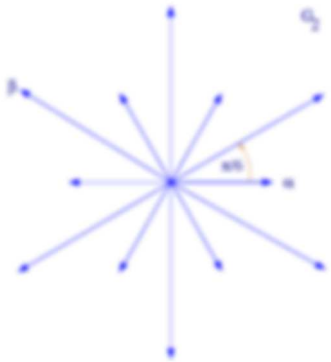
VRIJE
UNIVERSITEIT
BRUSSEL

Ring- en Moduultheorie



Geoffrey Janssens
Eric Jespers

Vakgroep Wiskunde

2^e Bachelor Wiskunde
2019–2020

Voorwoord

Naast groepentheorie, vormen (commutatieve) ring- en moduultheorie onmisbare hoofdstukken in de algebrakennis van een bachelor in de wiskunde. Kennis van deze onderdelen is onontbeerlijk in zowat elke (gevorderde) algebracursus. In het eerste hoofdstuk in deze cursus worden groeprepresentaties bestudeerd. Deze theorie is waardevol voor de studie van eindige groepen. In de cursus groepentheorie hebben we gezien dat (abstracte) algebra ontstaan is uit de studie van concrete objecten. Door groepsrepresentaties te ontwikkelen, beschikken we over nieuw gereedschap om eender welke abstracte eindige groep te bestuderen door middel van een homomorfisme naar de groep van lineaire transformaties van een vectorruimte. Daardoor wordt als het ware de abstracte groep opnieuw geconcretiseerd. Wij zullen slechts een initiële studie maken van groeprepresentaties en dit via lineaire algebra (een klassieke manier).

In het twee en derde hoofdstuk wordt de basis van de ring- en moduultheorie behandeld. Het hoofdstuk ringtheorie heeft belangrijke toepassingen zoals bijvoorbeeld de theorie van de velduitbreidingen en Galoistheorie. Modulen over ringen zijn een (verregaande) veralgemening van vectorruimten over velden. Naast belangrijke toepassingen die in gevorderde cursussen aan bod komen, worden modulen ook gebruikt om op een abstractere wijze groepsrepresentaties in te voeren (hetgeen de moderne manier is). Aldus vormen de drie hoofdstukken één geheel. Tenslotte komen enkele toepassingen in het vierde hoofdstuk aan bod, die in functie van de beschikbare tijd al dan niet behandeld worden.

Inhoudsopgave

Hoofdstuk 1

Representatietheorie

1.1 Inleiding

De theorie van groeprepresentaties is die tak van de wiskunde waarin eigenschappen van abstracte groepen worden bestudeerd via hun representaties als lineaire transformaties van vectorruimten. Representatietheorie is een zeer nuttige manier om groepentheoretische problemen op te lossen omdat zij problemen reduceert naar lineaire algebra, een zeer goed uitgewerkte theorie. Het is ook o.a. van belang in fysica. Bijvoorbeeld, representatietheorie wordt gebruikt om een beschrijving te geven van hoe de symmetriegroep van een fysisch systeem de oplossingen van de vergelijkingen van dat systeem beïnvloedt.

Frobenius (1849-1917)

Representatietheorie kan ook gedefinieerd worden voor andere wiskundige structuren, zoals o.a. associatieve algebra's, Lie en Hopf algebra's. In meer gevorderde cursussen komt dit aan bod.

De term "representatie van een groep" wordt ook in een algemenere context gebruikt. Het is een "beschrijving" van een groep als een groep van transformaties van een wiskundig object: een representatie is een homomorfisme van de groep naar de groep van automorfismen van een object. Als het object een vectorruimte is dan verkrijgen wij een lineaire representatie. In deze cursus beperken wij ons tot deze studie.

Brauer (1901-1977)

De algemene eigenschappen van representatietheorie van een eindige groep G, over de complexe getallen, werden ontdekt door Ferdinand Georg Frobenius rond de jaren 1900. Later is de modulaire (karakteristiek niet nul) representatietheorie ontwikkeld door Richard Brauer.

1.2 Achtergrond uit vorige cursussen

1.2.1 Herhaling Lineaire Algebra

In deze sectie herhalen we kort enkele beginselen uit de cursus Lineaire Algebra. Met K noteren we steeds een veld.

Definitie 1.2.1. Een verzameling $(V, +, \cdot_K)$ heet een vectorruimte over K voor twee gegeven bewerkingen

$$+ : V \times V \to V \text{ en } \cdot_K : K \times V \to V$$

indien de volgende eigenschappen voldaan zijn:

- $(V, +)$ is een abelse groep,
- $\cdot_K$ is een linker actie van K op V,
- $a.(u + v) = a.u + av$ en $(a + b).v = a.v + b.v$ voor alle $u, v \in V$ en $a, b \in K$.

De essentie van een vectorruimte V is geëncodeerd in een zogenaamde basis. Herinner dat een deelverzameling $B \subset V$ heet een *basis* indien $\text{vect}_K B = V$ (i.e. B is voortbrengend over K) en B is lineair onafhankelijk over K. Dus intuïtief is een basis een minimale voortbrengde verzameling.

Stelling 1.2.2. *Zij V een vectorruimte. Dan heeft V een basis B en bovendien is de cardinaliteit van iedere basis gelijk.*

De cardinaliteit van een basis wordt de *dimensie* van de vectorruimte genoemd en we noteren deze met $\dim_K(V)$. Het is mogelijk dat er geen eindige verzameling gevonden kan worden die een basis is voor V. Bijvoorbeeld is $\mathbb{R}$ oneindig dimensionaal als vectorruimte over $\mathbb{Q}$. Het bewijs voor het bestaan van een basis in deze context maakt gebruikt van de zogenaamde Lemma van Zorn (dat equivalent is met de intuïtief duidelijk, en toch msyterieuze, "keuze-axioma"). Merk op dat binnen deze context elke vector nog steeds als een **eindige** lineaire combinatie van elementen uit de basis geschreven kan worden. Heel belangrijk is dat het getal 'dimensie' de vectorruimte uniek bepaald op isomorfisme na:

Stelling 1.2.3. *Zij V en W vectorruimten over K. Indien $\dim_K V = \dim_K W$, dan bestaat zijn V en W isomorf (i.e. er bestaat een K-lineaire functie $f : V \to W$ dat ook bijectief is).*

Veronderstel nu dat V een eindigdimensionale K-vectorruimten is. Herinner dat

$$\mathrm{GL}(V) = \{f : V \to V \mid f \text{ is } K\text{-lineair en bijectief}\}.$$

Dit is een groep voor de bewerking $\circ$, de samenstelling van functies. Het eenheidselement uit de groep $\mathrm{GL}(V)$ is de afbeelding die elke vector $v \in V$ op zichzelf afbeeldt. Deze afbeelding noteren we als 1_V. Bovendien is $\mathrm{GL}(V)$ ook een K-vectorruimte voor de puntsgewijze optelling

$$f + g : V \to V; v \mapsto f(v) + g(v)$$

waar $f, g \in \mathrm{GL}(V)$ en de scalaire vermenigvuldiging van $f \in \mathrm{GL}(V)$ met een scalair $r \in K$ is gedefinieerd als

$$rf : V \to V : v \mapsto rf(v).$$

Als we het in vervolg spreken over de *groep* $\mathrm{GL}(V)$, dan veronderstellen we impliciet dat de groepsbewerking de samenstelling van afbeeldingen is $(\circ)$. Waar nodig zullen we echter ook lineaire combinaties van afbeeldingen uit $\mathrm{GL}(V)$ beschouwen, daarbij steunen we dan op de vectorruimtestructuur.

Vervolgens herriner dat de verzameling

$$\mathrm{GL}_n(K) = \{A \in M_n(K) \mid \det(A) \neq 0\}$$

van alle inverteerbare $n \times n$ matrices over het veld K een groep is voor de matrixvermenigvuldiging.

Stel nu dat $\dim_K V = n$. Dan is er een expliciete 1-1 verband tussen $\mathrm{GL}(V)$ en $\mathrm{GL}_n(K)$. We herhalen deze nu kort. Hiervoor moet men eerst een basis $B = \{e_1, \ldots, e_n\}$ van V vast te leggen. Door de lineariteitseigenschap is het beeld van een afbeelding $f \in \mathrm{GL}(V)$ bepaald door zijn beeld op de basis vectoren e_i. Meer precies stel dat

$$f(e_j) = \sum_{i=1}^{n} f_{ij} e_i \,.$$

Dan is $f(\vec{v}) = f_{[E,E]}.\vec{v}^T$, waarbij

$$f_{[E,E]} = (f_{ij}) \in M_n(K) \,.$$

Zodoende bekomen we het volgende.

Stelling 1.2.4. *De afbeelding*

$$\Phi : \mathrm{GL}(V) \to \mathrm{GL}_n(K) : f \mapsto f_{[E,E]} \tag{1.1}$$

is een groepsisomorfisme.

1.2.2 Herhaling acties van groepen

In de cursus 'Inleiding groepentheorie' is er de cruciale notie van 'acties' worden geïntroduceerd. We herhalen heel kort het nodige hieromtrent.

Definitie 1.2.5. Zij X een verzameling en G een groep. Indien er een functie

$$\phi : G \times X \to X$$

bestaat die voldoet aan

- $\phi(e_G, x) = x$ voor alle $x \in X$,
- $\phi(h, \phi(g, x)) = \phi(hg, x)$ voor alle $g, h \in G$ en $x \in X$,

dan zegt men dat G een linker actie uitvoert op X en ϕ heet *de linker actie* van G op X.

Indien ϕ duidelijk is uit de context wordt $\phi(g, x)$ ompacter geschreven als $g \cdot x$ of zelfs gx. Men kan een linker actie ook beschouwen als een groepshomomorfisme naar $\mathrm{Sym}(X)$. In representatie theorie wordt dikwijls dit standpunt voor een actie ingenomen. Herinner dat deze correspondentie als volgt werkt:

Actie $\rightsquigarrow$ homomorfisme: Gegeven een linker actie ϕ van G op X definieer de afbeelding

$$\widehat{\phi} : G \to \mathrm{Sym}(X) : g \mapsto \left(\widehat{\phi}(g) : X \to X : x \mapsto g \cdot x\right).$$

Dan vertalen de linker actie condities zich exact tot de feit dat $\widehat{\phi}$ een groepshomomorfisme is (Oefening).

Homomorfisme $\rightsquigarrow$ actie: Omgekeerd gegeven een groepshomomorfisme $\psi : G \to \mathrm{Sym}(X)$ dan is

$$\widetilde{\psi} : G \times X \to X : (g, x) \mapsto \psi_g(x)$$

een linker-actie van G op X (Oefening).

Gegeven een punt $x \in X$ is het dikwijls leerrijk om naar zijn *baan* (of *orbiet*) onder de actie ϕ van G te bestuderen:

$$\mathcal{O}_\phi(x) = \{g \cdot x \mid g \in G\}.$$

Aan de andere zijde van het spectrum heeft men de *stabilisator* van x onder G:

$$\mathrm{Stab}_\phi(x) = \{g \in G \mid g \cdot x = x\}.$$

Voorbeeld 1.2.6. Iedere groep G voert een linker actie uit op zichzelf via conjugatie

$$\lambda : G \times G \to G : (g, h) \mapsto g^{-1}hg.$$

In dit geval heet $\mathcal{O}_\lambda(h) = \{g^{-1}hg \mid g \in G\}$ de *conjugatieklasse* van h, genoteerd $\mathcal{C}_G(h)$ (of nog $\mathcal{C}(h)$). Alsook wordt dan

$$\mathrm{Stab}_\lambda(h) = \{g \in G \mid gh = hg\}$$

de *centralisator* van h in G genoemd en wordt genoteerd met $\mathrm{Cen}_G(h)$.

Enigszins verbazend is dat de orbiet en stabilisator van een punt $x \in X$ steeds nauw verbonden zijn met elkaar.

Stelling 1.2.7 (Orbiet-Stabilisator)**.** *Zij G een eindige groep, X een verzameling en ϕ een actie van G op X. Dan is*

$$\frac{|G|}{|Stab_\phi(x)|} = |\mathcal{O}_\phi(x)|.$$

1.3 Representaties

1.3.1 Wat is een representatie?

De intrede van de protagonist

Zij G een eindige groep met neutraal element e_G, indien de context het toelaat, dan noteren we e_G ook als e.

Definitie 1.3.1. Een (lineaire) *representatie* van een eindige groep G in een K-vectorruimte V is een groepshomomorfisme

$$\rho : G \to \mathrm{GL}(V) : g \mapsto \rho(g)\,.$$

Dus, voor $g, h \in G$,

$$\rho(gh) = \rho(g) \circ \rho(h)\,.$$

Wij noemen V een *representatieruimte* van G, of soms zeggen wij eenvoudig dat V een representatie is van G. Men noemt $n = \dim_K(V)$ de *graad* van ρ en noteren we met $\deg(\rho)$.

Omdat ρ een groepshomomorfisme is, weten wij dat de volgende eigenschappen voldaan zijn:

$$\rho(e) = 1_V \text{ en } \rho(g^{-1}) = \rho(g)^{-1},$$

voor alle $g \in G$. We zullen regelmatig de lineaire afbeelding

$$\rho(g)$$

eenvoudiger noteren als

$$\rho_g\,.$$

Dus met deze notatie

$$\rho_{e_G} = 1_V \text{ en } \rho_{gh} = \rho_g \circ \rho_h = \rho_g \rho_h,$$

voor alle $g, h \in G$.

In (1.1) hebben we gezien dat de afbeelding Φ een $1-1$ verband geeft tussen $\mathrm{GL}(V)$ en $\mathrm{GL}_n(K)$. Hierdoor heeft men voor iedere representatie een geassocieerd matrix-representatie.

Definitie 1.3.2. Voor een representatie $\rho : G \to \mathrm{GL}(V)$, met $E = \{e_1, \ldots, e_n\}$ een K-basis van V, is de afbeelding

$$A_\rho = \Phi \circ \rho : G \to \mathrm{GL}_n(K) : g \mapsto A_\rho(g) = (\rho(g))_{[E,E]} = (r_{ij}(g))$$

het *geassocieerd matrix-representatie (ten opzichte van de basis E).*

De samenstelling van lineaire afbeeldingen in $\mathrm{GL}(V)$ correspondeert met het matrixproduct in $\mathrm{GL}_n(K)$. Dus voor alle $g, h \in G$ geldt $A_\rho(gh) = A_\rho(g)A_\rho(h)$ en

$$r_{ik}(gh) = \sum_{j=1}^{n} r_{ij}(g)\, r_{jk}(h)\,.$$

Omgekeerd geldt ook dat met een groepshomomorfisme $A : G \to \mathrm{GL}_n(K)$ een representatie $\rho_A : G \to \mathrm{GL}(V)$ geassocieerd wordt, namelijk $\rho_A(g)$ is de lineaire transformatie $f : V \to V$ zodat $f_{[E,E]} = A(g)$. Dus $\rho_A = \Phi^{-1} \circ A$.

In het vervolg zullen wij dikwijls geen onderscheid maken tussen een representatie $\rho : G \to \mathrm{GL}(V)$ en het geassocieerd groepshomomorfisme $A_\rho : G \to \mathrm{GL}_n(K)$ en zullen de beiden noteren met de letter ρ.

"Gelijkheid" van representaties

De overstap van een representatie naar een matrix-representatie eist dat men eerst een basis E van V vastlegt. Bijgevolg hangt de geassocieerde matrix-representatie A_ρ af van zowel ρ als E. Uit lineaire algebra weten we echter dat een andere basis keuze resulteert in een geconjugeerde matrix $P^{-1}A_\rho P$. Aangezien conjugatie met P een isomorfisme van $\mathrm{GL}_n(K)$ naar $\mathrm{GL}_n(K)$ oplevert, zullen A_ρ en $P^{-1}A_\rho P$ dezelfde eigenschappen bezitten. Vandaar de volgende definitie.

Definitie 1.3.3. Zij ρ en τ representaties $G \to \mathrm{GL}(V)$. Men noemt ρ en τ *equivalent* (of *isomorf*) als er een K-vectorruimte-isomorfisme

$$\psi : V \to V$$

bestaat zodat, voor alle $g \in G$,

$$\psi \circ \rho(g) \circ \psi^{-1} = \tau(g).$$

Als $Q = \psi_{[E,E]}$. Dan geldt voor A_ρ en A_τ, de groepshomomorfismen geassocieerd met respectievelijk ρ en τ, dat voor alle $g \in G$,

$$Q^{-1}\, A_\rho(g)\, Q = A_\tau(g).$$

Filosofisch Intermezzo. Het doel van representaties theorie is om de eigenschappen van een groep G te doorgronden doormiddel van hoe G ageert op vectorruimten. In andere woorden, is het doel om G te verstaan via zijn beeld onder representaties. Echter in het algemeen is $\mathrm{Im}\,(\rho)$ niet isomorf met G en dus gaat er meestal informatie verloren in dit process. In het bijzonder heeft de volgende type aan representaties een bijzondere rol.

Definitie 1.3.4. Zij ρ een representatie van G. We noemen ρ *trouw* als $\mathrm{Ker}\,(\rho) = \{e\}$.

In het bijzonder, wegens de eerste isomorfisme stelling, is ρ trouw als en slechts als $\mathrm{Im}\,(\rho) \cong G$. Merk op dat een willekeurige representatie ρ van een groep G steeds een trouwe representatie van de quotiëntgroep $G/\mathrm{Ker}\,(\rho)$ induceert.

Op het eerste zicht is het niet duidelijk dat een gegeven groep steeds een trouwe representatie heeft. Dit is echter het geval en later zullen we een belangrijke constructie zien, namelijk de zogenaamde reguliere representatie.

1.3.2 Van acties naar representaties

We hebben gezien dat een groep G een actie uitvoert op een verzameling X indien er een groepshomomorfisme $\rho : G \to \mathrm{Sym}(X)$ bestaat. Vanuit deze optiek is een representatie van G een actie van G op een vectorruimte V dat bovendien compatibel is met de vectorruimte structuur van V. Het verband tussen representaties en acties gaat echter verder als simpelweg een gedachtegoed. Infeite leveren acties het archetype van een representatie op. Om dit formeel te maken, hebben we de notie van een vrije vectorruimte nodig.

Definitie 1.3.5. Zij X een verzameling. De *vrije K-vectorruimte voortgebracht door X*, genoteerd $K(X)$, is de verzameling

$$\{\sum_{x\in X}{}' a_x e_x \mid a_x \in K\}$$

voorzien met de bewerkingen

- optelling: $\sum'_{x\in X} a_x e_x + \sum'_{x\in X} b_x e_x = \sum'_{x\in X}(a_x + b_x)e_x$,
- Scalaire vermenigvuldiging: $b.\sum'_{x\in X} a_x e_x = \sum'_{x\in X}(ba_x)e_x$

waarbij $a_x, b_x, b \in K$, $\{e_x \mid x \in X\}$ een verzameling van formele symbolen bijectief met X en $\sum'$ de notatie is voor een eindige som.

Merk op dat de vrije K-vectorruimte als basis de verzameling $\{e_x \mid x \in X\}$ heeft. In het bijzonder, indien X oneindig groot is dan is $K(X)$ oneindig dimensionaal over K.

Veronderstel nu dat G een linker actie uitvoert op een verzameling X. Beschouw dan de vrije K-vectorruimte $V = K(X)$, met als basis $\{e_x \mid x \in X\}$. Voor $g \in G$ definieer

$$\rho(g) : V \to V$$

door

$$\rho(g)(e_x) = e_{g\cdot x},$$

met $x \in X$ en breidt dit lineair uit tot een willekeurig element van $K(X)$:

$$\rho(g)(\sum_{x\in X}{}' a_x e_x) = \sum_{x\in X}{}' a_x e_{g\cdot x}$$

Dan is

$$\rho : G \to \mathrm{GL}(V) : g \mapsto \rho(g)$$

een representatie. Men noemt dit de *permutatierepresentatie geassocieerd met de actie.*

Opmerking.

1. Omgekeerd, zie Sectie 1.2.2, als $\rho : G \to \mathrm{GL}(V)$ een representatie is dan definieert

   $$\lambda : G \times V \to V : (g, v) \mapsto \rho(g)(v)$$

   een linkse actie van G op V, maar met de extra eigenschap dat

   $$\lambda(g, \alpha_1 v_1 + \alpha_2 v_2) = \alpha_1.\lambda(g, v_1) + \alpha_2.\lambda(g, v_2)$$

   voor alle $\alpha_1, \alpha_2 \in K$ en $v_1, v_2 \in V$.

2. Zij $S_X = \mathrm{Sym}(X)$ de symmetrische groep op X. Voor een gegeven $\sigma \in S_X$ definieer de matrix $P_\sigma = (x_{ij})$ met $x_{ij} = \delta_{i,\sigma(j)}$. De matrices van de vorm P_σ heten *permutatie matrices.* Stel nu dat $\lambda : G \to \mathrm{Sym}(X)$ een actie is van G op X en ρ de geassocieerde permutatie representatie. Dan is de matrix representatie ρ (oefening) van de vorm

   $$A_\rho(g) = P_{\lambda(g)}.$$

   Dit verklaart de terminologie 'permutatie representatie' voor bovenstaande representatie geassocieerd met een actie.

De reguliere representatie

Zij G een eindige groep en beschouw de actie van G op zichzelf via linker vermenigvuldiging. Zoals gezien in het vorige deel, kunnen we dan hiermee een permutatie representatie associëren. Meer precies, beschouw de vrije K-vectorruimte $V = F(G)$ met als basis de verzameling $\{e_g \mid g \in G\}$ en definieer voor elke $g \in G$ de volgende lineaire transformatie (het is voldoende om de beelden van de basiselementen te geven)

$$\rho(g) : V \to V : e_h \mapsto e_{gh}.$$

Dan is

$$\rho : G \to \mathrm{GL}(V) : g \mapsto \rho(g)$$

een representatie van graad $|G|$. Men noemt dit de *reguliere representatie* van G. Merk op dat $\{\rho(g)(e_1) \mid g \in G\}$ een K-basis is voor V. Deze eigenschappen karakteriseert infeite de reguliere representatie.

