \langle f, g\rangle_H.$$

□

Eigenschap 2: Voor alle $f \in \mathbb{C}^{H/\sim}$ en $g \in \mathbb{C}^{G/\sim}$ met $f(1) = 0$ geldt $\langle \psi^* f, g\rangle_G = \langle f, i^* g\rangle_H$. (Merk op: $i^* g = h|_H$.)

Bewijs.

$$\begin{aligned}\langle \psi^* f, g\rangle_G &= \frac{1}{\#G}\sum_{[\sigma]\in G/\sim} f(\psi(\sigma))\overline{g(\sigma)}\#[\sigma]_G = \frac{1}{\#G}\sum_{C\in H/\sim} f(C)\sum_{\substack{[\sigma]_G\in G/\sim \\ \psi([\sigma]_G)=C}} \#[\sigma]_G\overline{g(\sigma)} \\ &= \frac{1}{\#G}\sum_{\substack{C\in H/\sim \\ C\neq\{1\}}} f(C)n\#C\overline{g(C)} = \frac{1}{\#G}\sum_{C\in H/\sim} f(C)n\#C\overline{g(C)} \\ &= \frac{1}{\#H}\sum_{C\in H/\sim} \#C f(C)\overline{g(C)} = \langle f, g|_H\rangle_H.\end{aligned}$$

□

Eigenschap 3: Er geldt $\psi^*(\mathcal{R}(H)) \subset \mathcal{R}(G)$.

Bewijs. Er geldt dat $\mathcal{R}(G) = \bigoplus_{S\,\text{simpel}} \mathbb{Z}\cdot[S] \subset \mathcal{R}(G)\otimes\mathbb{C} = \bigoplus_S \mathbb{C}\cdot[S] \cong \bigoplus_{\chi\in X(G)} \mathbb{C}\cdot\chi$. We hebben eerder al gezien dat

$$\langle [S], [S']\rangle = \begin{cases} 1 & \text{als } [S] = [S'] \\ 0 & \text{anders} \end{cases}.$$

Als $\chi \in \mathcal{R}(G)\otimes\mathbb{C}$, dan geldt:

$$x \in \mathcal{R}(G) \Leftrightarrow \forall \chi \in X(G) : \langle x, \chi\rangle_G \in \mathbb{Z} \tag{4}$$

(dit hebben we al gezien).

We moeten bewijzen dat $\psi^*(x) \in \mathcal{R}(G)$ voor alle $x \in \mathcal{R}(H)$ met $x(1) = 0$. Zij $x \in \mathcal{R}(H)$ met $x(1) = 0$ willekeurig gegeven. Zij ook $\chi \in X(G)$ willekeurig gegeven. Het is nu voldoende om te laten zien dat $\langle \psi^*(x), \chi \rangle_G \in \mathbb{Z}$.

Er geldt volgens eigenschap 2: $\langle \psi^*(x), \chi \rangle_G = \langle x, i^*\chi \rangle_H$. Omdat χ simpel is, geldt $\chi \in \mathcal{R}(G)$, dus $i^*\chi \in \mathcal{R}(H)$. Dus $i^*\chi = \sum_{\omega \in X(H)} n_\omega \omega$ met $n_\omega \in \mathbb{Z}$. Dus $\langle x, i^*\chi \rangle_H = \sum_{\omega \in X(H)} n_\omega \langle x, \omega \rangle_H \in \mathbb{Z}$, want $\langle x, \omega \rangle \in \mathbb{Z}$ volgens (4). We hebben nu dus laten zien dat $\langle \psi^*(x), \chi \rangle_G \in \mathbb{Z}$ voor alle $x \in \mathcal{R}(H)$ met $x(1) = 0$.

De afbeelding $\rho : \mathcal{R}(H) \to \mathbb{Z}$ gegeven door $x \mapsto x(1)$ is een ringhomomorfisme (ga dit zelf na). We hebben eigenschap 2 alleen bewezen voor elementen in de kern van ρ. We hebben laten zien dat $\psi^*(\ker \rho) \subset \mathcal{R}(G)$. De afbeelding ρ beeldt 1 op 1 af, dus $\mathcal{R}(H) = (\ker \rho) \oplus \mathbb{Z} \cdot 1$. Omdat ook ψ^* het element 1 op 1 afbeeldt, vinden we dat $\psi^*(\mathcal{R}(H)) \subset \mathcal{R}(G)$, wat we wilden bewijzen. □

Eigenschap 4: Voor elke $\chi \in X(H)$ geldt dat $\psi^*\chi \in X(G)$ en N werkt triviaal op het bij $\psi^*\chi$ behorende simpele $\mathbb{C}[G]$-moduul.