Eigenschap 1.3.6. *Zij W een K-vectorruimte en $\tau : G \to \mathrm{GL}(W)$ een representatie van G. Stel dat er een $w \in W \setminus \{0\}$ bestaat zodat*

1. *$\{\tau(g)(w) \mid g \in G\}$ een K-basis is voor W;*
2. *$|\{\tau(g)(w) \mid g \in G\}| = |G|$.*

Dan is W equivalent met de reguliere representatie.

Bewijs. Beschouw het isomorfisme van K-vectorruimten

$$\psi : V \to W$$

gedefinieerd door

$$\psi(e_g) = \tau(g)(w)$$

Dan volgt er, voor elke $h \in G$,

$$\begin{aligned} \psi \circ \rho(g) \circ \psi^{-1}(\tau(h)(w)) &= \psi(\rho(g)(e_h)) \\ &= \psi(e_{gh}) \\ &= \tau(gh)(w) \\ &= \tau(g)(\tau(h)(w)) \end{aligned}$$

Dus, voor elke $g \in G$,

$$\psi \circ \rho(g) \circ \psi^{-1} = \tau(g).$$

Bijgevolg is τ equivalent met de reguliere representatie van G. □

Een minder formele aanpak tot de vrije vectorruimte

We zullen nu een alternatieve constructie zien voor de vrije K-vectorruimte. Deze zal blijken weldegelijk isomorf te zijn met de constructie gegeven voordien.

Definitie 1.3.7. Zij X een willekeurige niet-ledige verzameling en K een veld. Veronderstel dat $f : X \to K$ een functie is. De *support* van f is de verzameling $S = \{x \in X | f(x) \neq 0\}$. We noemen de support van een functie eindig als S een eindige deelverzameling is van X.

Definitie 1.3.8. Zij X een willekeurige niet-ledige verzameling en K een veld. We definiëren $F(X) = \{f : X \to K \mid f$ heeft een eindige support $\}$. Samen met de puntsgewijze optelling van functies en de vermenigvuldiging met elementen uit K, is $F(X)$ een K-vectorruimte

De vectorruimte $F(X)$ is isomorf met $K(X)$, de *vrije K-vectorruimte voortgebracht door X*. Om dit te zien start, voor de gegeven verzameling X en het veld K, de functies δ_x te definiëren als volgt:

$$\delta_x : X \to K; \delta_x(y) = 1 \text{ als } x = y \text{ en } \delta_x(y) = 0 \text{ als } x \neq y.$$

De vectoren van $F(X)$ zijn precies eindige lineaire combinaties van de δ afbeeldingen. Infeite is de verzameling $\{\delta_x | x \in X\}$ een basis is voor $F(X)$. Bijgevolg als X een eindige verzameling is, dan is $|X|$ de dimensie van $F(X)$. Dus $F(X)$ en $K(X)$ zijn K-vectorruimten van dezelfde dimensie en bijgevolg, wegens Stelling 1.2.3, zijn $K(X)$ en $F(X)$ inderdaad isomorf.

Opmerking. De afbeelding

$$\iota : X \to F(X) : \iota(x) := \delta_x$$

is een inbedding van de verzameling X in $F(X)$, deze afbeelding is uiteraard injectief. Ze laat ons toe om de notatie te vereenvoudigen. Namelijk, in plaats van de lineaire combinatie

$$\sum_{x \in I} a_x \delta_x$$

(met $I \subset X$ een **eindige** deelverzameling van X) te schrijven, zullen we in het vervolg meestal (als de context het toelaat) gewoon

$$\sum_{x \in I} a_x x$$

schrijven. Men kan dus zeggen dat de vrije K-vectorruimte $F(X)$ de K-vectorruimte is die bestaat uit alle eindige K-lineaire combinaties van elementen uit X, waarbij we deze lineaire combinaties een betekenis gegeven hebben via de δ-functies.

1.3.3 Een eerste ontmoeting met voorbeelden

1. De cyclische groep:

Zij $C_n = \langle g \mid g^n = 1 \rangle$ de cyclische groep van orde n. Merk op dat indien $\rho : G \to \mathrm{GL}_m(\mathbb{C})$ een representatie is van een groep G dan moet $o(\rho(h)) \mid o(h)$ voor elke $h \in G$ (omdat ρ een groepshomomorfisme is).

Om te starten zullen we een representatie van graad 1 maken. Wegens het bovenstaande is het volgende een logische keuze:

$$\rho : C_n \to \mathbb{C} : g^i \mapsto \zeta_n^i$$

waar ζ_n een primitieve n-de eenheidswortel is.

2. De diëdergroep:

Zij $D_8 = \langle a, b \mid a^4 = 1,\ b^2 = 1,\ ba = a^{-1}b \rangle$ de diëdergroep van orde 8. Dus

$$D_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Definieer in $M_2(\mathbb{C})$ de matrices A en B:

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \text{ en } B = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Dan is

$$\rho : D_8 \to GL_2(\mathbb{C}) : a^k b^l \mapsto A^k B^l$$

(met $0 \leq k \leq 3$, $0 \leq l \leq 1$) een representatie van D_8 van graad 2.

Een andere aanpak had kunnen zijn via acties. Uit de cursus groepentheorie weten we dat D_8 de symmetrieën is van de vierkant. Indien de de vierkant tekenen in $\mathbb{R}^2$ met $(0, 0)$ als middelpunt van het vierkant, dan zijn er essentieel twee symmetrieën en deze komen overeen met a en b. Meer precies, a komt overeen met rotatie met 90 graden en b met spiegeling rond de rechte $y = -x$. Hierdoor voert D_8 een actie uit op $\mathbb{R}^2$ en de bijhorende representatie is gegeven door:

$$\psi : G \to \mathrm{GL}_2(\mathbb{R})$$

met

$$\psi(A) = \begin{pmatrix} \cos(\pi/2) & -\sin(\pi/2) \\ \sin(\pi/2) & \cos(\pi/2) \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ en } B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Voor de andere waarden *'breiden we ψ uit tot een homomorfisme'*. Hiermee bedoelen we dat we per definitie stellen dat

$$\psi(A^{i_1}B^{j_1}.\cdots.A^{i_l}B^{j_l}) := \psi(A)^{i_1}\psi(B)^{j_1}.\cdots.\psi(A)^{i_l}\psi(B)^{j_l}$$

voor alle $i_k, j_k \in \mathbb{Z}$. Hiermee 'forceren' we ψ tot een groepshomomorfisme. Hierbij moeten we wel opletten dat de relaties van D_8 geldig blijven (oefening).

3. De symmetrische groep S_3:

Stel $G = S_3 = \{(), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$, de symmetrische groep op 3 elementen. Stel $V = \mathbb{C}^3$ en kies als basis de standaardbasis

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} = \{e_1, e_2, e_3\}.$$

$$\rho : S_3 \to GL(\mathbb{C}^3) : g \mapsto \rho(g) : V \to V : e_i \mapsto e_{g(i)}, i = 1, 2, 3$$

Merk op dat $\rho(g)$ volledig bepaald is als het beeld van de basisvectoren van V onder $\rho(g)$ gekend is.

1.3.4 Systematische constructies

De voorgaande voorbeelden waren ad hoc. Maar gelukkig bestaan er heel veel methoden om representaties te maken. In deze sectie zullen we zien hoe de representaties van graad 1 te maken. Vervolgens vermelden we kort de noties 'Lifts', 'Restrictie' en 'Inductie'

Representaties van graad 1

Zij G, zoals steeds, een eindige groep. We wensen nu representaties van graad 1 te maken, d.w.z. groepshomomorfismen van de vorm $\rho : G \to K$. Om dit op een systematische manier te doen, hebben we de notie van de commutator deelgroep nodig.

Definitie 1.3.9. Zij $g, h \in H$. Dan heet

- $[g, h] = g^{-1}h^{-1}gh$ de *commutator* van g en h;
- $G' = \langle [g, h] \mid g, h \in G \rangle$ de *commutator* deelgroep van G.

Bijvoorbeeld indien G abels is, dan is $G' = \{e_G\}$. Om de commutator deelgroep te berekenen is volgende eigenschap handig. We laten het bewijs als oefening.

Eigenschap 1.3.10. *Zij G een eindige groep. Dan gelden de volgende eigenschappen:*

1. *G' is een normale deelgroep van G,*
2. *G/G' is abels*
3. *Indien $N \triangleleft G$ zodat G/N abels is, dan is $G' \subseteq N$.*

In woorden zegt de laatste eigenschap dat G' de kleinste normale deelgroep is zodat het quotiënt abels is. Het quotiënt wordt de *abelianisatie* van G genoemd en noteert men in de literatuur door G^{ab}. In de volgende resultaten zullen we een 'reductie-methode' zien om de 1-dimensionale representaties van een gegeven groep G te construeren.

Eigenschap 1.3.11. *Zij $\rho = G \to K^*$ een 1-dimensionale representatie van G. Dan geldt de volgende eigenschappen:*

1. *$G' \subseteq \ker(\rho)$*
2. *$\widetilde{\rho} : G/G' \to K^* : gG' \mapsto \rho(g)$ is een representatie van G/G'*

Bewijs. De eerste eigenschap volgt onmiddelijk uit de feit dat ρ een groepshomomorfisme is en dat $\rho(G) \subseteq K^*$ commutatief is.

Voor de tweede eigenschappen starten we met aan te tonen dat $\widetilde{\rho}$ goed-gedefinieerd is. Stel dat $g_1G' = g_2G'$. Dan is $g_1^{-1}g_2 \in G'$. Bijgevolg is

$$\widetilde{\rho}(g_1G') = \rho(g_1) = \rho(g_1)\rho(g_1^{-1}g_2) = \rho(g_2) = \widetilde{\rho}(g_2G').$$

□

Men zegt ook wel dat ρ een *groepshomomorfisme* $\widetilde{\rho}$ *induceert* op G/G'. Het omgekeerde procédé heet men 'lift'.

Definitie 1.3.12. Zij $\tau : G/G' \to K^*$ een 1-dimensionale representatie van G/G', dan heet de afbeelding

$$\widehat{\tau} : G \to K^* : g \mapsto \tau(gG')$$

de *lift* van τ tot G.

Opmerking. Merk op dat $\widehat{\psi}$ weldegelijk een groepshomomorfisme is (oefening) en bijgevolg een representatie van G.

Door de voorgaande constructies te combineren verkrijgen we nu een correspondentie tussen de 1-dimensionale representaties van G/G' en G.

Stelling 1.3.13. *Zij G een eindige groep. Dan is er een bijectie tussen de volgende verzamelingen*

$$\{\text{ 1-dim representaties van } G\} \underset{\Psi}{\overset{\Phi}{\rightleftharpoons}} \{\text{ 1-dim representaties van } G/G'\}$$

Bewijs. Meer concreet definiëren we

$$\Psi : \{ \text{ 1-dim repr. van G } \} \to \{ \text{ 1-dim repr. van G/G' } \} : \rho \mapsto \widetilde{\rho}$$

en

$$\Phi : \{ \text{ 1-dim repr. van G/G' } \} \to \{ \text{ 1-dim repr. van G } \} : \psi \mapsto \widehat{\psi}.$$

Wegens Eigenschap 1.3.11 en Definitie 1.3.12 zijn de afbeeldingen Ψ en Φ goed gedefinieerd. Er blijft aan te tonen dat $\Psi = \Phi^{-1}$. Dit volgt echter onmiddellijk uit de constructies (oefening). □

Later zullen we het tensor product van representaties definiëren. Hieruit zal volgen dat de verzameling van 1-dimensionale representaties een multiplicatieve structuur heeft.

Voor deze bewerking zal de verzameling zelfs een groep zijn en de afbeeldingen Ψ en Φ groepshomomorfismen. Meer algemeen, indien G abels is, zoals aangetoond zal worden in de oefeningen, is de verzameling $\{$ 1-dim representaties van $G\}$ steeds isomorf met G. Deze verzameling wordt ook wel *de duale van* G genoemd en genoteerd met $\widehat{G}$.

Lifts van representaties

De correspondentie in Stelling 1.3.13 is infeite een incarnatie van een veel algemener fenomeen.

Lemma 1.3.14. *Zij G een eindige groep en N een normale deelgroep van G. Dan geldt het volgende:*

1. *Zij $\rho : G \to \mathrm{GL}_n(K)$ een representatie van G zodat $N \subseteq \ker(\rho)$. Dan is*

$$\widetilde{\rho} : G/N \to \mathrm{GL}_n(K) : gN \mapsto \rho(g)$$

   een representatie van G/N.

2. *Zij $\tau : G/N \to \mathrm{GL}_n(K)$ een representatie van G/N. Dan is*

$$\widehat{\tau} : G \to \mathrm{GL}_n(K) : g \mapsto \tau(gN)$$

   een representatie van G, genaamd de lift van τ, met $N \subseteq \ker(\tau)$.

Het bewijs van de vorige lemma is analoog aan het geval waar $N = G'$. Verder merk op dat

$$\deg(\rho) = \deg(\widetilde{\rho}) \text{ en } \deg(\tau) = \deg(\widehat{\tau}).$$

Met behulp van deze opmerking en bovenstaande resultaat verkrijgen we, analoog aan Stelling 1.3.13, de volgende correspondentie.

Stelling 1.3.15. *Zij G een eindige groep en N een normale deelgroep van G. Dan is er een bijectie tussen de volgende verzamelingen*

$$\{ \text{ } n\text{-dim repr. } \rho \text{ van } G \text{ met } N \subseteq \ker(\rho)\} \underset{\Psi}{\overset{\Phi}{\rightleftharpoons}} \{ \text{ } n\text{-dim repr. } \tau \text{ van } G/N\}.$$

Hierbij is

$$\Phi(\rho) = \widetilde{\rho} \text{ en } \Psi(\tau) = \widehat{\tau}.$$

Restrictie en Inductie

Gegeven een groep G en een deelgroep H zullen we nu een methode zien om van representaties van G naar representaties van H te gaan en vice versa.

Om te starten stel dat $\rho : G \to \mathrm{GL}(V)$ een representatie is van G. De restrictie van ρ tot een deelgroep is duidelijk nog steeds een groepshomomorfisme. Vandaar:

Definitie 1.3.16. De homomorfisme

$$\rho|_H : H \to \mathrm{GL}(V) : h \mapsto \rho(h)$$

heet de *restrictie van ρ tot H*.

Meestal is het echter interessanter om vanuit een representatie van de kleinere groep H een representatie van de grotere groep G te kunnen construeren. Dit is het doel van 'inductie'. Helaas is zo'n constructie moeilijker dan die van restrictie. We zullen nu een concrete constructie bespreken.

Zij $\pi : H \to \mathrm{GL}(V)$ een representatie van H. Stel dat $n = [G : H]$. Dan is

$$G = g_1 H \ \dot\cup \ g_1 H \ \dot\cup \ \ldots \ \dot\cup \ g_n H \tag{1.2}$$

de disjuncte unie van n linker nevenklassen. De verzameling

$$\mathcal{T} = \{g_1, \ldots, g_n\}$$

heet een *transversaal* van H in G.

Om een representatie te maken moeten we eerst een representatie ruimte 'W' construeren. In niet formele taal is het idee om n isomorfe kopieën van V samen te nemen. Ieder van die kopieën labelen we met behulp van de elementen in de transversaal en laten nadien G ageren op deze labels. Meer wiskundig, construeer:

$$W := \bigoplus_{g_i \in \mathcal{T}} V^{(g_i)}$$

waarbij $V^{(g_i)} \cong V$ als een vectorruimte (dus infeite V_{g_i} is V maar waar de basis elementen van V een extra label 'g_i' krijgen). Dus elke element $w \in W$ kan geschreven worden als $\sum_{i=1}^{n} v_i^{(g_i)}$. Wegens (1.2) geldt dat voor iedere $g_i \in \mathcal{T}$ en $g \in G$:

$$g g_i = g_{j(i)} h_i$$

voor een $g_{j(i)} \in \mathcal{T}$ en $h_i \in H$. Daarom definieer:

$$\rho : G \to \mathrm{GL}(W) : g \mapsto \left(\rho_g : W \to W : \sum_{i=1}^{n} v_i^{(g_i)} \mapsto \sum_{i=1}^{n} \pi_{h_i}(v_i)^{(g_{j(i)})} \right)$$

De afbeelding ρ zullen we voortaan noteren als $\mathrm{Ind}_H^G(\pi)$.

Eigenschap 1.3.17. *Zij $H \leq G$ eindige groepen en $\pi : H \to \mathrm{GL}(V)$ een representatie van H. Dan is $Ind_H^G(\pi)$ een homomorfisme en dus een representatie van G.*

1.4 De bouwstenen

In de cursus 'Inleiding groepen theorie' is er worden gezien dat een groep G simpel heet indien $\{e_G\}$ en G de enige normale deelgroepen zijn van G. Bovendien bestaat er steeds deelgroepen $G_1, \ldots, G_l$ van G zodat G_i normaal is in G_{i-1},

$$\{e_G\} \subset G_l \subset \ldots \subset G_1 \subset G$$

en G_{i-1}/G_i een simpele groep is. Dus in een zekere zin is iedere eindige groep opgebouwd uit simpele groepen en vormen simpele groepen dus de bouwstenen van groepentheorie.

In deze sectie zullen we de bouwstenen van representatie theorie introduceren, de zogenaamde irreduciebele representaties.

1.4.1 Deelrepresentaties

Zij V een K-vectorruimte, G een eindige groep en $\rho : G \to \mathrm{GL}(V)$ een representatie van G. Herinner dat we de lineaire afbeelding $\rho(g)$ ook wel met ρ_g . wordt genoteerd.

Definitie 1.4.1. Veronderstel dat W een deelruimte is van V. Men zegt dat W invariant is onder de representatie van G (of ook, onder de actie van G op W) als voor alle $w \in W$ en alle $g \in G$,

$$\rho_g(w) \in W.$$

Dus de beperking van ρ_g tot W (deze noteren wij ρ_g^W of ook $(\rho_g)_{|W}$)

$$\rho_g^W : W \to W : w \mapsto \rho_g(w)$$

is een isomorfisme van de vectorruimte W naar zichzelf (dit is niet helemaal triviaal, denk hier even over na), en

$$\rho_{gh}^W = \rho_g^W \, \rho_h^W$$

voor alle $g, h \in G$. Bijgevolg is

$$\rho^W : G \to \mathrm{GL}(W) : g \mapsto \rho_g^W$$

een representatie van G in W. Men noemt dit een deelrepresentatie van G (of kortweg, een deelrepresentatie van ρ, of van V).

Voorbeeld 1.4.2. Beschouw de reguliere representatie ρ van G. Dus $V = K(G)$ de vrije K-vectorruimte met als basis $\{e_g \mid g \in G\}$. Definieer

$$e = \sum_{g \in G} e_g \,, \text{en } W = \mathrm{vect}_K\{e\} \,.$$

W is dus de deelruimte van V opgespannen door de vector e. Dan, voor elke $g \in G$,

$$\rho_g(e) = e.$$

Met andere woorden, elke vector van W wordt gefixeerd door ρ_g, en dat voor elke $g \in G$. Dus W is invariant onder ρ, en ρ^W is een deelrepresentatie van V. Omdat $\rho_g = 1_W$ voor alle $g \in G$, is deze isomorf met de triviale representatie.

Gegeven een G-invariante deelruimte W, weten we uit de cursus lineaire algebra dat men steeds een andere deelruimte W'' van V kan construeren zodat

$$V = W \oplus W''.$$

Echter, meestal zal W'' niet invariant zijn onder de representatie ρ van G. De stelling van Maschke, die fundamenteel is in de theorie, zegt dat men vanuit W'' nog andere complement W' kunnen construeren dat wel invariant is.

Stelling 1.4.3 (Maschke)**.** *Zij $\rho : G \to \mathrm{GL}(V)$ een representatie van G in V. Veronderstel dat $0 \neq |G| \in K$. Als W een invariante deelruimte is van V onder ρ, dan bestaat er een invariante deelruimte W' van V zodat*

$$V = W \oplus W'.$$

Dus W' is een G-invariant complement van W in V.

Bewijs. Zij W'' een willekeurig K-complement van W in V, d.w.z. W'' is een deelruimte van V zodat

$$V = W \oplus W''.$$

Zij $p : V \to W$ de projectie van V op W. Dus, als $v = w + w''$ met $v \in V$, $w \in W$ en $w'' \in W''$ dan $p(v) = w$. Beschouw dan de volgende lineaire afbeelding

$$p' = \frac{1}{|G|} \sum_{g \in G} \rho_g \circ p \circ \rho_g^{-1}.$$

We tonen aan dat p' een projectie is van V op W. Kies $v \in V$, dan geldt, met $v' = \rho_g^{-1}(v)$,

$$\rho_g(p(\rho_g^{-1}(v))) = \rho_g(p(v')) \in W\,,$$

omdat $p(v') \in W$ en W invariant is onder ρ, dus $p'(V) \subseteq W$.

Kies $w \in W$, nu volgt er dat

$$\rho_g(p(\rho_g^{-1}(w))) = \rho_g(\rho_g^{-1}(w)) = w$$

en dus

$$p'(w) = w.$$

Bijgevolg is

$$p' : V \to V : v \mapsto p'(v)$$

een projectie van V op W. Er volgt dat $W' = \ker(p')$ een complement voor deze projectie is, d.w.z.

$$V = W \oplus W'.$$

Ga zelf na als oefening dat voor alle $g \in G$, $\rho_g p' \rho_g^{-1} = p'$, waaruit

$$\rho_g p' = p' \rho_g,$$

voor alle $g \in G$.