Bewijs. Stel $\chi \in X(G)$. Dan geldt $\chi \in \mathcal{R}(H)$, dus met eigenschap 3 volgt nu dat $\psi^*\chi \in \mathcal{R}(G)$. Schrijf $\psi^*\chi = \sum_{\omega \in X(G)} n_\omega \omega$, met $n_{\omega \in \mathbb{Z}}$. We moeten bewijzen dat één van de n_ω gelijk is aan 1 en de andere allemaal gelijk zijn aan 0. We weten dat $\langle \psi^*\chi, \psi^*\chi \rangle_G = \sum_{\omega \in X(G)} n_\omega^2$. Anderzijds volgt uit eigenschap 1 dat $\langle \psi^*\chi, \psi^*\chi \rangle_G = \langle \chi, \chi \rangle_H = 1$. Er volgt dat alle n_ω op één na gelijk aan 0 zijn, en dat de laatste n_ω gelijk is aan 1 of -1.

Nu geldt: $\chi\psi = \psi^*\chi = \pm\omega$ voor een $\omega \in X(G)$. Dus $\chi\psi(1) = \pm\omega(1) \in \pm(\mathbb{Z}_{>0})$ en, anderzijds, $\chi\psi(1) = \chi(1) \in \mathbb{Z}_{>0}$. Dus het $+$-teken geldt, dus de laatste n_ω is gelijk aan 1.

Stel M is het bij $\psi^*\chi$ behorende $\mathbb{C}[G]$-moduul en $\tau \in N$. Dan is het spoor van τ op M gelijk aan $\psi^*\chi(\tau) = \chi(\psi(\tau)) = \chi(1) = \chi(\psi(1))$, wat gelijk is aan het spoor van 1 op M, dus gelijk is aan $\dim_{\mathbb{C}} M$. Dus τ werkt als 1 op M. □

Opmerking: We kunnen $\mathcal{R}(G)$ als volgt schrijven: $\mathcal{R}(G) = \sum_{\chi \in X(G)} \mathbb{Z} \cdot \chi$. We krijgen nu $\mathcal{R}(G)_{\text{eff}} = \sum_{\chi \in X(G)} \mathbb{Z}_{\geq 0} \cdot \chi$. Uit eigenschap 4 volgt dat $\psi^*(\mathcal{R}(H)_{\text{eff}}) \subset \mathcal{R}(G)_{\text{eff}}$.

Uit deze opmerking volgt dat er een afbeelding

$$\begin{array}{rcl} \psi^* : \{\text{e.v. } \mathbb{C}[H]\text{-modulen}\}/\cong & \longrightarrow & \{\text{e.v. } \mathbb{C}[G]\text{-modulen}\}/\cong \\ M & \longmapsto & \psi^* M \end{array}$$

bestaat met de volgende eigenschappen:

- N werkt triviaal op elke ψ^*M. (Als M simpel is weten we dit uit eigenschap 4, voor niet-simpele M volgt deze eigenschap omdat M dan een directe som van simpele modulen is.)
- Opgevat als $\mathbb{C}[H]$-moduul (dat kan omdat $\mathbb{C}[H] \subset \mathbb{C}[G]$ een deelring is) is ψ^*M isomorf met M. (Dit is hetzelfde als $i^*\psi^* = \text{id}$.)

We gaan nu bewijzen dat N de kern is van de actie van G op $\psi^*\mathbb{C}[H]$. We weten al dat $N \subset \ker(G \to \mathrm{Aut}_{\mathbb{C}}\psi^*\mathbb{C}[H])$. Verder geldt dat $\psi^*\mathbb{C}[H] \cong_{\mathbb{C}[H]} \mathbb{C}[H]$, dus $H \cap \ker(G \to \mathrm{Aut}_{\mathbb{C}}\psi^*\mathbb{C}[H]) = \{1\}$. Dus geldt dat $\ker(G \to \mathrm{Aut}_{\mathbb{C}}\psi^*\mathbb{C}[H]) \subset N$. Dus $N = \ker(G \to \mathrm{Aut}_{\mathbb{C}}\psi^*\mathbb{C}[H])$ en $N \lhd G$. □

13 De berekening van de karaktertafel

In dit hoofdstuk zullen we, gegeven een eindige groep G (bijvoorbeeld door middel van een vermenigvuldigtafel), de karaktertafel $[\chi(\sigma)]_{\chi \in X(G), [\sigma] \in G/\sim}$ berekenen.