Als nu $w' \in W'$ en $g \in G$ dan $p'(w') = 0$ en dus

$$p'(\rho_g(w')) = \rho_g(p'(w')) = 0.$$

Dus

$$\rho_g(w') \in W'$$

en W' is inderdaad een G-invariant complement van W in V. □

Gevolg 1.4.4. *Met de notaties en veronderstellingen van Stelling 1.4.3. Zij ρ^W en $\rho^{W'}$ de deelrepresentaties van ρ bekomen uit de deelruimten W en W'. Dan is*

$$\rho = \rho^W \oplus \rho^{W'} : G \to \mathrm{GL}(V)$$

met

$$\left(\rho_g^W \oplus \rho_g^{W'}\right)(w + w') = \rho_g(w) + \rho_g(w').$$

Men zegt dat ρ de directe som is van de representaties ρ^W en $\rho^{W'}$. Zij $R : G \to \mathrm{GL}_m(K)$ de geassocieerde afbeelding van ρ^W en $R' : G \to \mathrm{GL}_{m'}(K)$ de geassocieerde afbeelding van $\rho^{W'}$. Dus $m + m' = n = \dim_K(V)$. Dan is de geassocieerde afbeelding van $\rho : G \to \mathrm{GL}_n(K)$ gegeven door

$$g \mapsto \begin{pmatrix} R_g & 0 \\ 0 & R'_g \end{pmatrix}.$$

Analoog definieert men de directe som van een eindig aantal representaties. Dus als $R_i : G \to \mathrm{GL}_{n_i}(K)$ representaties zijn van de groep over het veld K, met $1 \leq i \leq m$, dan is de directe som

$$R_1 \oplus \cdots \oplus R_m : G \to \mathrm{GL}_{n_1 + \cdots n_m}(K)$$

met

$$g \mapsto \begin{pmatrix} (R_1)_g & 0 & 0 & \cdots & 0 & 0 \\ 0 & (R_2)_g & 0 & \cdots & 0 & 0 \\ \vdots & & & & \vdots & 0 \\ 0 & 0 & \cdots & \cdots & 0 & (R_m)_g \end{pmatrix}.$$

Indien R_i de matrixnotatie is van de representatie $\rho_i : G \to \mathrm{GL}(V_i)$ dan is $R_1 \oplus \cdots \oplus R_m$ de matrixnotatie van de representatie die wij noteren als $\rho_1 \oplus \cdots \oplus \rho_m$.

1.4.2 Irreducibele representaties

We hebben nu de nodige ingrediënten om de bouwstenen van representatie theorie te definieren.

Definitie 1.4.5. Zij $\rho : G \to \mathrm{GL}(V)$ een representatie van G en $V \neq \{0\}$. Dan noemt me ρ

- *irreducibel of simpel* indien V en $\{0\}$ de enige deelruimte van V zijn die invariant zijn onder G.
- *indecomposabel* indien er niet twee strikte deelruimten W en W' van V bestaan die invariant zijn onder G en zodat $V = W \oplus W'$.

Het is evident dat een representatie van graad 1 irreducibel is. Later zullen wij bewijzen dat elke niet-abelse groep ten minste één irreducibele representatie van graad verschillend van 1 heeft (over $\mathbb{C}$).

Verder merk op dat uit de definitie volgt dat iedere irreducibele representatie ook indecomposabel is. Omgekeerd, indien $0 \neq |G| \in K$, dan wegens Stelling 1.4.3 impliceert het bestaan van een niet-triviale echte G-invariante deelruimte dat ρ ook de direct som is van twee strikte deelrepresentaties. Bijgevolg in dit geval is elke indecomposabele representatie ook irreducibel. Samengevat, we hebben de volgende eigenschap.

Eigenschap 1.4.6. *Zij $\rho : G \to \mathrm{GL}(V)$ een representatie van G en $V \neq \{0\}$. Dan*

1. *Indien ρ irreducibel is, dan is ρ ook indecomposabel.*
2. *Indien $0 \neq |G| \in K$ en ρ is indecomposabel. Dan is ρ ook irreducibel.*

De conditie $0 \neq |G| \in K$ in het tweede punt is cruciaal. Zodra $|G| = 0$ in K (bv. $G = C_p$ en $K = \mathbb{Z}_p$) spreekt men van *modulaire representatie theorie* en in dit geval is het beschrijven van alle indecomposabele modulen nog steeds een actief onderzoeksdomein. Indien $0 \neq |G| \in K$ spreekt men ook wel van *klassieke representatie theorie* en deze cursus houd zich uitsluitend hiermee bezig.

De volgende herformulering van Mascke's stelling toont aan dat irreducibele representaties de bouwstenen zijn voor alle representaties.

Stelling 1.4.7 (Herformulering Maschke's stelling)**.** *Veronderstel $0 \neq |G| \in K$. Elke representatie $\rho : G \to \mathrm{GL}(V)$ van een eindige groep G in een vectorruimte V is de directe som van irreducibele representaties. Men zegt ook dat ρ volledig reducibel is.*

Bewijs. Wij bewijzen dit door inductie op $n = \dim_K(V)$. Een representatie van graad 1 is irreducibel, het geval $n = 1$ is dus bewezen. Veronderstel $n > 1$. Als ρ irreducibel is dan is er niets te bewijzen. Als ρ reducibel is, dan bestaan er door Stelling 1.4.3 invariante deelruimten W en W' zodat $\rho = \rho^W \oplus \rho^{W'}$, met $0 < \dim_K(W) < n$ en $0 < \dim_K(W') < n$. Wegens de inductiehypothese zijn ρ^W en $\rho^{W'}$ directe sommen van irreducibele representaties. Dus $\rho^W = \rho^{W_1} \oplus \cdots \oplus \rho^{W_k}$ en $\rho^{W'} = \rho^{W'_1} \oplus \cdots \oplus \rho^{W'_l}$ voor niet-nul invariante deelruimten van W respectievelijk W'. We mogen dus besluiten dat

$$\rho = \rho^{W_1} \oplus \cdots \oplus \rho^{W_k} \oplus \rho^{W'_1} \oplus \cdots \oplus \rho^{W'_l},$$

met alle ρ^{W_i} en $\rho^{W'_i}$ irreducibele representaties. □

Wij merken op dat de directe som ontbinding in irreducibelen **niet uniek** is. Inderdaad, neem bijvoorbeeld de triviale representatie $\rho : G \to \mathrm{GL}(V)$ met $\dim_K(V) = n > 2$. Dan kan men V op vele manieren als directe som van 1-dimensionale deelruimten schrijven. Omdat ρ de triviale representatie is, is elke deelruimte invariant en dus is V op vele manieren te schrijven als een som van irreducibelen.

Enkele voorbeelden

In Sectie 1.3.3 hebben we merdere voorbeelden gezien van representaties. Vervolgens hebben we enkele systematische constructies tegenkomen. We gaan nu hierop kort terugkomen.

De cyclische groep:

Zij $C_n = \langle g \mid g^n = 1 \rangle$ de cyclische groep van orde n. Dan hebben we de volgende verzameling aan representaties geconstrueerd:

$$\rho : C_n \to \mathbb{C} : g^i \mapsto \zeta_n^i$$

met ζ_n een primitieve n-de eenheidswortel. Al deze representaties zijn irreduciebel, want ze graad 1 hebben. Inderdaad zij W een deelruimte van $\mathbb{C}$. Dan is $\dim(W) \leq \dim \mathbb{C} = 1$. Bijgevolg is W of gelijk aan $\{0\}$ of $\mathbb{C}$. Deze argument werkt duidelijk in volledige algemeenheid:

Eigenschap 1.4.8. *Zij G een eindige groep en $\rho : G \to K^*$ een representatie van graad 1. Dan is ρ irreduciebel*

De diëdergroep:

Beschouw nu $D_8 = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle$. De representaties van graad 2 dat we hebben geconstrueerd zijn ook irreduciebel. Met de definitie is dit echter niet zo

eenvoudig om aan te tonen. Later zullen we een eenvoudige methode zien via karakters om dit aan te tonen.

De symmetrisch groep S_3:

Merk op dat uit Eigenschap 1.3.6 volgt dat de representatie van S_3 dat we voordien geconstrueerd hebben infeite isomorf is met de reguliere representatie van S_3. Bijgevolg levert Voorbeeld 1.4.2 een niet-triviale echte deelrepresentatie op.

Lifts van representaties:

Zij N een normale deelgroep van G, $\tau : G/N \to \mathrm{GL}(V)$ een representatie van G/N en $\widehat{\tau}$ de lift tot G. Dan geldt het volgende.

Eigenschap 1.4.9. *De representatie $\widehat{\tau}$ is irreduciebel als en slechts als τ irreduciebel is.*

Bewijs. Zij W een deelruimte van V. Veronderstel eerst dat het G/N-invariant is, i.e. voor alle $g \in G$ en $w \in W$ is $\tau(gN)(w) \in W$. Maar dan is ook $\widehat{\tau}(g)(w) = \tau(gN)(w) \in W$. Bijgevolg is W ook G-invariant. Het omgekeerde is analoog. Dus $\widehat{\tau}$ heeft een invariante deelruimte (en dus deelrepresentatie) als en slechts als τ er een heeft. Dit toont de eigenschap aan. □

Irreducibele voor G abels via Shur's Lemma

De volgende stelling zal nog verbazend vaak opduiken.

Stelling 1.4.10 (Het Lemma van Schur)**.** *Zij $\rho^1 : G \to \mathrm{GL}(V_1)$ en $\rho^2 : G \to \mathrm{GL}(V_2)$ twee irreducibele representaties van de groep G. Zij $f : V_1 \to V_2$ een K-lineaire transformatie zodat $\rho^2_g \circ f = f \circ \rho^1_g$, voor alle $g \in G$. Dan:*

1. *$f = 0$ of f is een isomorfisme,*
2. *als ρ^1 en ρ^2 niet equivalent zijn dan $f = 0$.*
3. *als $K = \mathbb{C}$, $V_1 = V_2$ en $\rho^1 = \rho^2$ dan is f een homotetie, d.w.z. $f = c1_{V_1}$ voor een $c \in \mathbb{C}$.*

Bewijs. Zij $W_1 = \ker(f)$, d.w.z., $\ker(f) = \{v_1 \in V_1 \mid f(v_1) = 0\}$. Dit is een deelruimte van V_1. Wij tonen nu aan dat het ook G-invariant is. Inderdaad, zij $g \in G$ en $w_1 \in \ker(f)$. Dan volgt uit het gegeven dat $(f\rho^1_g)(w_1) = \rho^2_g(f(w_1)) = 0$ en dus $\rho^1_g(w_1) \in \ker(f)$. Omdat per veronderstelling ρ^1 een irreducibele representatie is volgt er dat $\ker(f) = \{0\}$

of $\ker(f) = V_1$. In het laatste geval is $f = 0$. Veronderstel dus dat $f \neq 0$; dus $\ker(f) = \{0\}$, of m.a.w. f is injectief.

Zij $W_2 = \mathrm{Im}\,(f)$, het beeld van f. Dan is W_2 een deelruimte van V_2. Wij tonen nu aan dat W_2 een G-invariante deelruimte is. Inderdaad, zij $w_2 = f(v_1) \in W_2$, met $v_1 \in V_1$. Dan volgt weer uit het gegeven dat $\rho^2_g(w_2) = \rho^2_g(f(v_1)) = f(\rho^1_g(v_1) \in \mathrm{Im}\,(f)$. Omdat ρ^2 irreducibel is volgt er dat $W_2 = \{0\}$ of $W_2 = V_2$. Het eerste betekent $f = 0$ en het tweede betekent dat f surjectief is.

Wij besluiten bijgevolg dat ofwel $f = 0$, ofwel f is een isomorfisme. Dit bewijst het eerste gedeelte van de eigenschap.

Voor het tweede gedeelte, veronderstel dat $f \neq 0$. Dan volgt uit deel 1 dat f een isomorfisme is, en dus zijn ρ^1 en ρ^2 equivalent.

Voor het derde gedeelte veronderstellen wij $K = \mathbb{C}$, $V_1 = V_2$ en $\rho^1 = \rho^2$. Omdat $K = \mathbb{C}$ bestaat er een eigenwaarde $c \in \mathbb{C}$ van f. Zij v een bijhorende (niet-nul) eigenvector van f en zij $f' := f - c1_{V_1}$. Dan $f'(v) = f(v) - cv = 0$. Dus $\ker(f') \neq \{0\}$. Bovendien $\rho^2_g \circ f' = \rho^2_g \circ f - c1_{V_1} \circ \rho^2_g = f \circ \rho^1_g - c1_{V_1} \circ \rho^1_g = f' \circ \rho^1_g$ voor alle $g \in G$. Dus volgt uit deel 1 dat $f' = 0$, m.a.w., $f = c1_{V_1}$. □

Hiermee kunnen we aantonen dat abelse groepen uitsluitend 1-dimensionale irreduciebele representaties hebben. Later zullen we zien dat deze eigenschap abelse groepen karakteriseert.

Eigenschap 1.4.11. *Zij G een eindige abelse groep en $\rho : G \to \mathrm{GL}(V)$ een irreducibele representatie van G over $\mathbb{C}$. Dan is* $\dim V = 1$.

Bewijs. Veronderstel dat $\dim V > 1$. Het bewijs bestaat uit twee stappen.

Stap 1: Voor alle $g \in G$ bestaat er een $c_g \in \mathbb{C}$ zodat $\rho_g = c_g 1_V$.

Stap 2: Zij $v \in V$. Dan is $\mathrm{vect}_{\mathbb{C}}\{v\}$ een G-invariante deelruimte.

Zodra $\dim V > 1$ levert de tweede stap de gewenste contradictie op met de irreducibiliteit van ρ. We zullen nu de twee bovenstaande uitspraken aantonen.

De eerste uitspraak doet sterk denken aan het Lemma van Schur. Neem $g \in G$ vast. Om het derde deel van Schur's Lemma toe te passen moeten we aantonen dat $\rho_h \circ \rho_g = \rho_g \circ \rho_h$ voor alle $h \in G$. Dit volgt echter uit de feit dat G abels is en ρ een groepshomomorfisme. Bijgevolg zegt Stelling 1.4.10 dat $\rho_g = c_g 1_V$ voor een $c_g \in \mathbb{C}$.

De tweede uitspraak volgt onmiddellijk uit de eerste. □

Meer algemeen geldt de volgende stelling.

Stelling 1.4.12 (Ito's stelling)**.** *Zij G een eindige groep, N een abelse deelgroep van G en $\rho : G \to \mathrm{GL}_n(K)$ een irreduciebele representatie van G. Dan is*

$$n \leq [G : N].$$

Bovendien als N normaal is in G, dan is $n \mid [G : N]$.

Indien G abels, kan men N gelijk aan G nemen. Bijgevolg is de vorige stelling inderdaad een veralgemening van Eigenschap 1.4.11. Een voorbeeld van een abelse normale deelgroep is steeds het centrum $\mathcal{Z}(G) = \{g \in G \mid hg = gh \text{ voor alle } h \in G\}$. Dus men heeft steeds dat de graad van een irreduciebele representatie een deler is van $|G/\mathcal{Z}(G)|$ (en i.h.b. een deler van $|G|$.

1.5 Karakters

Zij $f : V \to V$ een lineare transformatie van een K-vectorruimte V met matrix $f_{[E,E]} = (f_{ij})$ ten opzichte van de basis $E = \{e_i \mid 1 \leq i \leq n\}$. Het spoor van f is

$$\mathrm{Tr}(f) = \sum_{i=1}^{n} f_{ii}.$$

Bijgevolg, $\mathrm{Tr}(f)$ is de som van de eigenwaarden van f (waarbij men rekening houdt met de multipliciteit van een eigenwaarde). Ga na dat deze definitie onafhankelijk is van de gekozen basis.

Definitie 1.5.1. Zij $\rho : G \to \mathrm{GL}(V)$ een representatie van een eindige groep in de K-vectorruimte V. Dan noemt men

$$\chi_\rho : G \to K : g \mapsto \chi_\rho(g) = \mathrm{Tr}(\rho_g)$$

het karakter van de representatie ρ. Het karakter van een irreducibele representatie noemen wij een irreducibel karakter.

1.5.1 Basis eigenschappen

Unitaire matrices

Zij $\rho : G \to \mathrm{GL}(V)$ een representatie van G, met geassocieerde matrix representatie A_ρ, en V een vectorruimte over een veld K. Meestal zijn wij geïnteresseerd in het geval dat $K = \mathbb{C}$. In dit geval hebben de matrices $A_\rho(g)$ bijzonder goede eigenschappen zoals diagonaliseerbaarheid en unitair. We zullen dit nu aantonen.

Zij nu V een $\mathbb{C}$-vectorruimte en zij

$$(\mid) : V \times V \to \mathbb{C} : (v, w) \mapsto (v|w)$$

een inwendig product, d.w.z. deze afbeelding is sesquilineair, hermitisch ($(v|w) = \overline{(w|v)}$ voor $v, w \in V$) en positief definiet ($(v|v) > 0$ als $v \neq 0$). Wij kunnen dan deze inwendig product 'normaliseren[1] t.o.v. ρ', i.e. definieer

$$\langle \mid \rangle : V \times V \to \mathbb{C}$$

door

$$\langle v \mid w \rangle = \sum_{g \in G} (\rho(g)(v) \ \mid \ \rho(g)(w)).$$

Ga na als oefening dat deze afbeelding een inproduct op de $\mathbb{C}$-vectorruimte V definieert. Kies $h \in G$. Er volgt dat

$$\begin{aligned}
\langle \rho(h)(v) \mid \rho(h)(w) \rangle &= \sum_{g \in G} (\rho(g)(\rho(h)(v)) \mid \rho(g)(\rho(h)(w))) \\
&= \sum_{g \in G} (\rho(gh)(v) \mid \rho(gh)(w)) \\
&= \sum_{g \in G} (\rho(g)(v) \mid \rho(g)(w)) \\
&= \langle v \mid w \rangle.
\end{aligned}$$

Men zegt dat het inproduct $\langle \mid \rangle$ *invariant is voor* G. Bijgevolg, als $\{e_1, \ldots, e_n\}$ een orthonormale basis is van V voor het inwendig product $\langle | \rangle$ dan is voor elke $g \in G$,

$$\langle e_i \mid e_j \rangle = \delta_{i,j}$$

en

$$\langle \rho(g)e_i \mid \rho(g)e_j \rangle = \delta_{i,j}.$$

[1] Merk op dat we in het bewijs van Maschke's Stelling een gelijkaardige aanpassing uitgevoerd hebben.

Een vierkante matrix U over $\mathbb{C}$ is een unitaire matrix en slechts als $\overline{U}^T = U^{-1}$. Uit de lineaire algebra weten we dat een matrix unitair is als en slechts als U als lineaire afbeelding het inwendig product respecteert, i.e. U is een isometrie. Dit is precies wat we bekomen voor iedere matrix $A_\rho(g)$. Uit de cursus lineaire algebra weten we eveens dat iedere unitaire matrix diagonaliseerbaar is. Bijgevolg, omdat g van eindige orde is en dus $A_\rho(g)$ ook, zijn de eigenwaarden van $A_\rho(g)$ $o(g)$-de eenheidswortels. We bekomen dus de volgende resultaat.

Eigenschap 1.5.2. *Zij G een eindige groep en ρ een complexe representatie van G. Dan gelden de volgende eigenschappen:*

1. *$A_\rho(g)$ is unitair voor iedere $g \in G$*
2. *$A_\rho(g)$ is diagonaliseerbaar met $o(g)$-de eenheidswortels.*

Eigenschappen

We hebben nu de nodige ingrediënten om de volgende essentiële eigenschappen van karakters aan te tonen.

Eigenschap 1.5.3. *Zij χ het karakter van een representatie ρ van graad n. Zij $g, h \in G$. Dan gelden de volgende eigenschappen:*

1. *$\chi(e_G) = n$,*
2. *$\chi(gh) = \chi(hg)$,*
3. *$\chi(hgh^{-1}) = \chi(g)$, m.a.w. het karakter χ is constant op elk van de conjugatie-klassen van G,*
4. *als $K = \mathbb{C}$ dan $\chi(g^{-1}) = \overline{\chi(g)}$,*
5. *als $K = \mathbb{C}$ dan $|\chi(g)| \leq \chi(e_G)$.*

Bewijs. Omdat $\rho(e_G) = 1_V \in \mathrm{GL}(V)$, en met de identieke van $\mathrm{GL}(V)$ de eenheidsmatrix correspondeert, is het duidelijk dat $\chi(e_G) = n$. Als $A, B \in M_n(K)$ dan is het welbekend dat $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$. Dus volgt $\chi(gh) = \chi(hg)$ voor alle $g, h \in G$. Er volgt dan ook dat $\chi(hgh^{-1}) = \chi(h^{-1}hg) = \chi(g)$.

Veronderstel nu dat $K = \mathbb{C}$ en $g \in G$. Wegens Eigenschap 1.5.2 zijn de matrices $A_\rho(g)$ unitair is. Dus $A_\rho(g)^{-1} = \overline{A_\rho(g)}^T$, en dus $\chi(g^{-1}) = \overline{\chi(g)}$.