Uit de lineaire algebra is het begrip *eigenwaarde* bekend. Zij k een lichaam, V een eindig-dimensionale k-vectorruimte en $\varphi : V \to V$ een endomorfisme van V.

Als λ een element van k is, dan zijn de volgende beweringen equivalent:

1. λ is een eigenwaarde van φ.
2. Er is een $v \in V$, $v \neq 0$ waarvoor geldt dat $\varphi(v) = \lambda v$.
3. $V_\lambda = \{v \in V : \varphi(v) = \lambda v\} \neq 0$. (De *eigenruimte* van φ met eigenwaarde λ)
4. $f(\lambda) = 0$, waarbij f het *karakteristieke polynoom* van φ is: $f = \det(X \cdot \mathrm{id} - \varphi) \in k[X]$.
5. $V'_\lambda = \{v \in V : \exists m \geq 1 : (\lambda \cdot \mathrm{id}_V - \varphi)^m(v) = 0\} \neq 0$. (De *gegeneraliseerde eigenruimte*)

Zij f het karakteristieke polynoom van φ. Als $k = \bar{k}$ (of, algemener, als $f \in k[X]$ een product is van lineaire factoren), dan $V = \bigoplus_{\lambda \in k} V'_\lambda$, en $f = \prod_{\lambda \in k} (X - \lambda)^{\dim V'_\lambda}$.

Definitie 13.1. *Het endomorfisme φ heet* semisimpel *als $V = \bigoplus_{\lambda \in k} V_\lambda$, of, equivalent, als voor alle $\lambda \in k$ geldt dat $V_\lambda = V'_\lambda$.*

Zij nu $k = \mathbb{C}$, en $V = Z(k[G])$. We hebben eerder al gezien dat $V = \prod_{C \in G/\sim} k \cdot (\sum_{\sigma \in C} \sigma)$. Als we $C_i := \sum_{\sigma \in C} \sigma$ definiëren voor $i = 1, \ldots, t$, dan krijgen we $V = k \cdot C_1 \oplus k \cdot C_2 \oplus \cdots \oplus k \cdot C_t$.

Omdat V een k-vectorruimte en een commutatieve ring is, is er voor elke $\alpha \in V$ een k-lineaire afbeelding $\alpha : V \to V$ gegeven door $x \mapsto \alpha x$.

We hebben eerder gezien dat het isomorfisme

$$Z(k[G]) \quad \xrightarrow{\sim} \quad \prod_{\chi \in X(G)} k.$$

werkt op C_j door

$$C_j \quad \longmapsto \quad \left(\#C_j \frac{\chi(\sigma_j)}{\chi(1)} \right)_{\chi \in X(G).}$$

We geven nu een algoritme dat gegeven G de karaktertafel uitrekent:

1. Bereken de conjugatieklassen $C_1, \ldots, C_t$ van G en $\#C_i$.
2. Bereken gehele getallen $n_{ijk} \geq 0$ met $C_i C_j = \sum_{k=1}^{t} n_{ijk} C_k$.
3. Bereken voor $i = 1, \ldots, t$ de gemeenschappelijke eigenruimten van $C_1, \ldots, C_i$ en de bijbehorende eigenwaarden.
4. De gemeenschappelijke eigenruimten van $C_1, \ldots, C_t$ zijn 1-dimensionaal. Noem ze $V_1, \ldots, V_t$. Zij λ_{ij} de eigenwaarde van C_i op V_j. Als nu V_j hoort bij χ_j en $\sigma_i \in C_i$, dan is $\lambda_{ij} = \#[\sigma_i] \frac{\chi_j(\sigma_i)}{\chi_j(1)}$. Uit de al bekende formule

$$\sum_{\chi \in X(G)} \chi(1)\chi(\sigma) = \begin{cases} \#G \text{ als } \sigma = 1 \\ 0 \text{ als } \sigma \neq 1 \end{cases}$$

zien we dat

$$\frac{1}{\#[\sigma_i]} \sum_{j=1}^{t} \chi_j(1)^2 \lambda_{ij} = \begin{cases} \#G \text{ als } \sigma_i = 1 \\ 0 \text{ als } \sigma_i \neq 1 \end{cases}$$

en dus dat

$$\sum_{j=1}^{t} \chi_j(1)^2 \lambda_{ij} = \begin{cases} \#G \text{ als } \sigma_i = 1 \\ 0 \text{ als } \sigma_i \neq 1. \end{cases}$$

Los uit dit lineaire systeem $\chi_j(1)^2$ op en definieer $\chi_j(\sigma_i) = \chi_j(1)\lambda_{ij}/\#[\sigma_i]$.