We tonen nu de laatste eigenschap aan. Zij A_ρ de matrix representatie geassocieerd aan ρ. Wegens Eigenschap 1.5.2, en stelling van Lagrange, bestaat er een inverteerbare matrix $P \in \mathrm{GL}_n(\mathbb{C})$ en $|G|$-de eenheidswortels $\zeta_1, \ldots, \zeta_n$ zodat

$$A_\rho(g) = P^{-1} \begin{pmatrix} \zeta_1 & 0 & \ldots & 0 \\ 0 & \zeta_2 & 0 & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \zeta_n \end{pmatrix} P.$$

In het bijzonder is $\chi(g) = \zeta_1 + \ldots + \zeta_n$. Zodoende verkrijgen we het gewenste:

$$|\chi(g)| \leq \sum_{i=1}^{n} |\zeta_i| = n = \chi(e_G).$$

□

De verzameling

$$\mathcal{Z}(\chi) := \{g \in G \mid |\chi(g)| = \chi(e_G)\}$$

heet het *centrum van de karakter* χ. Verder heet

$$\ker(\chi) := \{g \in G \mid \chi(g) = \chi(e_G)\}$$

de *kern van de karakter* χ. De komt van het volgende.

Eigenschap 1.5.4. *Zij $\rho : G \to GL(V)$ een representatie van G en zij χ_ρ het bijhorende karakter. Dan is $\ker(\rho) = \ker(\chi_\rho)$. In het bijzonder is $\ker \chi_\rho \triangleleft G$.*

Bewijs. Per definitie $\ker(\rho) = \{g \in G \mid \rho_g = 1_V\}$. Indien $g \in \ker(\rho)$ dan is wegens Eigenschap 1.5.3

$$\chi_\rho(g) = \mathrm{Tr}(\rho_g) = \mathrm{Tr}(1_V) = \dim V = \chi(e_G).$$

Omgekeerd neem $g \in \ker(\chi_\rho)$. Zoals in het bewijs van Eigenschap 1.5.3, volgt uit Eigenschap 1.5.2 dat $\chi_\rho(g) = \sum_{i=1}^{n} \zeta_i$ met $n = \dim V$ en ζ_i een $|G|$-de eenheidswortel. Omdat $g \in \ker(\chi_\rho)$, hebben we dus dat

$$n = \sum_{i=1}^{n} \zeta_i.$$

Het is een eenvoudige oefening in complexe analyse dat dit mogelijk is als en slechts als $\zeta_i = 1$ voor alle i. Bijgevolg verkrijgen we de omgekeerde inclusie. □

Infeite kan men veel meer aantonen.

Stelling 1.5.5. *Zij $N \triangleleft G$ eindige groepen. Dan bestaan er irreduciebele representaties $\rho_1, \ldots, \rho_m$ van G zodat*

$$N = \bigcap_{i=1}^{m} \ker(\chi_{\rho_i}).$$

We zullen zien dat de verzameling van alle karakters van een gegeven groep G een rijke structuur heeft (het zal zowel een zogenaamde K-algebra zijn en de vectorruimten van alle klassefuncties voortbrengen). Een eerste bewerking dat men heeft op de verzameling van alle karakters is de optelling.

Eigenschap 1.5.6. *Zij $\rho^1 : G \to \mathrm{GL}(V_1)$ en $\rho^2 : G \to \mathrm{GL}(V_2)$ twee representaties van een eindige groep G en zij χ^1 en χ^2 hun karakters. Dan is*

$$\chi_{\rho^1 \oplus \rho^2} = \chi^1 + \chi^2.$$

Bewijs. Zij A_{ρ_1} en A_{ρ_2} de geassocieerde matrix representaties van ρ^1 en ρ^2. De representatie van $\rho := \rho^1 \oplus \rho^2$ is gegeven door

$$g \mapsto A_\rho(g) = \begin{pmatrix} A_{\rho_1}(g) & 0 \\ 0 & A_{\rho_2}(g) \end{pmatrix},$$

met $g \in G$. Dus

$$\mathrm{Tr}(A_\rho(g)) = \mathrm{Tr}(A_{\rho_1}(g)) + \mathrm{Tr}(A_{\rho_2}(g))$$

en bijgevolg

$$\chi(g) = \chi^1(g) + \chi^2(g) = (\chi^1 + \chi^2)(g).$$

□

Opmerking. Zij N een normale deelgroep van G en beschouw het quotiënt G/N als de verzameling van alle linker neveklassen van N in G. Dan voert N een linker actie uit op G/N via linker vermenigvuldiging:

$$\varphi : N \times G/N \to G/N : (m, gN) \mapsto (mg)N.$$

Zij ρ de permutatierepresentatie geassocieerd aan φ (cf. Sectie 1.3.2). Wegens Stelling 1.4.7 bestaan er irreduciebele representaties $\rho_1, \ldots, \rho_m$ van G zodat

$$\rho = \rho_1 \oplus \cdots \oplus \rho_m.$$

Men kan aan aantonen dat $N = \bigcap_{i=1}^{m} \ker \chi_{\rho_i}$ (hetgeen Stelling 1.5.5 zou aantonen).

1.5.2 Karakters versus Representaties

Zij G een eindige groep. We definiëren een afbeelding als volgt:

$$(\,|\,) : \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C} : (\phi|\psi) = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}\,.$$

Het is eenvoudig na te gaan dat deze afbeelding een inwendig product is op de vectorruimte $\mathbb{C}^G$. Dit inproduct, gecombineerd met karakters, levert eenvoudige (en rekenkundige) methodes op om allerlei eigenschappen na te gaan. Een voorbeeld hiervan zal zijn irreducibiliteit. Maar eerst tonen we aan dat de irreducibele complexe karakters een orthonormale verzameling vormen (wiens bewijs in een latere sectie zal volgen).

Stelling 1.5.7 (Rij-Orthogonaliteitsrelaties)**.** *Als χ een irreducibel complex karakter van een eindige groep is dan*

$$(\chi|\chi) = 1.$$

Als χ en χ' irreducibele complexe karakters zijn van twee niet equivalente irreducibele complexe representaties van een eindige groep dan

$$(\chi|\chi') = 0.$$

In Stelling 1.4.7, hebben we aangetoond dat elke complexe representatie een directe som is van irreducibele complexe representaties. Gebruikmakend van het vorige resultaat berekenen wij nu het aantal keer dat een irreducibele component voorkomt in deze som.

Stelling 1.5.8. *Zij ϕ het karakter van een complexe representatie ρ van een eindige groep G en veronderstel dat*

$$\rho = \rho^1 \oplus \cdots \oplus \rho^k,$$

een directe som van irreducibele complexe representaties. Als ρ' een irreducibele complexe representatie is van G met karakter χ', dan is het aantal ρ^i equivalent met ρ' gelijk aan

$$(\phi|\chi') = \langle \phi, \chi' \rangle.$$

Wij noemen dit de multipliciteit van ρ' in ρ. Merk op dat het vorige aantoont dat de multipliciteit onafhankelijk is van de gekozen ontbinding als een directe som.

Bewijs. Zij χ_i het karakter van ρ^i. Wegens Eigenschap 1.6.7 weten wij dat

$$\phi = \chi_1 + \cdots + \chi_k.$$

Dus

$$(\phi|\chi') = (\chi_1|\chi') + \cdots + (\chi_k|\chi').$$

Wegens Stelling 1.5.7 weten wij dat $(\chi_i|\chi') = 0$ als ρ^i en ρ' niet equivalent zijn, anders $(\chi_i|\chi') = 1$. Dus volgt het resultaat. □

Gevolg 1.5.9. *Twee complexe representaties zijn equivalent als en slechts als zij hetzelfde karakter hebben.*

Bewijs. Wij weten reeds dat equivalente complexe representaties hetzelfde karakter hebben. Omgekeerd, uit Stelling 1.5.8 volgt dat twee representaties met hetzelfde karakter equivalente directe som ontbindingen hebben. □

Dit resultaat reduceert de studie van complexe representaties van een eindige groep G tot een studie van complexe karakters. De volgende stelling karakteriseert een irreducibele representatie in termen van haar karakter.

Stelling 1.5.10. *Zij ϕ het karakter van een complexe representatie ρ. Dan $(\phi|\phi) \in \mathbb{N}$ en $(\phi|\phi) = 1$ als en slechts als ρ irreducibel is.*

Bewijs. Zij ρ een complexe representatie. Dan is ρ de directe som van irreducibele representaties

$$\rho = \underbrace{\rho^1 \oplus \cdots \oplus \rho^1}_{m_1} \oplus \cdots \oplus \underbrace{\rho^k \oplus \cdots \oplus \rho^k}_{m_k},$$

een directe som van irreducibele representaties ρ^i met geassocieerd karakter χ_i, $m_i \in \mathbb{N}$ en ρ^i niet isomorf met ρ^j als $i \neq j$. Het karakter ϕ van ρ is dan

$$\phi = m_1\chi_1 + \cdots + m_k\chi_k$$

en

$$m_i = (\phi|\chi_i).$$

Wegens de orthogonaliteitsrelaties verkrijgen wij dan

$$(\phi|\phi) = \sum_{i=1}^{k} m_i^2.$$

Het is duidelijk dat $\sum_{i=1}^{k} m_i^2 = 1$ als en slechts als $k = 1$ en $m_1 = 1$, dus precies wanneer ρ irreducibel is. □

1.5.3 Karakters als basis voor Klassefuncties

De conjugatieklasse van $h \in G$ is de verzameling

$$\mathcal{C}_h = \{ghg^{-1} \mid g \in G\}.$$

De orbit-stabilisatorstelling heeft als gevolg

$$|\mathcal{C}_h| = [G : C_G(h)],$$

de index van de stabilisator $C_G(h)$ van h in G.

Definitie 1.5.11. Zij G een eindige groep. Wij noemen een functie $f : G \to \mathbb{C}$ een klassefunctie als $f(ghg^{-1}) = f(h)$ voor alle $g, h \in G$.

In Eigenschap 1.5.3 (iii) hebben we aangetoond dat een karakter constant is op een conjugatieklasse. Karakters zijn dus voorbeelden van klassefuncties.

Eigenschap 1.5.12. *Zij f een klassefunctie op G en zij $\rho : G \to \mathrm{GL}(V)$ een complexe representatie van G. Definieer de volgende lineaire afbeelding $V \to V$:*

$$\Lambda_f = \sum_{g \in G} f(g)\rho_g.$$

Als ρ irreducibel is van graad n en χ als bijhorend karakter heeft, dan

$$\Lambda_f = c1_V$$

met

$$c = \frac{1}{n}\sum_{g \in G} f(g)\chi(g) = \frac{|G|}{n}(f|\overline{\chi}).$$

Bewijs. Zij $h \in G$. Dan

$$\rho_h^{-1} \circ \Lambda_f \circ \rho_h = \sum_{g \in G} f(g)\rho_{h^{-1}}\rho_g\rho_h = \sum_{g \in G} f(g)\rho_{h^{-1}gh}.$$

Er volgt dat

$$\rho_h^{-1}\Lambda_f\rho_h = \sum_{x \in G} f(hxh^{-1})\rho_x.$$

Omdat f constant is op conjugatieklassen volgt er dan

$$\rho_h^{-1}\Lambda_f\rho_h = \sum_{x \in G} f(x)\rho_x = \Lambda_f.$$

Dus hebben wij aangetoond dat, voor alle $h \in G$,

$$\Lambda_f \circ \rho_h = \rho_h \circ \Lambda_f.$$

Wegens het Lemma van Schur (Stelling 1.4.10), volgt er dat $\Lambda_f = c1_V$ voor een $c \in \mathbb{C}$. Verder is

$$nc = \mathrm{Tr}(c1_V) = \sum_{g \in G} f(g)\,\mathrm{Tr}(\rho_g) = \sum_{g \in G} f(g)\chi(g).$$

Bijgevolg

$$c = \frac{1}{n}\sum_{g \in G} f(g)\chi(g) = \frac{|G|}{n}\,(f|\overline{\chi}).$$

□

De verzameling van klassefuncties, samen met de puntsgewijze optelling en scalaire vermenigvuldiging, vormt een $\mathbb{C}$-vectorruimte, genoteerd als H.

Stelling 1.5.13. *Zij $\chi_1, \ldots, \chi_k$ de irreducibele complexe karakters van een eindige groep G. Dan is $\{\chi_1, \ldots, \chi_k\}$ een orthonormale basis van de vectorruimte H van de klassefuncties.*

Bewijs. Wegens de orthogonaliteitsrelaties weten wij dat $\{\chi_1, \ldots, \chi_k\}$ een orthonormale verzameling is van H. Hieruit volgt onmiddelijk dat ze ook een lineair onafhankelijke deelverzameling van H vormen (oefening). Zij $W = \mathrm{span}\{\chi_1, \ldots, \chi_k\}$. Er blijft te bewijzen dat de verzameling voortbrengend is, i.e. $W = H$. Uit de cursus Lineaire Algebra weten we dat

$$H = W \oplus W^\perp$$

waar $W^\perp = \{f \in H \mid (f|\chi_i) = 0 \text{ voor alle } 1 \leq i \leq k\}$ het orthogonaal complement is van W. Het is dus voldoende om aan te tonen dat $W^\perp = 0$.

Bijgevolg veronderstel dat $(f|\chi_i) = 0$ voor $1 \leq i \leq k$. Uit $\overline{\chi_i(g)} = \chi_i(g^{-1})$ en de definitie van $(\,|\,)$ volgt dat $(f|\chi_i) = (f^*|\overline{\chi_i})$ met $f^* : G \to \mathbb{C} : g \mapsto f(g^{-1})$.

Dus we weten dat $(f^*|\overline{\chi_i}) = 0$ voor $1 \leq i \leq k$. Voor zulke functie f^* weten wij wegens Eigenschap 1.5.12 dat $\Lambda_{f^*} = 0$ voor elke irreducibele complexe representatie ρ van G. Omdat elke representatie de directe som is van irreducibele representaties (Stelling 1.4.7) volgt er dat $\Lambda_{f^*} = 0$ voor elke representatie ρ. Passen wij dit nu toe voor de reguliere complexe representatie R dan volgt er

$$0 = \Lambda_{f*}(e_{e_G}) = \sum_{g \in G} f^*(g)R_g(e_{e_G}) = \sum_{g \in G} f^*(g)e_g.$$

Dus $f^*(g) = 0$ voor alle $g \in G$, m.a.w., $f^* = 0$. Maar bijgevolg is ook $f = 0$, zoals gewenst. □

1.5.4 Karaktertabel

Herinner dat twee basissen van een vectorruimte steeds dezelfde kardinaliteit hebben. Naast de irreduciebele karakters bestaat er nog een andere interessante basis voor de vectorruimte bestaande uit klassefuncties.

Stelling 1.5.14. *Het aantal irreducibele complexe representaties van een eindige groep G (op equivalentie na) is gelijk aan het aantal conjugatieklassen van G.*

Bewijs. Zij $C_1, \ldots, C_m$ de verschillende conjugatieklassen van G. Beschouw de indicator functie $I_{C_i} : G \to \mathbb{C}$ dat gedefinieerd is als volgt:

$$I_{C_i}(g) = \begin{cases} 1 & \text{als } g \in C_i \\ 0 & \text{als } g \notin C_i \end{cases}$$

Deze functies I_{C_i} zijn duidelijk klassefuncties. Het is bovendien eenvoudig na te gaan dat $\{I_{C_1}, \ldots, I_{C_m}\}$ een $\mathbb{C}$-basis vormen voor H. Wegens Stelling 1.5.13 volgt er dat m gelijk is aan het aantal irreducieble representaties (op equivalentie na). □

De irreduciebele karakters $\{\chi_1, \ldots, \chi_m\}$ en hun waarden op elke conjugatie klassen wordt gewoonlijk weergegeven door de zogenaamde *karaktertabel*. Dit is het rooster waarvan de rijen gelabeld worden met de irreduciebele karakters en de kolommen met conjugatieklassen. Op plaats (i, j) in het rooster staat de waarde van χ_i op de conjugatie klasse C_j. Wegens Stelling 1.5.14 is de karakter tabel een $m \times m$-rooster. Met behulp van deze visuele steun wordt de naam van Stelling 1.5.7 ook duidelijker. Inderdaad de rij-orthogonaliteitsrelaties drukken uit hoe het inproduct van 'rij χ_i' is met 'rij χ_j'. De volgende resultaat zegt wat het inproduct is van 'kolom C_i' met 'kolom C_j' van de karaktertabel.

Eigenschap 1.5.15 (Kolom-orthogonaliteitsrelaties)**.** *Zij $\chi_1, \ldots, \chi_k$ de irreducibele complexe karakters van G. Zij $g \in G$ en stel $c(g) = |\mathcal{C}_g|$, het aantal elementen in de conjugatieklasse van g. Dan*

1. $\sum_{i=1}^{k} \overline{\chi_i(g)}\chi_i(g) = \frac{|G|}{c(g)}$,
2. *voor elke g die niet geconjugeerd is met h, geldt* $\sum_{i=1}^{k} \overline{\chi_i(h)}\chi_i(g) = 0$.

Bewijs. Zij $f_g : G \to \mathbb{C}$ zodat $f_g(h) = 1$ als $h \in \mathcal{C}_g$ en $f_g(h) = 0$ als $h \notin \mathcal{C}_g$. Omdat f_g een klassefunctie is volgt er uit Stelling 1.5.13 dat

$$f_g = \sum_{i=1}^{k} c_i \chi_i$$

met

$$c_i = (f_g \mid \chi_i) = \frac{c(g)}{|G|}\overline{\chi_i(g)}.$$

Dus, voor elke $h \in G$,

$$f_g(h) = \frac{c(g)}{|G|}\sum_{i=1}^{k} \overline{\chi_i(g)}\,\chi_i(h).$$

Nemen wij $g = h$ dan volgt het eerste gedeelte van de eigenschap. Als h en g niet geconjugeerd zijn dan volgt het tweede gedeelte. □

Omdat een karakter χ constant is op een conjugatieklasse C noteren wij dikwijls

$$\chi(C) = \chi(g)$$

als $g \in C$.

Stelling 1.5.16. *Zij G een eindige groep. Dan is G abels als en slechts als alle irreducibele complexe representaties graad 1 hebben. Bovendien is er in dit geval precies $|G|$ irreducibele complexe representaties.*

Bewijs. Uit Eigenschap 1.4.11 weten we reeds dat als G abels is dat dan alle irreduciebele representaties graad 1 hebben.

Omgekeerd veronderstel dat alle irreduciebele representaties graad 1 hebben. Zij k de aantal conjugatieklassen van G. Neem $g = 1$ in de eerste formula van Eigenschap 1.5.15. Dan bekomen we dat

$$\sum_{i=1}^{k} \overline{\chi_i(1)}\chi_i(1) = \sum_{i=1}^{|G|} \chi_i(1)^2 = |G|.$$

Maar $\chi_i(1) = 1$. Dus bekomen we dat $k = |G|$. Bijgevolg bestaat iedere conjugatieklasse uit een singelton (i.e. $\mathcal{C}(g) = \{g\}$). Hieruit volgt elke $g \in \mathcal{Z}(G)$ en dus $G = \mathcal{Z}(G)$ abels.

De 'bovendien' volgt nu uit Stelling 1.5.14 want als G abels is dan bestaat iedere conjugatieklasse uit een singelton (i.e. $\mathcal{C}(g) = \{g\}$). □

Gevolg 1.5.17. *Een niet-abelse, eindige groep G, heeft steeds een irreducibele complexe representatie van graad strikt groter dan* 1.

1.5.5 Nuttige identiteiten en overblijvende bewijzen

Via de reguliere representatie

We beschouwen nu de reguliere representatie over de complexe getallen, i.e. ρ is een homomorfisme van G naar de vrije vectorruimte $\mathbb{C}(G)$ over het veld $\mathbb{C}$.

Eigenschap 1.5.18. *Veronderstel dat G een eindige groep is, en r_G het karakter van de reguliere representatie van G over de complexe getallen. Dan is*

$$r_G(g) = \begin{cases} 0 & \text{als } g \neq e_G \\ |G| & \text{als } g = e_G \end{cases}$$

Bewijs. Noteer de reguliere representatie als ρ. Merk op dat $\rho_g(e_h) = e_{gh}$. Ten opzichte van de standaardbasis $\{e_g | g \in G\}$ is de matrixvoorstelling R_g dus een permutatiematrix. Dus elke kolom van R_g bevat precies één 1 en voor de rest allemaal nullen. Aangezien als $g \neq e_G$ dan $gh \neq h$, voor alle $h \in G$, zijn de diagonaalelementen van de matrix van R_g allemaal 0. Bijgevolg $r_G(g) = \mathrm{Tr}(\rho_g) = 0$ als $g \neq e_G$. Anderzijds hebben wij dat $r_G(e_G) = \mathrm{Tr}(\rho_{e_G}) = |G|$. □

Eigenschap 1.5.19. *Zij ρ een irreducibele complexe representatie van graad n van een eindige groep G. Dan is de multipliciteit van ρ in de reguliere complexe representatie van G gelijk aan n.*

Bewijs. Zij χ het karakter van ρ. Wegens Eigenschap 1.5.18 weten wij dat

$$(r_G|\chi) = \frac{1}{|G|} \sum_{g \in G} \overline{r_G(g)} \chi(g) = \frac{1}{|G|} |G| \chi(e_G) = n.$$

□

Merk op dat wij dus aangetoond hebben dat elke irreducibele representatie (op equivalentie na) voorkomt in de reguliere representatie. Bijgevolg bevat deze laatste alle informatie over de representaties van G.

Gevolg 1.5.20. *Voor een eindige groep G bestaan er slechts eindig veel irreducibele karakters.*

Gevolg 1.5.21. *Zij $\chi_1, \ldots, \chi_k$ de irreducibele complexe karakters van een eindige groep G, met respectievelijk graden $n_1, \ldots, n_k$. Dan:*

1. $\sum_{i=1}^{k} n_i^2 = |G|$,
2. *als $e_G \neq g \in G$ dan $\sum_{i=1}^{k} n_i \chi_i(g) = 0$.*

Bewijs. Wegens Eigenschap 1.5.19 weten wij dat, voor alle $g \in G$,

$$r_G(g) = \sum_{i=1}^{k} n_i \chi_i(g).$$

Wegens Eigenschap 1.5.18 verkrijgen wij dan dat

$$r_G(e_G) = \sum_{i=1}^{k} n_i n_i$$

en

$$0 = r_G(g) = \sum_{i=1}^{k} n_i \chi_i(g)$$

als $g \neq e_G$. □

Via Shur's Lemma

Gevolg 1.5.22. *Wij gebruiken de notatie en terminologie van Stelling 1.4.10. Veronderstel dat $0 \neq |G| \in K$. Zij*

$$\varphi : V_1 \to V_2$$

een lineaire transformatie en stel

$$\varphi^0 = \frac{1}{|G|} \sum_{g \in G} \rho^2_{g^{-1}} \varphi \rho^1_g.$$

Dan

1. *als ρ^1 en ρ^2 niet equivalent zijn dan $\varphi^0 = 0$.*
2. *als $K = \mathbb{C}$, $V_1 = V_2$ en $\rho^1 = \rho^2$ dan $\varphi^0 = (\frac{1}{n} \operatorname{Tr} \varphi) 1_{V_1}$, met $n = \dim_{\mathbb{C}}(V_1)$, de graad van ρ^1.*

Bewijs. Eerst merken we het volgende op, voor $h \in G$,

$$\begin{aligned}
\rho^2_h \varphi^0 \left(\rho^1_h\right)^{-1} &= \frac{1}{|G|} \sum_{g \in G} \rho^2_h \rho^2_{g^{-1}} \varphi \rho^1_g \rho^1_{h^{-1}} \\
&= \frac{1}{|G|} \sum_{g \in G} \rho^2_{hg^{-1}} \varphi \rho^1_{gh^{-1}} \\
&= \frac{1}{|G|} \sum_{x \in G} \rho^2_{x^{-1}} \varphi \rho^1_x \\
&= \varphi^0
\end{aligned}$$

Dus volgt uit Stelling 1.4.10 dat $\varphi^0 = 0$ als ρ^1 en ρ^2 niet equivalent zijn. In het geval dat $K = \mathbb{C}$, $V_1 = V_2$ en $\rho^1 = \rho^2$ volgt er dat $\varphi^0 = c1_{V_1}$ voor een $c \in \mathbb{C}$. Er volgt dan ook dat

$$\mathrm{Tr}(\varphi^0) = nc$$

en

$$\mathrm{Tr}(\varphi^0) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\left(\rho^1_{g^{-1}} \varphi \rho^1_g\right) = \mathrm{Tr}(\varphi)\,.$$

Dus $c = \frac{1}{n} \mathrm{Tr}(\varphi)$. □

Wij herschrijven nu Gevolg 1.5.22 in matrixnotatie. Stel dus, voor $g \in G$,

$$\rho^1_g = \left(r^1_{i,j}(g)\right) \text{ en } \rho^2_{g^{-1}} = \left(r^2_{i,j}(g^{-1})\right).$$

Stel dat φ bepaald is door de matrix $(c_{i,j})$ en φ^0 door een matrix $(c^0_{i,j})$. Dan

$$c^0_{i,l} = \frac{1}{|G|} \sum_{g \in G} \sum_{j,k} r^2_{i,j}(g^{-1}) c_{j,k} r^1_{k,l}(g).$$

Wegens Gevolg 1.5.22 is deze uitdrukking nul voor gelijk welke keuze van de elementen $c_{k,l} \in \mathbb{C}$ (d.w.z. voor alle lineaire transformaties φ), op voorwaarde dat ρ^1 en ρ^2 niet equivalent zijn. Dus volgt er

Gevolg 1.5.23. *Als ρ^1 en ρ^2 niet equivalent zijn dan*

$$\frac{1}{|G|} \sum_{g \in G} r^2_{i,j}(g^{-1})\, r^1_{k,l}(g) = 0$$

voor alle i, j, k, l.

Gevolg 1.5.24. *Als $K = \mathbb{C}$, $V_1 = V_2$ en $\rho^1 = \rho^2$ dan*

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G} r^2_{i,j}(g^{-1})\, r^1_{k,l}(g) &= \frac{1}{n}\delta_{i,l}\delta_{j,k} \\ &= \begin{cases} \frac{1}{n} & \text{als } l = i \text{ en } k = j \\ 0 & \text{anders} \end{cases}\end{aligned}$$

Bewijs. Wegens Gevolg 1.5.22 weten wij dat $\varphi^0 = c1_{V_1}$, d.w.z. $c^0_{i,l} = c\delta_{i,l}$ met $c = \frac{1}{n}\operatorname{Tr}(\varphi)$. Dus

$$c^0_{i,l} = \frac{1}{|G|}\sum_{g\in G}\sum_{j,k} r^2_{i,j}(g^{-1})c_{j,k}r^1_{k,l}(g) = c\delta_{i,l} = \frac{1}{n}\sum_{j,k}\delta_{j,k}c_{j,k}\delta_{i,l}\,.$$

De laatste gelijkheid volgt uit $\operatorname{Tr}(\varphi) = \sum_k c_{k,k} = \sum_{j,k}\delta_{j,k}c_{j,k}$. Het resultaat volgt nu onmiddellijk door de coëfficiënten van $c_{j,k}$ te vergelijken. □

Bewijs rij-orthogonaliteitsrelaties

In de rest van dit hoofdstuk werken wij met $K = \mathbb{C}$. Zoals eerder vermeld zijn matrices geassocieerd aan een representatie dan unitair. We zullen nu Gevolg 1.5.23 en Gevolg 1.5.24 herschrijven als orthogonaliteitsrelaties in een vectorruimte van functies over de complexe getallen.

Beschouw $\mathbb{C}^G$, de verzameling van alle functies van de groep G naar $\mathbb{C}$. Samen met de puntsgewijze optelling en scalaire vermenigvuldiging is dit een vectorruimte. We definiëren een afbeelding als volgt.

$$\langle\ ,\ \rangle : \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C} : \langle\phi,\psi\rangle = \frac{1}{|G|}\sum_{g\in G}\phi(g^{-1})\psi(g)$$

Deze afbeelding is symmetrisch omdat

$$\frac{1}{|G|}\sum_{g\in G}\phi(g^{-1})\psi(g) = \frac{1}{|G|}\sum_{g\in G}\phi(g)\psi(g^{-1})\,.$$

en bilineair.

Bovendien, als $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ een representatie is van een eindige groep G. Dan voldoet de bijhorende karakter χ_ρ aan $\overline{\chi(g)} = \chi(g^{-1})$ en dus volgt er dat $(\phi|\chi) = \langle\phi,\chi\rangle = \langle\chi,\phi\rangle$.

Het is nu bijzonder nuttig en interessant om op te merken dat een representatie ρ functies $r_{i,j} : G \to \mathbb{C}$ definieert zodat $(r_{i,j}(g))$ de matrixvoorstelling is van ρ_g. Gevolg 1.5.23 en Gevolg 1.5.24 kunnen nu als volgt geformuleerd worden.

Gevolg 1.5.25. *(i) Als ρ^1 en ρ^2 niet equivalent zijn dan geldt $\langle r^1_{i,j}, r^2_{k,l}\rangle = 0$ voor alle i, j, k, l.*

(ii) Voor elke representatie ρ geldt $\langle r_{i,j}, r_{k,l}\rangle = \frac{1}{n}\delta_{i,l}\delta_{j,k}$.

Hiermee kunnen we eindelijk het bewijs geven van de rij-orthogonaliteitsrelaties.

Stelling 1.5.26 (Rij-orthogonaliteitsrelaties)**.** *Als χ een irreducibel complex karakter van een eindige groep is dan*

$$(\chi|\chi) = 1.$$

Als χ en χ' irreducibele complexe karakters zijn van twee niet equivalente irreducibele complexe representaties van een eindige groep dan

$$(\chi|\chi') = 0.$$

Bewijs. Zij ρ een complexe irreducibele representatie van graad n met karakter χ, en zij $R_g = (r_{i,j}(g))$ haar matrixnotatie. De functie $\chi \in \mathbb{C}^G$ is de puntsgewijze som van de functies $r_{i,i}$, $\chi = \sum_i r_{i,i}$. Bijgevolg

$$(\chi|\chi) = \langle\chi, \chi\rangle = \langle\sum_i r_{i,i}, \sum_j r_{j,j}\rangle = \sum_{i,j}\langle r_{i,i}, r_{j,j}\rangle\,.$$

Wegens Gevolg 1.5.25 (ii) weten wij dat

$$\langle r_{i,i}, r_{j,j}\rangle = \frac{1}{n}\delta_{i,j}.$$

Dus

$$(\chi|\chi) = \frac{1}{n}\left(\sum_{1\le i,j\le n}\delta_{i,j}\right) = \frac{n}{n} = 1.$$

Zij χ' een karakter van complex irreducibele representatie van graad m en veronderstel dat χ en χ' niet equivalent zijn. Schrijf $R'_g = (r'_{i,j}(g))$. Dan

$$(\chi|\chi') = \langle\chi, \chi'\rangle = \sum_{i,j}\langle r_{i,i}, r'_{j,j}\rangle.$$

Wegens Gevolg 1.5.25 (i) weten wij dat

$$\langle r_{i,i}, r'_{j,j}\rangle = 0$$

en dus

$$(\chi|\chi') = 0.$$

□

1.5.6 Nog eens inductie

Zij G een eindige groep, H een deelgroep en $\psi : H \to \mathrm{GL}(V)$ een K-representatie van G met karakter χ_ψ. Dan hebben we gezien dat $\mathrm{Ind}_H^G(\psi)$ de inductie van ψ tot G een K-representatie is van G. We noteren de karakter van $\mathrm{Ind}_H^G(\psi)$ met $\chi_\psi \uparrow G$. We zullen nu het karakter berekenen van deze representatie in functie van het karakter χ_ψ van ψ. We voeren eerst een notatie in.

Indien χ een karakter is van H dan noteren we met $\dot{\chi}$ de volgende afbeelding

$$\dot{\chi}(g) = \begin{cases} \chi(g) & \text{als } g \in H \\ 0 & \text{als } g \notin H \end{cases}$$

Stelling 1.5.27. *Zij χ een karakter van H. Dan is $\chi \uparrow G$ gegeven door de volgende formule:*

$$(\chi \uparrow G)(g) = \frac{1}{|H|} \sum_{y \in G} \dot{\chi}(y^{-1}gy)$$

voor alle $g \in G$.

Bewijs. Zij $\psi : H \to \mathrm{GL}(V)$ een representatie van H met karakter χ. Stel dat $n = [G : H]$. Dan is

$$G = g_1 H \ \dot\cup \ g_1 H \ \dot\cup \ \ldots \ \dot\cup \ g_n H$$

de disjuncte unie van n linker nevenklassen met transversaal $\mathcal{T} = \{g_1, \ldots, g_n\}$. Verder zij $W := \bigoplus_{g_i \in \mathcal{T}} V^{(g_i)}$ met $V^{(g_i)} \cong V$ als vectorruimte. Dan is

$$\mathrm{Ind}_H^G(\psi) : G \to \mathrm{GL}(W) : g \mapsto \left(\mathrm{Ind}_H^G(\psi)(g) : W \to W : \sum_{i=1}^n v_i^{(g_i)} \mapsto \sum_{i=1}^n \psi_{h_i}(v_i)^{(g_j)} \right)$$

waar

$$g g_i = g_j h_i$$

voor een $g_j \in \mathcal{T}$ en $h_i \in H$.

Zij $\mathcal{B} = \{b_1, \ldots, b_{\dim V}\}$ een basis van V en neem in iedere isomorfe kopie $V^{(g_i)}$ dezelfde basis maar dat we dan noteren als $\mathcal{B}_{g_i} = \{b_1^{(g_i)}, \ldots, b_{\dim V}^{(g_i)}\}$ (om te herinneren in

welke kopie we aan het werken zijn). Tenslotte beschouw als basis $\mathcal{B}_W$ voor W de unie van alle $\mathcal{B}_{g_i}$. Zij A_ψ de matrix representatie van ψ ten opzichte van de basis $\mathcal{B}$ van V. Meer concreet, noteer $A_\psi(h) = (\alpha_{ij}(h))$ en dan is

$$hb_j = \sum_{j=1}^{\dim V} \alpha_{ij}(h) b_i.$$

Hieruit volgt dat

$$\mathrm{Ind}_H^G(\psi)(g)(b_s^{(g_i)}) = \sum_{t=1}^{\dim V} \alpha_{ts}(h_i) b_t^{(g_j)}$$

voor $1 \leq s \leq \dim . V$ en $1 \leq i \leq n$.

Om deze formules overzichtelijker te maken breiden we de $\{\alpha_{ij}\}$ uit tot afbeeldingen $\dot{\alpha_{ij}} : G \to K$:

$$\dot{\alpha_{ij}}(g) = \begin{cases} \alpha_{ij}(g) & \text{als } g \in H, \\ 0 & \text{als } g \notin H. \end{cases}$$

Hiermee kunnen we bovenstaande actie van g op de basis van W herschrijven:

$$\mathrm{Ind}_H^G(\psi)(g)(b_s^{(g_i)}) = \sum_{j=1}^{n} \sum_{t=1}^{\dim V} \dot{\alpha}_{ts}(g_j^{-1} g g_i) b_t^{(g_j)}$$

We breiden A_ψ eveens uit van H tot G door $\dot{A}_\psi(g) = (\dot{\alpha}_{ij}(g))$ te stellen voor $g \in G$. Ten opzichte van de basis van W vinden we dat de matrix representatie $A_\psi \uparrow G$ van $\mathrm{Ind}_H^G(\psi)$ gegeven wordt door:

$$g \mapsto (A_\psi \uparrow G)(g) = \begin{pmatrix} \dot{A}_\psi(g_1^{-1} g g_1) & \cdots & \dot{A}_\psi(g_1^{-1} g g_n) \\ \vdots & & \vdots \\ \dot{A}_\psi(g_n^{-1} g g_1) & \cdots & \dot{A}_\psi(g_n^{-1} g g_n) \end{pmatrix}$$

Hiermee vinden we een eerste uidrukking voor $\chi \uparrow G$:

$$(\chi \uparrow G)(g) = \sum_{i=1}^{n} \dot{\chi}(g_i^{-1} g g_i).$$

Bijgevolg vinden we duidelijk de gezochte formule:

$$(\chi \uparrow G)(g) = \frac{1}{|H|} \sum_{y \in G} \dot{\chi}(y^{-1} g y)$$

□

Als we in de formule van bovestande stelling $g = 1$ stellen, vinden we onmiddelijk volgend resultaat.

Gevolg 1.5.28. *deg($\chi \uparrow G$) = $|G : H|\chi(1)$.*

Voorbeeld 1.5.29. Zij

$$1_H : H \to GL_1(K) : h \mapsto 1$$

de triviale representatie van H en $\{g_1, \ldots, g_n\}$ een transversaal van H in G. Stel dat

$$gg_i = g_j h_i$$

voor een $g_j \in \mathcal{T}$ en $h_i \in H$. Dan zien we dat

$$\mathrm{Ind}_H^G(1_H)(g) : W \to W : v_i^{(g_i)} \mapsto v_i^{(g_j)}.$$

waar $W = \oplus_{i=1}^n K^{(g_i)}$.

Nu beschouw G/H als de verzameling $\{g_1H, \ldots, g_nH\}$ van linker nevenklassen van H in G. Dan voert G een linker actie ρ uit op G/H via linker vermenigvuldiging:

$$\rho : G \times G/H \to G/H : (g, g_iH) \mapsto (gg_i)H.$$

Aangezien $gg_i = g_j h_i$ zien we dat $\rho(g, g_iH) = gg_iH = g_jh_iH = g_jH$. Tenslotte beschouw de vrije K-vectorruimte $K(G/H)$ voortgebracht door de verzameling G/H. Dan is W isomorf, als vectorruimte, met $K(G/H)$ (oefening). Met al het bovenstaande ziet men dat $\mathrm{Ind}_H^G(1_H)$ equivalent is met de permutatierepresentatie geassocieerd met de actie ρ (oefening).

Dit voorbeeld toont aan dat geïnduceerde representaties dikwijls heel interessante representaties opleveren. Helaas, zoals in dit voorbeeld, indien ψ een irreduciebele representatie van H is dan is niet noodzakelijk $\mathrm{Ind}_H^G(\psi)$ weer irreduciebel.

Voorbeeld 1.5.30. Beschouw $D_8 = \langle a, b \mid a^4 = 1 = b^2, bab = a^{-1}\rangle$ de diheder groep van order 8. Dan hebben we gezien dat D_8 exact een 2-dimensionale irrediciebele representatie ρ heeft. Zij nu $T : \langle a\rangle \to \mathbb{C} : a \mapsto \sqrt{-1}$ een 1-dimensionale representatie van de deelgroep $H = \langle a\rangle$. Merk op dat $\langle a\rangle$ van index 2 is in D_8. Een direct berekening (oefening) toont aan dat

$$\rho \cong \mathrm{Ind}_{\langle a\rangle}^{D_8}(T).$$

1.6 Het tensor product $\otimes$

Gegeven twee K-vectorruimten V en W, kan men het direct product $V \times W$ bouwen[2], hetgeen aanleiding geeft tot een vectorruimte van dimensie $\dim_K V + \dim_K W$. Met

[2]Voor een eindig aantal vectorruimten $V_1, \ldots, V_l$ is het direct product $V_1 \times \cdots \times V_l$ isomorf met het direct som $V_1 \oplus \cdots \oplus V_l$ (dus we kunnen even goed $V \oplus W$ beschouwen). Echter voor oneindig veel vectorruimten zijn de twee constructies niet meer isomorf, zoals je later zal zien In de cursus categorie theorie.

behulp van dit hebben we de directe som van representaties gedefinieerd, hetgeen op zijn beurd aanleiding gaf tot de som van karakters. Nu wensen we aan te tonen dat ook het product $\chi_1.\chi_2$ van twee karakters χ_1, χ_2 ook een karakter is. Dus gegeven twee representaties $\rho_1 : G \to \mathrm{GL}(V)$ en $\rho_2 : G \to \mathrm{GL}(W)$ wensen we hieruit een nieuwe representatie $\rho : G \to \mathrm{GL}(Z)$ construeren zodat

$$\chi_\rho = \chi_{\rho_1}.\chi_{\rho_2}.$$

In het bijzonder moeten we een K-vectorruimte Z construeren zodat

$$\dim_K(Z) = \dim_K(V).\dim_K(W).$$

Het bovenstaande is de inhoud van de volgende secties.

1.6.1 $\otimes$ van vectorruimten

Zij V en W twee K-vectorruimten. Om te starten, beschouw de vrije K-vectorruimte

$$K(V \times W) = \{ \sum_{(v,w)\in V\times W}{}' k_{(v,w)} e_{(v,w)} \mid k_{(v,w)} \in K\}.$$

Merk op dat $K(V\times W)$ oneindigdimensionaal is met dimensie $|V|.|W|$, i.p.v. de gewenste $\dim(V).\dim(W)$. De reden hiervan is dat de constructie van de vrije vectorruimte de extra vectorruimte structuur van $V \times W$ 'vergeet'. I.h.b. indien $\mathcal{B}_V$ en $\mathcal{B}_W$ basissen zijn van V, resp. W, dan brengen de elementen $\{e_{(b_1,b_2)} \mid b_1 \in \mathcal{B}_V, b_2 \in \mathcal{B}_W\}$ de vrije vectorruimte $K(V \times W)$ **niet** voort.

Om het bovenstaande probleem op te lossen zullen we een quotiënt van $K(V \times W)$ beschouwen die de vectorruimte structuur van $V\times W$ wel detecteert. Concreet, definieer:

$$S_1 = \{(k_1 v + k_2 v', w) - k_1(v, w) - k_2(v', w) \,|v, v' \in V, w \in W, k_1, k_2 \in K\},$$

$$S_2 = \{(v, k_1 w + k_2 w') - k_1(v, w) - k_2(v, w') \,|v \in V, w, w' \in W, k_1, k_2 \in K\},$$

en zij

$$N := \mathrm{vect}_K\{S_1, S_2\}.$$

de deelruimte van F voortgebracht door $S_1 \cup S_2$.

Definitie 1.6.1. De quotiëntvectorruimte $K(V \times W)/N$ heet het *tensor product* van V en W en wordt genoteerd met $V \otimes W$.

Voor twee vectoren $v \in V$ en $w \in W$ noteren we

$$v \otimes w := e_{(v,w)} + N.$$

Vectoren uit $V \otimes W$ van de vorm $v \otimes w$, voor een $v \in V$ en $w \in W$ worden ook soms *pure tensoren* genoemd. Merk op dat niet alle vectoren van $V \otimes W$ pure tensoren zijn.

Lemma 1.6.2. *Het tensorproduct is bilineair, i.e.*

$$(k_1 v_1 + k_2 v_2) \otimes w = k_1(v_1 \otimes w) + k_2(v_2 \otimes w)$$

en

$$v \otimes (b_1 w_1 + b_2 w_2) = b_1(v \otimes w_1) + b_2(v \otimes w_2)$$

voor alle $v, v_1, v_2 \in V; w, w_1, w_2 \in W$ *en* $k_1, k_2, b_1, b_2 \in K$.

Bewijs. Bewijs dit als oefening. □

We kunnen nu aantonen dat het tensor product inderdaad de gewenste dimensie heeft.