Voorbeeld
Zij $G = S_3$.

1. $C_1 = (1)$, $C_2 = (1\ 2\ 3) + (1\ 3\ 2)$, $C_3 = (1\ 2) + (1\ 3) + (2\ 3)$, $\#C_1 = 1$, $\#C_2 = 2$, $\#C_3 = 3$.
2. $C_1 = 1$, $C_2^2 = 2C_1 + C_2$, $C_3^2 = 3C_1 + 3C_2$, $C_2 C_3 = 2C_3$.
3. C_1: eigenruimte $k \cdot C_1 + k \cdot C_2 + k \cdot C_3$ met eigenwaarde 1.

   C_2: vermenigvuldiging met C_2 wordt op de basis C_1, C_2, C_3 gegeven door de matrix $\begin{pmatrix} 0 & 2 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. Het karakteristieke polynoom van deze matrix is $(X(X-1)-2)(X-2) = (X+1)(X-2)^2$. De eigenruimte van C_2 bij $\lambda = -1$ is $k \cdot (2C_1 - C_2)$ en die bij $\lambda = 2$ is $k \cdot (C_1 + C_2) \oplus k \cdot C_3$.

   C_3: $C_3(2C_1 - C_2) = 2C_3 - 2C_3 = 0$, dus C_3 heeft eigenwaarde 0 in $(2C_1 - C_2)$. Verder is $C_3(C_1 + C_2) = 3C_3$ en $C_3 C_3 = 3(C_1 + C_2)$, dus vermenigvuldiging met C_3 wordt op de basis $(C_1 + C_2), C_3$ gegeven door de matrix $\begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}$. Het karakteristieke polynoom is $X^2 - 9 = (X-3)(X+3)$. De eigenruimte van C_3 bij $\lambda = 3$ is $k \cdot (C_1 + C_2 + C_3)$ en die bij $\lambda = -2$ is $k \cdot (C_1 + C_2 - C_3)$.
4. De eigenwaarden van C_i bij V_j zijn als volgt:

$V_j \backslash \mathbb{C}_i$	C_1	C_2	C_3
$2(C_1 - C_2)$	1	-1	0
$C_1 + C_2 + C_3$	1	2	3
$C_1 + C_2 - C_3$	1	2	-3

We moeten nu het stelsel

$$\chi_1(1)^2(1\ -1\ 0) + \chi_2(1)^2(1\ 2\ 3) + \chi_3(1)^2(1\ 2\ -3) = (6\ 0\ 0)$$

oplossen. Dit geeft $\chi_1(1)^2 = 4$, $\chi_2(1)^2 = 1$ en $\chi_3(1)^2 = 1$ en dus $\chi_1(1) = 2$, $\chi_2(1) = 1$ en $\chi_3(1) = 1$.
Dit geeft de karaktertafel:

$\chi_j(\sigma_i)$			
	2	-1	0
	1	1	1
	1	1	-1.

14 Inductie en de stelling van Brauer

Zij k een lichaam en $n \in \mathbb{Z}_{\geq 0}$.

Definitie 14.1. *Een* monomiale $n \times n$ *matrix over* k *is een inverteerbare matrix* $(a_{ij})_{1 \leq i,j \leq n}$ *over* k *waarvoor* $n(n-1)$ *van de* a_{ij}*'s gelijk zijn aan 0.*

De verzameling $\mathrm{Mon}(n,k)$ van monomiale $n \times n$-matrices over k is een ondergroep van $GL(n,k)$.

We hebben het volgende korte exacte rijtje

$$1 \longrightarrow (k^*)^n \longrightarrow \mathrm{Mon}(n,k) \longrightarrow S_n \longrightarrow 1,$$

en de afbeelding $S_n \to \mathrm{Mon}(n,k)$ die σ afbeeldt op de permutatiematrix van σ geeft een splitsing. We zien dat $\mathrm{Mon}(n,k) \cong (k^*)^n \rtimes S_n$.

Zij nu $k = \mathbb{C}$ en G een eindige groep. Zij verder M een eindig voortgebracht $k[G]$-moduul.

Definitie 14.2. M *heet* monomiaal *als er een basis* $b_1, \ldots, b_n$ *voor* M *bestaat zodat*

$$\forall \sigma \in G\, \forall i \in \{1, \ldots, n\} : \exists j \in \{1, \ldots, n\}, a \in k^* : \sigma b_i = a b_j$$

of, equivalent, als er een isomorfisme $M \cong_k k^n$ *bestaat zodat het beeld van* $G \to \mathrm{Aut}_k(M) \cong \mathrm{Aut}_k(k^n) \cong GL(n,k)$ *bevat is in* $\mathrm{Mon}(n,k)$.