Stelling 1.6.3. *Zij* $\mathcal{B}_V = \{e_i\}$ *en* $\mathcal{B}_W = \{f_j\}$ *bassisen van respectievelijk de* K*-vectorruimten* V *en* W*. Dan is*

$$\{e_i \otimes f_j \mid e_i \in \mathcal{B}_V, f_j \in \mathcal{B}_W\}$$

een basis voor $V \otimes W$*. In het bijzonder is*

$$\dim_K V \otimes W = \dim_K V . \dim_K W.$$

Bewijs. Zij $v \in V$ en schrijf $v = \sum_{i=1}^{\dim V} k_i e_i$ ten opzicht van de basis $\mathcal{B}_V$. Wegens Lemma 1.6.2 is dan $v \otimes w = \sum_{i=1}^{\dim V} k_i(e_i \otimes w)$. Als men nu hetzelfde doet met w en dan verkrijgen we dat $\{e_i \otimes f_j\}$ inderdaad een voortbrengende verzameling is.

We moeten nog enkel aantonen dat de verzameling vectoren $\{e_i \otimes f_j\}$ lineair onafhankelijk zijn. Veronderstel het tegendeel, dan bestaat er een lineaire combinatie met een eindig aantal termen

$$\sum_{i=1}^{\dim V} \sum_{j=1}^{\dim W} c_{i,j}(e_i \otimes f_j) = 0 \tag{1.3}$$

We zullen nu een bijzonder lineaire functie van $V \otimes W$ naar K definiëren. Zij $\varphi_{i,j} : V \times W \to K$ gedefinieerd via $\varphi_{i,j}(v, w) = 1$ indien $(v, w) = (e_i, f_j)$ en 0 elders. Deze

functie is bilineair (oefening). We kunnen $\varphi_{i,j}$ lineair uitbreiden tot een functie $\widehat{\varphi}_{i,j}$ op de vrije vectorruimte $K(V \times W)$:

$$\widehat{\varphi}_{i,j}\left(\sum_{(v,w)\in V\times W} a_{(v,w)}(v,w)\right) := \sum_{(v,w)\in V\times W} a_{(v,w)}\varphi((v,w))$$

waar $a_{(v,w)} \in K$. De functie $\widehat{\varphi}_{i,j}$ is, per constructie, lineair. Bijgevolg is de deelruimte $N = \text{vect}_K(S_1, S_2)$ vanuit de definitie van het tensor product in de kern van $\widehat{\varphi}_{i,j}$ (oefening). Dus is er een geïnduceerde lineaire functie $\psi_{i,j}(v \otimes w) := \widehat{\varphi}_{i,j}((v,w))$ van $V \otimes W$ naar K. Bovendien, per definitie van $\varphi_{i,j}$, is $\psi_{i,j}(e_k \otimes f_l) = \delta_{k,i}\delta_{l,j}$.

Neem nu het beeld onder $\psi_{i,j}$ van de vergelijking (1.3). Dan verkrijgen we dat $c_{i,j}e_i \otimes f_j = 0$ en dus $c_{i,j} = 0$. Aangezien (i,j) willekeurig gekozen was, toont dit het gewenste aan. □

In het bewijs voor de lineair onafhankelijkheid in bovenstaande stelling hebben we vanuit een concrete bilinaire functie $\varphi_{i,j} : V \times W \to W$ een lineaire functie $\psi_{i,j} : V \otimes W \to K$ geconstrueerd zodat $\psi_{i,j}(v \otimes w) = \varphi_{i,j}((v,w))$. Deze procedure maakt infeite niet gebruik van de concrete functievoorschrift van $\varphi_{i,j}$ en werkt ook voor willekeurige codomeinen. Meer precies, we verkrijgen de volgende eigenschap (het bewijs laten we als oefening).

Eigenschap 1.6.4 (Universele Eigenschap)**.** *Veronderstel dat $f : V \times W \to Y$ een bilineaire functie is naar de K-vectorruimte Y. Dan bestaat er een unieke lineaire afbeelding $\tilde{f} : V \otimes W \to Y$ zodanig dat*

$$\tilde{f}(v \otimes w) = f(v,w)$$

voor alle $v \in V$ en $w \in W$.

Opmerking. Dikwijls wordt het tensor product $V \otimes W$ gedefinieerd als een vectorruimte Z zodat iedere bilineaire functie $f : V \times W \to Y$ uitgebreid kan worden tot een lineaire functie $\tilde{f} : Z \to Y$ zoals in de Universele Eigenschap hierboven. Vervolgens wordt dan aangetoond dat, op isomorfisme na, er een unieke vectorruimte Z is dat aan de universele eigenschap voldoet. In deze (klassieke) aanpak wordt het tensor product slechts in een tweede fase concreet geconstrueerd. Deze uniciteit om aan de Universele Eigenschap te voldoen zullen we niet gebruiken, vandaar onze aanpak tot het onderwerp. In latere cursussen zal je echter het grote nut van de Universele Eigenschap zien.

1.6.2 $\otimes$ van representaties

Met behulp van het tensor product van vectorruimten, kan men ook het tensor product van representaties definiëren die op hun beurt aanleiding zullen geven tot het product van karakters.

Zij $\rho^1 : G \to \mathrm{GL}(V_1)$ en $\rho^2 : G \to \mathrm{GL}(V_2)$ twee representaties van een eindige groep G. Voor een gegeven $g \in G$ beschouw de functie

$$\rho_g^1 \times \rho_g^2 : V_1 \times V_2 \to V_1 \otimes V_2 : (v, w) \mapsto \rho_g^1(v) \otimes \rho_g^2(w).$$

Doordat ρ_g^1 en ρ_g^2 lineair zijn is $\rho_g^1 \times \rho_g^2$ bilineair. Bijgevolg wegens Eigenschap 1.6.4 kan $\rho_g^1 \times \rho_g^2$ uitgebreid worden tot een lineaire afbeelding van $V_1 \otimes V_2$ naar zichzelf die we noteren met $\rho^1 \otimes \rho^2$. Deze functie heeft bovendien de eigenschap dat

$$(\rho_g^1 \otimes \rho_g^2)(v_1 \otimes v_2) = \rho_g^1(v_1) \otimes \rho_g^2(v_2),$$

voor $v_1 \in V_1$ en $v_2 \in V_2$. We laten als oefening dat $\rho_g^1 \otimes \rho_g^2 \in \mathrm{GL}(V_1 \otimes V_2)$.

Definitie 1.6.5. Veronderstel dat $\rho^1 : G \to \mathrm{GL}(V_1)$ en $\rho^2 : G \to \mathrm{GL}(V_2)$ twee representaties van een eindige groep G zijn. De afbeelding

$$\rho^1 \otimes \rho^2 : G \to \mathrm{GL}(V_1 \otimes V_2) : g \mapsto \rho_g^1 \otimes \rho_g^2.$$

heet het tensorproduct van ρ^1 en ρ^2.

Lemma 1.6.6. *Het tensorproduct van twee representaties is een representatie.*

Bewijs. Bewijs dit als oefening. □

Wij geven nu deze representatie in matrixnotatie en dit in functie van de matrixrepresentaties A_{ρ^1} en A_{ρ^2} van ρ^1 en ρ^2 respectievelijk. Zij $\{e_i \mid 1 \leq i \leq n_1\}$ een basis voor V_1, dus $\dim_K(V_1) = n_1$ en zij $\{f_k \mid 1 \leq k \leq n_2\}$ een basis voor V_2, dus $\dim_K(V_2) = n_2$. Zij $A_{\rho^1}(g) = (r_{i,j}^1(g))_{1 \leq i,j \leq n_1}$ en $A_{\rho^2}(g) = (r_{k,l}^2(g))_{1 \leq k,l \leq n_2}$. Dus

$$\begin{aligned} \rho_g^1(e_j) &= \sum_{i=1}^{n_1} r_{i,j}^1(g) e_i \,, \\ \rho_g^2(f_l) &= \sum_{k=1}^{n_2} r_{k,l}^2(g) f_k \,. \end{aligned}$$

Dan

$$(\rho^1 \otimes \rho^2)_g(e_j \otimes f_l) = \rho^1_g(e_j) \otimes \rho^2_g(f_l) = \sum_{i=1}^{n_1} \sum_{k=1}^{n_2} r^1_{i,j}(g)\, r^2_{k,l}(g)\, (e_i \otimes f_k).$$

Dus de matrixnotatie voor $(\rho^1 \otimes \rho^2)_g$ is

$$\left(r^1_{i,j}(g)\, r^2_{k,l}(g)\right)$$

of nog anders gevisualiseerd

$$\begin{pmatrix} r^1_{1,1}(g)A_{\rho^2}(g) & \dots & r^1_{1,n_1}(g)A_{\rho^2}(g) \\ \vdots & \ddots & \vdots \\ r^1_{n_1,1}(g)A_{\rho^2}(g) & \dots & r^1_{n_1,n_1}(g)A_{\rho^2}(g) \end{pmatrix}.$$

De matrix representatie van $(\rho^1 \otimes \rho^2)_g$ is dus de zogenaamde *Kroneckerproduct* van de matrices $A_{\rho^1}(g)$ en $A_{\rho^2}(g)$, die we noteren met $A_{\rho^1}(g) \otimes A_{\rho^2}(g)$.

Eigenschap 1.6.7. *Zij $\rho^1 : G \to \mathrm{GL}(V_1)$ en $\rho^2 : G \to \mathrm{GL}(V_2)$ twee representaties van een groep G en zij χ^1 en χ^2 hun karakters. Dan is*

$$\chi_{\rho^1 \otimes \rho^2} = \chi^1 \cdot \chi^2.$$

Bewijs. Zij A_{ρ^1} en A_{ρ^2} de matrix vorm van ρ^1 en ρ^2. Meer precies stel,

$$A_{\rho^1}(g) = (r^1_{i,j}(g)), \;\; A_{\rho^2}(g) = (r^2_{k,l}(g)).$$

Wij verkrijgen dan

$$\chi^1(g) = \sum_i r^1_{i,i}(g), \;\; \chi^2(g) = \sum_k r^2_{k,k}(g),$$

$$\psi(g) = \sum_{i,k} r^1_{i,i}(g)\, r^2_{k,k}(g) = \chi^1(g)\, \chi^2(g).$$

□

Samengevat, gegeven een eindige groep G, verkrijgen we dat de verzameling $\mathrm{Ch}_K(G)$ van alle karakters over K van G een rijke structuur heeft.

Eigenschap 1.6.8. *Zij G een eindige groep. Dan is de verzameling $Ch(G)$ met de puntsgewijze optelling, vermenigvuldiging en scalaire vermenigvuldiging een K-algebra.*

In de master cursus 'knopen theorie' zal je zien dat de verzameling $\mathrm{Rep}_K(G)$ van alle K-representaties van G met de puntsgewijze scalaire vermenigvuldiging en optelling en het tensor product een zogenaamde 'symmetric monoidal category' is.

Zij $G = G_1 \times G_2$ het direct product van twee deelgroepen G_1 en G_2. Met behulp van het tensor product kunnen we de irreduciebele karakters van G bepalen in functie van de irreduciebele karakters van G_1 en G_2.

Stelling 1.6.9. *Zij $G = G_1 \times G_2$ een eindige groep en ρ een representatie van G. Dan bestaan er representaties ρ_i van G_i zodat*

$$\chi_\rho = \chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} . \chi_{\rho_2}.$$

Bovendien is χ_ρ irreduciebel als en slechts als χ_{ρ_1} en χ_{ρ_2} irreduciebel zijn.

De bovenstaande resultaat zegt dus dat om de irreduciebele karakters van $G = G_1 \times G_2$ op te stellen we de producten moeten nemen van de irreduciebele karakters van G_1 en van G_2.

1.6.3 Symmetrisch en anti-symmetrisch deel

De representaties

Voor een gegeven representatie $\rho : G \to GL(V)$ kunnen we dus ook $\rho \otimes \rho$ beschouwen. Hiervoor onderzoeken we nu twee speciale invariante deelruimten van het tensorproduct $V \otimes V$. Zij $\{e_i \mid 1 \leq i \leq n\}$ een K-basis van V en zij

$$t : V \otimes V \to V \otimes V$$

het automorfisme gedefinieerd door

$$t(e_i \otimes e_j) = e_j \otimes e_i,$$

voor $1 \leq i, j \leq n$. Er ook volgt dat

$$t(v_1 \otimes v_2) = v_2 \otimes v_1$$

voor alle $v_1, v_2 \in V$. Verder

$$t^2 = 1_{V \otimes V}.$$

Definieer

$$\mathrm{Sym}^2(V) = \{w \in V \otimes V \mid t(w) = w\}$$

en

$$\mathrm{Alt}^2(V) = \{w \in V \otimes V \mid t(w) = -w\}.$$

Een basis voor de deelruimte $\mathrm{Sym}^2(V)$ is de verzameling

$$\{e_i \otimes e_j + e_j \otimes e_i \mid 1 \leq i \leq j \leq n\}.$$

Stel immers dat $w \in \mathrm{Sym}^2(V)$, en $w = \sum_{i,j} \lambda_{i,j} e_i \otimes e_j$. Omdat $t(w) = w$ geldt dus $t(w) = \sum_{i,j} \lambda_{i,j} e_j \otimes e_i = \sum_{i,j} \lambda_{i,j} e_i \otimes e_j = w$, dus $\lambda_{i,j} = \lambda_{j,i}$. De verzameling brengt dus $\mathrm{Sym}^2(V)$ voort. Stel dat $\sum_{i,j} \lambda_{i,j}(e_i \otimes e_j + e_j \otimes e_i) = 0$, dan volgt onmiddellijk dat $\lambda_{i,j} = 0$ omdat de $e_i \otimes e_j$ lineair onafhankelijk zijn in $V \otimes V$. Volkomen analoog toont men aan dat de verzameling

$$\{e_i \otimes e_j - e_j \otimes e_i \mid 1 \leq i < j \leq n\}.$$

een basis is voor $\mathrm{Alt}^2(V)$.

Als nu $w \in V \otimes V$ en $0 \neq 1 + 1 \in K$ dan

$$w = \frac{1}{2}(w + t(w)) + \frac{1}{2}(w - t(w)).$$

Zij $w_1 = \frac{1}{2}(w + t(w))$ en $w_2 = \frac{1}{2}(w - t(w)$. Dan $t(w_1) = w_1$ en $t(w_2) = -w_2$. Dus

$$V \otimes V = \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V),$$

De deelruimten $\mathrm{Sym}^2(V)$ en $\mathrm{Alt}^2(V)$ zijn invariant onder de actie van G. Dus definiëren zij representaties. Men noemt deze het *symmetrisch kwadraat,* respectievelijk het *alternerend kwadraat* van de gegeven representatie.

Hun bijhorende karakters

Eigenschap 1.6.10. *Zij $K = \mathbb{C}$ en V een $\mathbb{C}$-vectorruimte. Zij $\rho : G \to \mathrm{GL}(V)$ een representatie van graad n van de groep G en zij χ haar karakter. Zij χ_s^2 het karakter van het symmetrisch kwadraat $\mathrm{Sym}^2(V)$ en zij χ_a^2 het karakter van het alternerend kwadraat $\mathrm{Alt}^2(V)$. Dan gelden de volgende eigenschappen voor $g \in G$:*

1. $\chi_s^2(g) = \frac{1}{2}\left(\chi(g)^2 + \chi(g^2)\right)$,
2. $\chi_a^2(g) = \frac{1}{2}\left(\chi(g)^2 - \chi(g^2)\right)$.

Bovendien

$$\chi^2 = \chi_s^2 + \chi_a^2.$$

Bewijs. Zij $g \in G$. Wij weten dat $R(g) \in \mathrm{GL}_n(\mathbb{C})$ een basis van eigenvectoren heeft, zeg $\{e_1, \ldots, e_n\}$. Bijgevolg bestaan $c_1, \ldots, c_n \in \mathbb{C}$ zodat

$$\rho_g(e_i) = c_i e_i$$

en dus

$$\chi(g) = \sum_{i=1}^{n} c_i, \quad \chi(g^2) = \sum_{i=1}^{n} c_i^2.$$

Ook

$$(\rho_g \otimes \rho_g)(e_i \otimes e_j + e_j \otimes e_i) = c_i c_j (e_i \otimes e_j + e_j \otimes e_i)$$

en

$$(\rho_g \otimes \rho_g)(e_i \otimes e_j - e_j \otimes e_i) = c_i c_j (e_i \otimes e_j - e_j \otimes e_i).$$

Dus

$$\chi_s^2(g) = \sum_{1 \le i \le j \le n} c_i c_j = \sum_{i=1}^{n} c_i^2 + \sum_{1 \le i < j \le n} c_i c_j = \frac{1}{2}\left(\sum_{i=1}^{n} c_i\right)^2 + \frac{1}{2}\sum_{i=1}^{n} c_i^2$$

en

$$\chi_a^2(g) = \sum_{1 \le i < j \le n} c_i c_j = \frac{1}{2}\left(\sum_{i=1}^{n} c_i\right)^2 - \frac{1}{2}\left(\sum_{i=1}^{n} c_i^2\right).$$

Duidelijk volgt dat $\chi^2 = \chi_s^2 + \chi_a^2$. Dit volgt ook uit het feit dat $V \otimes V = \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$, een directe som van G-invariante deelruimten. □

1.7 Samenvatting en allesomvattende voorbeelden

1.7.1 Samenvatting stellingen Karaktertheorie

We geven nu een stappenplan en een beknopte samenvatting van alle de resultaten dat kunnen helpen om een karaktertabel van een groep G op te stellen.

Voor het opstellen van een karakter tabel kan men in de volgende volgorde nadenken:

(i) De conjugatieklassen en de ordes van de centralisatoren, via Orbiet-Stablilizator, bepalen. Hiermee weten we ook de grootte van de karaktertabel.

(ii) De commutator deelgroep G' berekenen (bv. met behulp van Eigenschap 1.3.10).

(iii) Het quotiënt G/G' beschrijven.

(iv) Bepaal al de irreduciebele representaties van de abelse groep G/G'. Indien G/G' cyclisch is, zijn deze beschreven in Sectie 1.3.3. Anders, wegens de fundamentele stelling van eindige abelse groepen, is G/G' een direct product van cyclische groepen en dus de representaties verkregen via producten van karakters (Stelling 1.6.9).

(v) Met behulp van lift, zie Stelling 1.3.13, schrijf alle 1-dimensionale representaties van G op.

(vi) Vind op 1 of ander manier een karakter χ van graad minstens 2. Hierbij houd in achterhoofd dat de graad een deler van $|G|$ moet zijn. Natuurlijke aanpakken hiervoor zijn: (i) de groep later ageren op een verzameling en de geassocieerde permutatierepresentatie opstellen (zie sectie 1.3.2) ; (ii) m.b.v Stelling 1.5.27 bereken het karakter van $\mathrm{Ind}_H^G(\psi)$ voor een strikte deelgroep H (bijvoorbeeld cyclisch) en ψ een 1-dimensionale representatie van H ; (iii) De lift van een irreduciebel karakter, van graad minstens 2, van een quotiënt G/N (cf. Stelling 1.3.15)

(vii) Ga na dat χ irreduciebel is door na te gaan dat $(\chi \mid \chi) = 1$.

(viii) Eenmaal je een irreduciebele karakter van hogere graad hebt, kan je onmiddelijk er nieuwe maken. Bijvoorbeeld via: (i) product met een 1-dimensionele karakter; (ii) complex geconjugeerde; (iii) alternerend en symmetrisch deel (niet noodzakelijk irreduciebel).

(ix) De vorige stappen herhalen totdat je genoeg getallen in het karaktertabel kan opvullen. De overblijvende gaten kan je nu proberen te vinden via de rij en kolom-orthogonaliteitsrelaties.

Laten we nu gewoon een samenvattend lijst aan eigenschappen en stellingen over karakters samenbundelen:

1. G heeft steeds een triviaal karakter χ dat gedefinieerd is als volgt

$$\chi(g) = 1, \text{ voor alle g} \in \text{G}$$

2. Stelling 1.3.13 en 1.5.16: Iedere groep G heeft $|G/G'|$ karakters van graad 1. Deze karakters χ zijn allen van de vorm

$$\chi_\psi(g) := \psi(g[G, G])$$

met ψ een irreduciebele representatie (noodzakelijk van dimensie 1) van G/G' is.

3. Indien $N \triangleleft G$ en ψ een irreduciebel karakter van G/N. Dan bekomen we een irreduciebel karakter $\widehat{\psi}$ van G als volgt

$$\widehat{\psi}(g) = \psi(gN)$$

(we zeggen dat $\widehat{\psi}$ de lift is van ψ). Hiermee bekomen we alle irreduciebel karakters van G die in hun kern N omvatten.

4. Stelling 1.6.9: Zij $G = G_1 \times G_2$ en χ_i een irreduciebele karakter van G_i. Dan is de karakter χ gedefinieerd als

$$\chi(g_1, g_2) = \psi_1(g_1)\psi_2(g_2),\ g_1 \in G_1, g_2 \in G_2$$

een irreduciebele karakter van G. Bovendieen is iedere irreduciebele karakter van G van deze vorm.

5. Eigenschap 1.5.3 Zij $g \in G$ van orde n en χ een karakter van G. Dan is $\chi(g)$ een som van n-de eenheidswortels. Bovendien is $|\chi(g)| \leq \chi(1)$.

6. Eigenschap 1.5.21: De waarden $\chi_i(1),\ 1 \leq i \leq k$ (dit zijn de waarden van de eerste kolom van de karakertabel) voldoen aan

$$\sum_{i=1}^{k} \chi_i(1)^2 = |G|.$$

7. Rij orthogonaliteit-relaties (i.e. Stelling 1.5.7): voor alle i, j is $\langle \chi_i, \chi_j \rangle = \delta_{ij}$.

8. Kolom orthogonaliteit-relaties (i.e. Stelling 1.5.15): voor iedere $g, h \in G$ geldt er dat

$$\sum_{i=1}^{k} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |C_g(g)|\ , & \text{indien } g \text{ en } h \text{ geconjugeerd zijn,} \\ 0, & \text{anders.} \end{cases}$$

9. Eigenschap 1.5.3: Zij $g \in G$ en χ een karakter van G. Dan geldt dat

$$\chi(g^{-1}) = \overline{\chi(g)},\ g \in G.$$

In het bijzonder als g geconjugeerd is met g^{-1}, dan is $\chi(g)$ een reëel getal voor ieder karakter χ van G.

10. Voor een karakter χ van G definiëren we $\overline{\chi}$ als volgt:

$$\overline{\chi}(g) = \overline{\chi(g)},\ g \in G.$$

Indien χ irreduciebel is, dan is $\overline{\chi}$ eveneens een irreduciebel karakter.

11. Eigenschap 1.6.7: Indien χ en ψ twee karakters zijn van G, dan is het product

$$(\chi\psi)(g) = \chi(g)\psi(g),\ g \in G$$

weer een karakter van G.

12. Zij χ een irreduciebele karakter van G en λ een karakter van G van graad 1. Dan is $\chi.\lambda$ weer een irreduciebele karakter van G.

13. Eigenschap 1.6.10: Zij χ een karakter van G, dan zijn χ_S en χ_A het ook. Waar

$$\begin{aligned} \chi_S(g) &= \tfrac{1}{2}(\chi^2(g) + \chi(g^2)), \\ \chi_A(g) &= \tfrac{1}{2}(\chi^2(g) - \chi(g^2)). \end{aligned}$$

14. Neem een deelgroep H van G en een karakter ψ van H. Dan is $\psi \uparrow G$ weer een karakter van G. En we kunnen het eveneens uitrekenen met behulp van Stelling 1.5.27.

15. Stelling 1.5.5: Indien $N \triangleleft G$ dan bestaan er irreduciebele karakters $\chi_1, \ldots, \chi_s$ van G zodat

$$N = \bigcap_{i=1}^{s} Ker\chi_i.$$

16. De groep G is niet simpel als en slechts als

$$\chi(g) = \chi(1)$$

voor een niet-triviale irreduciebel karakter χ van G en voor een $g \in G$ verschillend van het neutraal element.

17. Isomorfe groepen hebben gelijke karaktertabellen. Het omgekeerde is niet geldig. Kijk hiervoor naar D_8 en Q_8.

18. Ito's stelling : als χ een irreduciebel karakter van G dan is $\chi(1)$ een deler van $\frac{|G|}{|Z(G)|}$.

1.7.2 Karaktertabel van S_5

We gaan nu de karaktertabel van S_5 berekenen uitsluitend met behulp van alle theorie samengevat hierboven en hierbij houden we de stappenplan in de achterhoofd.

de conjugatieklassen: Zij $\sigma \in S_n$. Herinner dat

$$\mathcal{C}_{S_n}(\sigma) = \{\tau \in S_n \mid \ \sigma \text{ en } \tau \text{ hebben zelfde cyclus-structuur}\}.$$

Bijgevolg, in het geval van S_5 zijn er 7 conjugatieklassen. Representanten hiervoor zijn

$$1, (12), (123), (12)(34), (1234), (123)(45) \text{ en } (12345).$$

Het aantal elementen per conjugatieklassen kunnen we via combinatoriek berekenen. Bijvoorbeeld het aantal 2-cycli is gelijk aan het aantal keuzes om twee getallen te kiezen uit 5 (dus er zijn er $\binom{5}{2} = 10$). Het aantal 3-cycli is $\frac{5.4}{2}.2$ (want op $\frac{5.4}{2}$ manieren kan je twee getallen kiezen en de .2 omdat voor ieder paar gekozen getallen er twee mogelijke 3-cycli zijn). De aantal permutaties met structuur $(3, 2)$ is 20 wegens helemaal dezelfde reden als bij de 3-cycli. Het aantal met structuur $(2, 2)$ is $5.\frac{\binom{4}{2}}{2} = 15$ want als je een getal vast kiest en er nog twee andere kiest dan zijn de twee overblijvende vast (het delen door twee is wegens het commuteren van disjuncte cyclci zoals (12)(34) en (34)(12)). Analoog is het aantal $(2, 3)$-cycli 30 en de 5-cycli is de rest.

Het aantal elementen in de centralisatoren van de representanten kan nu eenvoudig worden berekend met behulp van

$$|\mathcal{C}_G(x)| = |G : \mathrm{Cen}_G(x)| = \frac{|G|}{|\mathrm{Cen}_G(x)|}.$$

Samengevat hebben we volgende tabel:

g_i	1	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
$\lvert\mathcal{C}_G(g_i)\rvert$	1	10	20	15	30	20	24
$\lvert\mathrm{Cen}_G(g_i)\rvert$	120	12	6	8	4	6	5

Bijgevolg heeft S_5 juist 7 irreduciebele karakters.

1-dimensionale karakters: De enige normale deelgroepen van S_5 zijn $\{1\}, S_5$ en A_5. We weten ook dat $S_5/A_5 \cong C_2$ en dat S_5 niet abels is. Bijgevolg is $S_5' = A_5$. Dus heef S_5 twee lineaire karakters χ_1 en χ_2. Deze bekomen we door de irreduciebele karakters van C_2 te liften. Deze zijn gegeven door:

$$\chi_1 = 1_G, \text{ en}$$

$$\chi_2(g) = \begin{cases} 1 & \text{als } g \text{ een even permutatie is,} \\ -1 & \text{als } g \text{ een oneven permutatie is.} \end{cases}$$

Permutatie karakter: We gaan nu een hoger dimensionale representatie maken met behulp van acties. Een natuurlijk keuze is de permutatie actie:

$$\varphi : S_5 \times \{1,2,3,4,5\} \to \{1,2,3,4,5\} : (\sigma, i) \mapsto \sigma(i).$$

De karakter van de geassocieerde permutatierepresentatie ziet er als volgt uit (oefening):

$$\chi(g) = |fix(g)| - 1,\ g \in G.$$

waar $fix(g)$ de getallen zijn die vast blijven onder g (bv. voor $g = (123)(4)(5)$ is $fix(g) = \{4,5\}$). We gaan na als deze irreduciebel is:

$$\langle \chi, \chi \rangle = \frac{4^2}{120} + \frac{2^2}{12} + \frac{1^2}{6} + \frac{(-1)^2}{6} + \frac{(-1)^2}{5} = 1.$$

Bijgevolg is de gemaakte karakter χ irreduciebel en we noteren deze met χ_3.

Nu dat we een eerste karkater van hogere graad geconstrueerd hebben, kunnen we onmiddelijk een twee maken doormiddel van product met 1-dimensionale:

$$\chi_4 := \chi_3 \chi_2$$

is weer een irreduciebele karakter van S_5

Momenteel hebben we dus het volgende deel van de karaktertabel van S_5.

g_i	1	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
$\lvert \mathrm{Cen}_G(g_i) \rvert$	120	12	6	8	4	6	5
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1

Via alternerend en symmetrisch deel er nog meer karakters: Aangezien we 7 conjugatieklassen hebben, weten we dat we nog 3 irreduciebele karakters missen. We missen dus nog te veel data om de tabel verder op te vullen met behulp van de rij en kolom orthogonaliteitsrelaties. Bijgevolg moeten we weer lukken een karakter van hogere graad te maken. In dit voorbeeld zullen we er construeren met behulp van het alternerend en symmetrisch deel (in de volgende voorbeelden zullen we via inductie werken).

Noteer even weer $\chi = \chi_3$. We berekenen nu χ_A en χ_S en bekomen de volgende waarden:

g_i	1	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
$\lvert\mathrm{Cen}_G(g_i)\rvert$	120	12	6	8	4	6	5
χ_S	10	4	1	2	0	1	0
χ_A	6	0	0	-2	0	0	1

Laten we de irreducibiliteit nagaan:

$$\langle \chi_A, \chi_A \rangle = \frac{36}{120} + \frac{4}{8} + \frac{1}{5} = 1$$

Dus χ_A is een nieuw irreduciebel karakter van S_5 die we noteren met χ_5. Merk op dat $\chi_5 \cdot \chi_2 = \chi_5$ en dus niet een nieuw karakter oplevert.

Berekenen van de andere inproducten geeft ons dat:

$$\begin{aligned} \langle \chi_S, \chi_1 \rangle &= \tfrac{10}{120} + \tfrac{4}{12} + \tfrac{1}{6} + \tfrac{2}{8} + \tfrac{1}{6} = 1, \\ \langle \chi_S, \chi_3 \rangle &= \tfrac{40}{120} + \tfrac{8}{12} + \tfrac{1}{6} - \tfrac{1}{6} = 1, \\ \langle \chi_S, \chi_S \rangle &= \tfrac{100}{120} + \tfrac{16}{12} + \tfrac{1}{6} + \tfrac{4}{8} + \tfrac{1}{6} = 3. \end{aligned}$$

Dus we zien dat

$$\chi_S = \chi_1 + \chi_3 + \psi$$

voor een irreduciebel karakter ψ van graad 5. In andere woorden $\psi = \chi_S - \chi_1 - \chi_3$ en we noteren deze irreduciebel karakter met χ_6. Ditmaal geeft $\chi_7 = \chi_6 \chi_2$ ons wel een nieuw irreduciebele karakter van S_5. Hiermee hebben we de laatste irreduciebele karakter van S_5 gevonden. Samengevat:

g_i	1	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
$\lvert\mathrm{Cen}_G(g_i)\rvert$	120	12	6	8	4	6	5
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1
χ_5	6	0	0	-2	0	0	1
χ_6	5	1	-1	1	-1	1	0
χ_7	5	-1	-1	1	1	-1	0

Eenmaal we χ_5 gevonden hadden, zou het wel gelukt zijn om via de Rij- en Kolomorthogonaliteitsrelaties de laatste twee rijen te reconstrueren.

1.7.3 Karaktertabel van $PSL(2,7)$

Ditmaal gaan we de karaktertabel van $PSL(2,7)$ uitwerken.

Conjugatie klassen en centralisatoren:

De conjugatieklassen en ordes van de centralisatoren van $PSL(2,7)$ bepalen is een goede oefening in lineaire algebra. Dit is nu echter niet de focus en bijgevolg zullen we even de conjugatie klassen aannemen en simpelweg oplijsten:

	$o(g_i)$	$\lvert\mathrm{Cen}_G(g_i)\rvert$	$\lvert\mathcal{C}_G(g_i)\rvert$
$g_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} Z$	1	168	1
$g_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} Z$	2	8	21
$g_3 = \begin{pmatrix} 2 & -2 \\ 2 & 2 \end{pmatrix} Z$	4	4	42
$g_4 = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} Z$	3	3	56
$g_5 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} Z$	7	7	24
$g_6 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} Z$	7	7	24

1-dimensionale representaties: De groep $PSL(2,7)$ is een simpele groep. We zullen deze feit nu aannemen. In het bijzonder zijn de enige normale deelgroepen 1 of $PSL(2,7)$ zelf. Aangezien $PSL(2,7)$ niet abels is, moet $PSL(2,7)' = PSL(2,7)$. In het bijzonder heeft $PSL(2,7)$ slechts 1 karakter van graad 1, namelijk de triviale representatie.

Hoger dimensionale karakters via inductie

Begin eerst met een deelgroep T van $PSL(2,7)$ te definiëren:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} Z \ : \ a \in \mathbb{Z}_7^*, b \in \mathbb{Z}_7 \right\}$$

Waar $Z = \{\pm I\}$. Men kan eenvoudig nagaan dat $|T| = 21$. We zullen vanuit representaties van T, met behulp van inductie, representaties van $PSL(2,7)$ construeren.

stap 1, inductie uit karakters van graad 1 van T

In deze stap berekenen we de waarden van de karakter $(1_T) \uparrow PSL(2,7)$ van de geïnduceerde representatie $\mathrm{Ind}_T^{PSL(2,7)}(1_T)$. Meer concreet zullen we de volgende resultaat bewijzen.

Eigenschap 1.7.1. *Zij λ een niet-triviaal karakter van graad 1 van T en 1_T de triviale karakter. Dan geldt het volgende:*

- $(1_T) \uparrow PSL(2,7) = 1_G + \chi$ *voor een irreduciebele karakter χ van $PSL(2,7)$,*
- $\lambda \uparrow PSL(2,7)$ *is irreduciebel.*

T als deelgroep van S_7: Om dit aan te tonen beginnen we met een deelgroep van S_7 te construeren die isomorf is met T. Beschouw volgende permutaties:

$$a = (1234567), b = (235)(476).$$

Neem als deelgroep $H = \langle a, b \rangle$. Dat $o(a) = 7$ en $o(b) = 3$ is welbekend. Met behulp van $b^{-1}ab = (b(1)b(2)b(3)b(4)b(5)b(6)b(7))$ levert simpel rekenwerk dat $b^{-1}ab = a^{-1}$. Waarmee we reeds eenvoudig zien dat $|H| = 21$ (duidelijk is $|H| \leq 21$, maar door de stelling van Lagrange moet 3 en 7 delers zijn van $|H|$ en dus is het zelfs een gelijkheid).

Als we $\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} Z$ op b sturen en $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} Z$ op a sturen dan bekomen we dat T en H isomorf zijn.

Karaktertabel van T: De conjugatieklassen en karaktertabel van H berekenen is ook een goede oefening (die analoog gevonden kan worden aan het karaktertabel van S_5). Maar omdat de focus van dit voorbeeld is op $PSL(2,7)$ zullen we deze gegevens even aannemen en oplijsten. De conjugatieklassen van H zijn gegeven door:

$$\{1\}, \{a, a^2, a^4\}, \{a^3, a^5, a^6\}, \{a^i b : 0 \leq i \leq 6\}, \{a^i b^2 : 0 \leq i \leq 6\}.$$

We nemen als representanten $1, a, a^3, b$ en b^2. De karaktertabel is gegeven door:

g_i	1	a	a^3	b	b^2
$\lvert\mathrm{Cen}_G(g_i)\rvert$	21	7	7	3	3
χ_1	1	1	1	1	1
χ_2	1	1	1	ω	ω^2
χ_3	1	1	1	ω^2	ω
χ_4	3	$\eta + \eta^2 + \eta^4$	$\eta^3 + \eta^5 + \eta^6$	0	0
χ_5	3	$\eta^3 + \eta^5 + \eta^6$	$\eta + \eta^2 + \eta^4$	0	0

waar $\eta = e^{(2\pi i)/7}$ en $\omega = e^{(2\pi i)/3}$.

Laten we nu alles vertalen naar T. We bekomen volgende representanten:

$$h_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} Z,\ h_2 = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} Z,\ h_3 = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix} Z,$$

$$h_4 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} Z,\ h_5 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} Z$$

En de karakters van graad 1 van T zijn:

h_i	h_1	h_2	h_3	h_4	h_5
$\lvert\mathrm{Cen}_G(h_i)\rvert$	21	3	3	7	7
1_T	1	1	1	1	1
λ_1	1	ω	ω^2	1	1
λ_2	1	ω^2	ω	1	1

De inducties:
Met behulp van Stelling 1.5.27 kan men nu eenvoudig $1_T \uparrow PSL(2,7)$ en $\lambda_i \uparrow PSL(2,7)$ berekenen. We laten de uitwerkingen als oefening over:

g_i	g_1	g_2	g_3	g_4	g_5	g_6
$\lvert\mathrm{Cen}_G(g_i)\rvert$	168	8	4	3	7	7
$1_T \uparrow PSL(2,7)$	8	0	0	2	1	1
$\lambda_1 \uparrow PSL(2,7)$	8	0	0	-1	1	1
$\lambda_2 \uparrow PSL(2,7)$	8	0	0	-1	1	1

Irreducibiliteit van de inducties: We zien dat $\lambda_1 \uparrow PSL(2,7) = \lambda_2 \uparrow PSL(2,7)$. Vanaf nu spreken we dan ook over λ. Nu willen we natuurlijk weten of we reeds irreduciebele karakters gevonden hebben. Men rekent eenvoudig na dat

$$\langle 1_T \uparrow PSL(2,7), 1_T \uparrow PSL(2,7)\rangle = 2$$

en

$$\langle 1_T \uparrow PSL(2,7), 1_{PSL(2,7)}\rangle = 1.$$

Dus $1_T \uparrow PSL(2,7) = 1_{PSL(2,7)} + \chi$ (met χ een irreduciebele karakter van $PSL(2,7)$ van graad 7). Ook vinden we dat

$$\langle \lambda \uparrow PSL(2,7), \lambda \uparrow PSL(2,7)\rangle = 1.$$

Dus is $\lambda \uparrow PSL(2,7)$ irreduciebel. Noteer $\phi = \lambda \uparrow PSL(2,7)$.

Uit bestaande karakters nieuwe construeren.

Met behulp van χ_S vinden we nog een irreduciebele (het uitrekenen van χ_A geeft niet veel nuttigs in dit voorbeeld). De waarden van χ en χ_S staan uitgeschreven in volgende tabel.

g_i	g_1	g_2	g_3	g_4	g_5	g_6
$\lvert\mathrm{Cen}_G(g_i)\rvert$	168	8	4	3	7	7
χ	7	-1	-1	1	0	0
χ_S	28	4	0	1	0	0

We gaan nu verder zoals we bij het begin van de samenvatting hebben gezegd. We berekenen nu het inproduct met de reeds gekende irreduciebele karakters en halen hieruit een nieuw karakter. Zo vinden we dat

$$\langle \chi_S, 1_G \rangle = \langle \chi_S, \phi \rangle = \langle \chi_S, \chi \rangle = 1.$$

Bijgevolg is er een karakter ζ van $PSL(2,7)$ zodat

$$\chi_S = 1_G + \phi + \chi + \zeta.$$

Men vindt onmiddellijk dat $\langle \zeta, \zeta \rangle = 4$. Bijgevolg is $\zeta = 2\psi$ voor een irreduciebel karakter ψ of ζ is de som van vier verschillende irreduciebele karakters. Maar we weten dat er 6 irreduciebele karakters zijn en we kennen er reeds drie en geen van hen komt voor in de ontbinding van ζ. Dus kan ζ niet de som zijn van vier verschillende irreduciebele karakters (anders hebben we er zeven in totaal). Dus $\zeta = 2\psi$. De waarden van ζ en ψ zijn gegeven in onderstaande tabel.

g_i	g_1	g_2	g_3	g_4	g_5	g_6
$\lvert\mathrm{Cen}_G(g_i)\rvert$	168	8	4	3	7	7
ζ	12	4	0	0	-2	-2
ψ	6	2	0	0	-1	-1

Opvullen via orthonogonaliteitsrelaties:

De overblijvende irreduciebele karakters kan men vinden met behulp van de kolom orthogonaliteitsrelaties en de reeds gekende irreduciebele karakters 1_G, ϕ, ψ en χ. Het oplossen van de stelsels zou het volgende opleveren:

g_i	g_1	g_2	g_3	g_4	g_5	g_6
$\lvert\mathrm{Cen}_G(g_i)\rvert$	168	8	4	3	7	7
$1_{PSL(2,7)}$	1	1	1	1	1	1
χ	7	-1	-1	1	0	0
ϕ	8	0	0	-1	1	1
ψ	6	2	0	0	-1	-1
χ_5	3	-1	1	0	α	$\overline{\alpha}$
χ_6	3	-1	1	0	$\overline{\alpha}$	α

met $\alpha = (-1 + i\sqrt{7})/2$.

Hoofdstuk

2 Ringen en idealen

2.1 Inleiding

Ringtheorie is de studie van ringen. Dit zijn algebraïsche structuren in dewelke een optelling en vermenigvuldiging gedefinieerd zijn en die aan eigenschappen analoog aan de gehele getallen voldoen. In ringtheorie bestudeert men de structuur van ringen, hun representaties (een andere terminolgie is "moduultheorie"), speciale klassen van ringen (o.a. groepringen, lichamen, universele omhullende algebra's[1]).

Dedekind (1831-1916)

Noether (1882-1935)

Commutatieve ringen zijn veel beter gekend dan niet commutatieve ringen. Dit vooral dankzij de wisselwerking met algebraïsche meetkunde en getaltheorie (beide gebieden geven natuurlijke voorbeelden van commutatieve ringen). Vrij recent probeert men ook voor zekere klassen van niet commutatieve ringen een "meetkundige methode" te gebruiken door hen te beschouwen als ringen van functies op "niet-commutatieve ruimten".

De studie van ringen is ontstaan uit de theorie van polynoomringen en de theorie van algebraïsche gehele getallen. Het concept "ring" werd ingevoerd door Richard Dedekind.

De term ring (Zahlring) werd ingevoerd door David Hilbert in het artikel Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker Vereinigung, Vol. 4, 1897.

De eerste axiomatische definitie van een ring werd gegeven door Adolf Fraenkel in een essay in Journal für die reine und angewandte Mathematik (A. L. Crelle), vol. 145, 1914.

In 1921, gaf Emmy Noether de eerste axiomatische fundering van de theorie van commutatieve ringen in haar belangrijk artikel Ideal Theory in Rings.

[1]Sommigen denken, geheel ten onrechte, dat er maar één algebra bestaat.