Voorbeeld
Zij $G = D_4 = \langle \rho, \sigma \rangle$.

Er zijn vier 1-dimensionale simpele modulen en elk 1-dimensionaal moduul is monomiaal. Er is één 2-dimensionaal simpel moduul. Het beeld van ρ is $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ en dat van σ is $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Beide zijn monomiale matrices, dus ook dit simpele moduul is monomiaal.

Dus, iedere representatie van D_4 is monomiaal.

Definitie 14.3. *Een eindig voortgebracht $k[G]$-moduul M heet een* permutatiemoduul *als M een k-basis heeft die door G gepermuteerd wordt.*

Merk op dat een permutatiemoduul van dimensie groter dan 1 een deelmoduul heeft dat wordt opgespannen door de som van de basisvectoren.

Stelling 14.4 (Stelling van Brauer). *Stel G is een eindige groep en M een eindig voortgebracht $\mathbb{C}[G]$-moduul. Dan zijn er twee monomiale $\mathbb{C}[G]$-modulen M_1 en M_2 zodanig dat $M \oplus M_1 \cong_{\mathbb{C}[G]} M_2$.*

Gevolg 14.5. *Zij G een eindige groep en zij m de exponent van G. Dan kan elk eindig voortgebracht $\mathbb{C}[G]$-moduul M gedefinieerd worden over $\mathbb{Q}(\zeta_m)$. Dat wil zeggen, er is een isomorfisme $M \cong_{\mathbb{C}} \mathbb{C}^n$ zodanig dat het beeld van $G \to \mathrm{Aut}_{\mathbb{C}}(M) \cong GL(n,\mathbb{C})$ bevat is in $GL(n,\mathbb{Q}(\zeta_m))$.*

In het vorige hoofdstuk hebben we het volgende diagram gezien:

$$\begin{array}{ccccccc}
\{\text{e.v. } \mathbb{C}[G_2]\text{-modulen}\}/\cong_{\mathbb{C}[G_2]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_2) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_2)\otimes_{\mathbb{Z}}\mathbb{C} & \cong & \mathbb{C}^{G_2/\sim} \\
\downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*\otimes \mathrm{id}} & & \downarrow{\scriptstyle (\varphi/\sim)^*} \\
\{\text{e.v. } \mathbb{C}[G_1]\text{-modulen}\}/\cong_{\mathbb{C}[G_1]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_1) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_1)\otimes_{\mathbb{Z}}\mathbb{C} & \cong & \mathbb{C}^{G_1/\sim}.
\end{array}$$

We kunnen ook afbeeldingen φ_* omhoog construeren. Merk op dat $\varphi_*(M) = k[G_2] \otimes_{k[G_1]} M$ een $k[G_2]$-moduul is omdat $k[G_2]$ een $k[G_2]$-$k[G_1]$-bimoduul is.

In het speciale geval dat $G_1 = H$ een ondergroep van $G_2 = G$ is en $\varphi = i$ de inclusie $H \subset G$ is, noemen we i_* ook wel *inductie* van H naar G met notatie $i_* = \mathrm{Ind}_H^G$.

Zij nu G een eindige groep, $H \subset G$ een ondergroep en M een $k[H]$-moduul. Hoe ziet $\mathrm{Ind}_H^G M = k[G] \otimes_{k[H]} M$ er uit?

Schrijf $G = \coprod_{\rho\in P} \rho H$. Dan is $k[G] = \bigoplus_{\rho\in P} \rho \cdot k[H]$. Hieruit volgt dat $k[G] \otimes_{k[H]} M = \bigoplus_{\rho\in P} \rho \cdot M$. Als nu $\sigma \in G$, $x \in M$ en $\rho \in P$, dan zijn er een $\rho' \in P$ en een $\tau \in H$ zodat $\sigma\rho = \rho'\tau$. Hieruit zien we dat $\sigma(\rho x) = \rho'(\tau x) \in \rho' \cdot M$.

Voorbeeld
Als $M = k$, dan is $\mathrm{Ind}_H^G k$ een permutatiemoduul met als onderliggende vectorruimte $k^{G/H}$.

Een eindig voortgebracht $k[G]$-moduul N is monomiaal dan en slechts dan als N van de vorm $\bigoplus_{i=1}^{r} \mathrm{Ind}_{H_i}^G(M_i)$ is, met $H_i \subset G$ een ondergroep en M_i een 1-dimensionaal $k[H_i]$-moduul.