2.2 Ringen: Definities en voorbeelden

Definitie 2.2.1. Zij R een verzameling met twee (binaire) bewerkingen, genaamd optelling en vermenigvuldiging,

$$\begin{aligned} + &: R \times R \to R \quad : \quad (a,b) \mapsto a+b \\ \cdot &: R \times R \to R \quad : \quad (a,b) \mapsto a \cdot b \end{aligned}$$

(Zoals gewoonlijk wordt de vermenigvuldiging genoteerd door juxtapositie.) Dan wordt R een ring (met eenheidselement) (Eng. ring, Fr. anneau) genoemd als aan de volgende voorwaarden voldaan is:

1. R is een commutatieve groep voor de optelling,
2. de vermenigvuldiging is associatief, d.w.z. $(rs)t = r(st)$, voor alle $r, s, t \in R$,
3. er bestaat een element 1 in R zodat $1r = r1 = r$, voor alle $r \in R$,
4. de vermenigvuldiging is distributief ten opzichte van de optelling, d.w.z. $(s + t)r = sr + tr$ en $r(s + t) = rs + rt$, voor alle $r, s, t \in R$.

Als de vermenigvuldiging ook commutatief is ($rs = sr$, voor alle $r, s \in R$), dan spreken we van een commutatieve ring.

Het is eenvoudig na te gaan dat het eenheidselement uniek is. (Vele auteurs eisen niet het bestaan van een eenheidselement voor een ring. In dat geval noemt men het object in Definitie 2.2.1 een ring met 1, of ring met eenheidselement.)

Wij merken op dat de voorwaarde dat de optelling commutatief eigenlijk overbodig is. Inderdaad, voor $r, s \in R$ geldt er

$$(r + s)(1 + 1) = r(1 + 1) + s(1 + 1) = r + r + s + s$$

en

$$(r + s)(1 + 1) = (r + s)1 + (r + s)1 = r + s + r + s.$$

Uit deze twee vergelijkingen volgt er dat $r + s = s + r$.

Als R een ring is, dan noteren wij met 0 het eenheidselement voor de optelling. Wij noemen dit ook het nulelement. De additieve inverse van $r \in R$ wordt $-r$ genoteerd. Bovendien is, per definitie, $r - s = r + (-s)$, voor $r, s \in R$.

In elke ring R geldt dat $0a = 0 = a0$, voor elke $a \in R$. Inderdaad,

$$0a + 0a = (0 + 0)a = 0a$$

zodat $0a = 0a - 0a = 0$.

Om de bewerkingen van een ring te specifiëren noteren wij een ring soms ook als $(R, +, .)$.


WEYL (1885-1955)

Zij R een ring. Een element $u \in R$ noemt men een eenheid (of inverteerbaar element) als het een linker en rechter inverse heeft. Dus u is een eenheid als er $x, y \in R$ bestaan zodat $ux = 1 = yu$. Het is welbekend dat dan $x = y$ en dat dit element uniek is. Het wordt genoteerd u^{-1}. Duidelijk is ook u^{-1} een eenheid en $(u^{-1})^{-1} = u$.

De verzameling $U(R)$ van de eenheden van een ring R is een groep voor de vermenigvuldiging (met eenheidselement 1). Deze groep noemt men de groep van de eenheden (of eenhedengroep) van R.

Voorbeelden 2.2.2.
(1) $\mathbb{Z}$ is een commutatieve ring.

(2) $R = \{0\}$ met de triviale bewerkingen $0 + 0 = 0 = 0.0$ is een commutatieve ring. Men noemt dit de triviale ring. Het is de enige ring met eenheidselement waarin $1 = 0$. Immers, als $1 = 0$, dan volgt hieruit voor elke $a \in R$ dat $a = 1a = 0a = 0$.

(3) Zij R een niet-triviale ring. Het element $0 \in R$ is dan geen eenheid. Indien alle niet-nul elementen van R inverteerbaar zijn, dan noemt men R een lichaam (Eng. division ring, skewfield). M.a.w. R is een lichaam als $U(R) = R \setminus \{0\}$. Een commutatief lichaam noemt men een *veld* of *veld* (Engels: *field*). Elk veld is dus een commutatieve ring.

Bekende voorbeelden van lichamen zijn $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Het meest bekende voorbeeld van een lichaam dat geen veld is, is de ring van de (reële) quaternionen, genoteerd $\mathbb{H} = \mathbf{H}(\mathbb{R})$. Deze ring is per definitie de 4-dimensionale reële vectorruimte met (standaard) basis $\{1, i, j, k\}$. Dus

$$\mathbf{H}(\mathbb{R}) = \{a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

De optelling wordt componentsgewijze gedefinieerd. Voor de vermenigvuldiging definieert men in eerste instantie:

$$i^2 = j^2 = k^2 = -1;$$
$$ij = k,\ jk = i,\ ki = j;$$

en

$$ji = -k,\ kj = -i, ik = -j.$$

Men breidt deze regels uit, via de distributiviteit, tot de volledige verzameling $\mathbb{H}$. Er volgt dat $\mathbb{H}$ een niet-commutatieve ring is. Bovendien, als

$$0 \neq h = a + bi + cj + dk \in \mathbb{H}$$

dan is

$$h(a - bi - cj - dk) = (a^2 + b^2 + c^2 + d^2)1 \neq 0.$$

Dus heeft h als multiplicatieve inverse

$$\frac{1}{a^2 + b^2 + c^2 + d^2} (a - bi - cj - dk).$$

Er volgt dat $\mathbb{H}$ inderdaad een lichaam is.

Merk op dat al het vorige geldig blijft als wij $\mathbb{R}$ vervangen door een veld K zodat

$$\text{als } (0,0,0,0) \neq (a,b,c,d) \in K^4 \text{ dan } a^2 + b^2 + c^2 + d^2 \neq 0.$$

De aldus bekomen ring noteren wij $\mathbf{H}(K)$. Bijvoorbeeld, de rationale quaternionenalgebra $\mathbf{H}(\mathbb{Q})$ is een lichaam dat een vier dimensionale vectorruimte is over $\mathbb{Q}$, echter $\mathbf{H}(\mathbb{C})$ is geen lichaam. Indien wij $\mathbb{R}$ vervangen door een commutatieve ring R dan is $\mathbf{H}(R)$ nog steeds een ring, doch zeker geen lichaam in het algemeen.

(4) Zij $R = \mathbb{Z}/n\mathbb{Z}$, de ring van de gehelen modulo n, met n een strikt positief geheel getal. (De elementen van deze ring zijn de verzamelingen $x + n\mathbb{Z}$, ook genoteerd als $\overline{x}$, met $x \in \mathbb{Z}$) Het is welbekend dat

$$U(R) = \{x + n\mathbb{Z} \mid x \in \mathbb{Z},\ \text{ggd}(n, x) = 1\}.$$

In cursus groepentheorie zagen we dat

$$|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n),$$

met φ de Euler φ-functie. Bovendien is $\mathbb{Z}/p\mathbb{Z}$ een veld met p elementen als p een priemgetal is.

(5) Als R een ring is, dan noteren wij met $\mathrm{M}_n(R)$ (soms noteert men dit ook door $\mathrm{M}_{n,n}(R)$) de verzameling van alle $n \times n$-matrices met componenten in R. Wij voorzien $M_n(R)$ van de gebruikelijke bewerkingen: als $A = (a_{ij})$ en $B = (b_{ij})$ dan is de (i,j)-de component van $A + B$ het element $a_{ij} + b_{ij}$, en de (i,j)-de component van AB is het element

$$\sum_{k=1}^{n} a_{ik} b_{kj}.$$

Er volgt dat $M_n(R)$ een ring is met als eenheidselement de identiteitsmatrix I. Indien R niet triviaal is en $n \geq 2$ dan is deze ring niet commutatief.

Indien F een veld is, dan noteert men de groep $U(M_n(F))$ meestal als $GL_n(F)$, en dit wordt de algemene lineaire groep van graad n genoemd. Uit de lineaire algebra weet men dat de elementen in $GL_n(F)$ precies die matrices zijn in $M_n(F)$ die een niet

nul-determinant hebben. Deze groep is in bijectief verband met de inverteerbare lineaire afbeeldingen van F^n naar zichzelf ($F^n = \{(f_1, \ldots, f_n) \mid f_i \in F,\ 1 \leq i \leq n\}$).

(6) Als R een ring is, dan is $R[X]$ de verzameling der veeltermen

$$r_n X^n + r_{n-1} X^{n-1} + \ldots + r_0$$

met coëfficiënten r_i in R. Een element $r_n X^n + r_{n-1} X^{n-1} + \ldots + r_0$ wordt uniek gedefinieerd door een (coëfficiënten)rij $(r_0, r_1, r_2, \ldots)$, elke $r_i \in R$, maar slechts eindig veel coëfficiënten r_i zijn niet nul. Men definieert bewerkingen op $R[X]$ als volgt. Als $f, g \in R[X]$ gedefinieerd worden door de respectievelijke coëfficiëntenrijen (a_i) en (b_i), dan wordt $f + g$ gedefinieerd door de coëfficiëntenrij (c_i) met $c_i = a_i + b_i$. Het product fg wordt gefinieerd door de coëfficiëntenrij (d_i) met

$$d_i = \sum_{k=0}^{i} a_k b_{i-k}.$$

Merk op dat de som- en productrijen slechts eindig veel niet-nul termen hebben. Men verifieert dan dat $R[X]$ een ring is. Bovendien is deze ring commutatief als en slechts als R commutatief is.

De polynomenring $R[X_1, X_2]$ in twee commuterende veranderlijken X_1 en X_2 definieert men als volgt:

$$R[X_1, X_2] = (R[X_1])[X_2].$$

In het algemeen, de polynomenring $R[X_1, \ldots, X_n]$ in $n > 1$ commuterende veranderlijken $X_1, \ldots, X_n$ definieert men recursief als volgt:

$$R[X_1, \ldots, X_n] = (R[X_1, \ldots, X_{n-1}])[X_n].$$

(7) Neem een (commutatieve) ring R, en een verzameling I.

$$R^I = \{f :\ I \to R \mid f \text{ is een afbeelding}\}$$

is opnieuw een (commutatieve) ring R voor de volgende bewerkingen. Zij $f, g \in R^I$, dan worden $f + g$ en fg als volgt gedefinieerd:

$$(f + g)(x) = f(x) + g(x) \quad ; \quad (fg)(x) = f(x)g(x)$$

voor elke $x \in I$.

(8) Zij K een veld, en V een vectorruimte over K. We noteren met $\mathrm{End}_K(V)$ de verzameling der endomorfismen van V, dit is de verzameling van alle K-lineaire afbeeldingen van

V naar V. Samen met de puntsgewijze optelling en de samenstelling van afbeeldingen, is dit een ring, die niet commutatief is als $\dim_K(V) > 1$.

(9) Zij H de $\mathbb{C}$-vectorruimte bestaande uit de klassefuncties op een eindige groep G. Wij weten dat de irreducibele karakters een orthonormale basis vormen. Uiteraard hebben wij ook een product op H. Inderdaad, zij $\chi, \psi \in H$ dan is het product $\chi\,\psi : G \to \mathbb{C}$ gedefinieerd door

$$(\chi\,\psi)(g) = \chi(g)\,\psi(g),$$

voor $g \in G$. Er volgt dat $(H, +, \cdot)$ een commutatieve ring is.

(11) Als $R_1, R_2, \ldots, R_n$ ringen zijn, dan is $R_1 \times R_2 \times \cdots \times R_n$ met de componentsgewijze gedefinieerde bewerkingen

$$\begin{aligned}(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) &= (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)\\ (a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) &= (a_1 b_1, a_2 b_2, \cdots, a_n b_n)\end{aligned}$$

opnieuw een ring. $R_1 \times R_2 \times \cdots \times R_n$ wordt het product van de ringen $R_1, R_2, \ldots, R_n$ genoemd. In het bijzonder is R^n een ring.

(12) Neem een veld K, en stel $R = K\langle x, y\rangle$ de veeltermring in twee niet-commuterende variabelen x en y, met commutatieregel

$$xy - yx = 1.$$

We noemen R een ring van differentiaaloperatoren, of ook, de eerste Weyl algebra over K.

Bijzondere ringen van afbeeldingen

Veronderstel dat $A, +$ een commutatieve groep is, met 0 als eenheidselement. De verzameling van alle afbeeldingen van A naar zichzelf noteren we als A^A. Voor $f, g \in A^A$, definiëren wij zoals gebruikelijk $f + g$ als de afbeelding

$$f + g : A \to A : x \mapsto f(x) + g(x)\,.$$

Het is eenvoudig na te gaan dat $A^A, +$ een commutatieve groep is, met als eenheidselement voor de optelling de nulafbeelding. De structuur $A, \circ$ is een monoïde met als eenheidselement de identieke afbeelding. Men kan nagaan dat $(f + g) \circ h = f \circ h + g \circ h$ maar dat niet noodzakelijk $h \circ (f + g) = (h \circ f) + (h \circ g)$. Als h een homomorfisme is van de groep $A, +$, dan geldt echter wel $h \circ (f + g) = (h \circ f) + (h \circ g)$ voor alle $f, g \in A^A$. Vandaar de volgende definitie.

Definitie 2.2.3. Veronderstel dat $A, +$ een commutatieve groep is. De *endomorfismering van A* is de verzameling van alle homomorfismen van A naar zichzelf, voorzien van de puntsgewijze optelling en de samenstelling. We noteren deze ring als $\mathrm{End}(A), +, \circ$, of ook als $\mathrm{End}(A)$.

In het algemeen is een endomorfisme van een algebraïsche structuur een afbeelding die de *structuur respecteert*. Voor groepen betekent dit dus een groephomomorfisme, voor vectorruimten een lineaire afbeelding. Een vectorruimte samen met de optelling van vectoren is eveneens een abelse groep. Een homomorfisme van deze abelse groep is echter niet noodzakelijk een lineaire afbeelding. De volgende definitie is dus niet onverwacht voor de endomorfismering van een vectorruimte.

Definitie 2.2.4. Veronderstel dat V een vectorruimte is over het veld K. De *endomorfismering van V* is de verzameling van alle K-lineaire afbeeldingen van V naar zichzelf, voorzien van de puntsgewijze optelling en de samenstelling. We noteren deze ring als $\mathrm{End}_K(V), +, \circ$, of ook als $\mathrm{End}_K(V)$.

In de rest van deze paragraaf definiëren we het begrip groepring. Veronderstel dat G een willekeurige groep is (multiplicatief genoteerd, met éénheidselement e) en R een willekeurige ring. Beschouw de verzameling van alle afbeeldingen van $G \to R$ met eindige support. We noteren deze verzameling als RG. De optelling in RG definiëren we als de puntsgewijze optelling. Voor elke twee elementen $\alpha, \beta \in RG$, definiëren we het product $\alpha\beta$ als de afbeelding van $G \to R$:

$$(\alpha\beta)(z) = \sum_{\substack{x,y \in G \\ xy=z}} \alpha(x)\beta(y)\,.$$

De support van α en β is eindig, dus er zijn maar een eindig aantal koppels (x, y) waarvoor $\alpha(x)\beta(y) \neq 0$. Van deze verzameling zijn er maar een deel waarvoor $xy = z$. Bovenstaande som is dus eindig, en de support van $\alpha\beta$ is ook eindig.

Het eenheidselement voor de vermenigvuldiging in RG is de afbeelding $\delta : G \to R$, $\delta(e_G) = 1_R$ en $\delta(g) = 0_R$, voor alle $g \neq e_G$.

Definieer voor elk element $g \in G$, de afbeelding $u_g : G \to R$, $u_g(h) = 1_R$ als $h = g$ en $u_g(h) = 0_R$ als $h \neq g$. Elk element $\alpha \in RG$ kan dan geschreven worden als eindige som

$$\sum_{g \in G} r(g)u_g\,.$$

We berekenen nu $u_g u_h$. Dit is de afbeelding

$$(u_g u_h)(z) = \sum_{xy=z} u_g(x)u_h(y)\,.$$

Uit de definities volgt dat $u_g(x)u_h(y) \neq 0$ als en slechts als $x = g$ en $y = h$. Dus $(u_g u_h)(z) \neq 0$ als en slechts als $z = gh$, dus het product $u_g u_h = u_{gh}$. We noteren het eenheidselement δ als u_{e_G} of u_e. We kunnen dus stellen dat RG de verzameling is van alle eindige sommen

$$\sum_{g \in G} r_g u_g \,,$$

waarbij er slechts een eindig aantal $r_g \in R$ verschillend zijn van nul. We bepalen nu het product van twee willekeurige elementen in RG. Voor een willekeurige $z \in G$ geldt

$$\begin{aligned}\left(\sum_{g\in G} r_g u_g\right)\left(\sum_{h\in G} r_h u_h\right)(z) &= \sum_{\substack{x,y\in G\\ xy=z}} \left((\sum_{g\in G} r_g u_g)(x)\right)\left((\sum_{h\in G} r_h u_h)(y)\right)\\ &= \sum_{\substack{x,y\in G\\ xy=z}} r_x r_y\\ &= \sum_{x,y\in G} r_x r_y u_{xy}(z)\end{aligned}$$

Dus

$$\left(\sum_{g\in G} r_g u_g\right)\left(\sum_{h\in G} r_h u_h\right) = \sum_{g,h\in G} r_g r_h u_{gh} \tag{2.1}$$

Verifieer als oefening dat de vermenigvuldiging distributief is ten opzichte van de optelling.

Definitie 2.2.5. Veronderstel dat G een groep is en R een ring. De verzameling RG, samen met de hierboven gedefinieerde optelling en vermenigvuldiging, noemen we de *groepring* van G over R.

Definitie 2.2.5 berust op een "concrete" definitie van de objecten u_g. In de literatuur wordt dit soms achterwege gelaten, en definieert men de elementen van de "abstracte" ring RG als *eindige*[2] *sommen van de vorm*

$$\sum_{g\in G}{}' r(g) u_g \,,$$

zonder in te gaan op de precieze aard van de elementen u_g. Vergelijking (2.1) *definieert* dan het product in RG. In Hoofdstuk 3 zal deze werkwijze toch vrij "concreet" blijken.

[2]let op de notatie $\sum'$

Uit Vergelijking (2.1) volgt dat RG commutatief is als en slechts als R en G commutatief zijn. De elementen u_g (met $g \in G$) noteert men dikwijls eenvoudig als g. Dus $\sum r_g u_g = \sum r_g g$. Het element $1g$ noteert men dan gewoonlijk ook als g en re_G noteert men als r. Dus $R = \{re = r \mid r \in R\}$ is een deelring van RG en $G = \{u_g = g \mid g \in G\}$ is een deelgroep van $U(RG)$.

Indien $R = k$ een veld is, dan is kG een k-algebra. In dit geval noemt men kG gewoonlijk een *groepalgebra*.

Domeinen

Definitie 2.2.6. Een element a in een ring R noemen we een nuldeler als $a \neq 0$, en als er een $b \neq 0$ in R bestaat zodat $ab = 0$ of $ba = 0$. Een commutatieve ring R zonder nuldelers noemen we een *gehele ring* of *domein*.

Stelling 2.2.7. *Een commutatieve ring R is een domein als en alleen als volgende implicatie geldt voor elke $a, b, c \in R$:*

$$ab = ac \quad \text{en} \quad a \neq 0 \quad \Longrightarrow \quad b = c \tag{2.2}$$

Bewijs. Onderstel eerst dat (2.2) geldt. Uit $a \neq 0$ en $ab = 0 = a0$ volgt dan dat $b = 0$, en er zijn dus geen nuldelers.

Omgekeerd, onderstel dat er geen nuldelers zijn. Als $a \neq 0$, en $ab = ac$, dan is $a(b - c) = 0$, en dus $b = c$ (anders is $b - c$ een nuldeler). □

Uit Stelling 2.2.7 volgt onmiddellijk dat elk veld een domein is. Als R een domein is dan is ook de polynomenring $R[X]$ een domein. Toon zelf aan dat het product van commutatieve ringen geen domein is (zelfs als de ringen in kwestie zelf domeinen zijn) en dat een matrixring $M_{nn}(R)$, met $n \geq 2$, nuldelers heeft.

2.3 Deelringen

Definitie 2.3.1. Zij R een ring. Een deelverzameling $S \subseteq R$ wordt een *deelring* van R genoemd, als S een ring is, met de bewerkingen geïnduceerd door de bewerkingen op R, en als bovendien S hetzelfde eenheidselement als R heeft voor de vermenigvuldiging.

Stelling 2.3.2. *Zij S een niet-lege deelverzameling van een ring R. Dan is S een deelring als en slechts als aan de volgende voorwaarden voldaan is*

1. *voor alle $a, b \in S$: $a - b, ab \in S$,*
2. *het eenheidselement van R behoort tot S.*

Bewijs. Het *criterium voor deelgroepen* levert onmiddellijk dat $S \subset R$ een deelgroep is van $R, +$ als en slechts als $a - b \in S$ voor alle $a, b \in S$. Uit de definitie van deelring volgt dat S gesloten moet zijn voor de optelling en de vermenigvuldiging, waardoor de vermenigvuldiging noodzakelijk associatief is, en distributief ten opzichte van de optelling. Tenslotte moet het eenheidselement voor de vermenigvuldiging ook tot S behoren, volgens de definitie van deelring. □

Voorbeelden 2.3.3.
(1) $\mathbb{Z}$ is een deelring van $\mathbb{Q}$.

(2) $\mathbb{Q}$ is een deelring van $\mathbb{R}$.

(3) $\mathbb{R}$ is een deelring van $\mathbb{C}$.

(4) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is een deelring van $\mathbb{C}$. De ring $\mathbb{Z}[i]$ wordt ook de *ring der gehelen van Gauß*[3] genoemd.

(5) $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is een deelring van $\mathbf{C}$. Bovendien is dit een veld, en dus noemen wij dit een deelveld van $\mathbb{C}$.

(6) D is een deelring van $M_{nn}(R)$, waar D de verzameling is van alle diagonaal matrices in $M_{nn}(R)$.

(7) Zij R een ring. Voor $a \in I$ beschouw

$$S = \{f \in R^I \mid f(a) = 0\}$$

Dan is S een ring met eenheidselement, maar geen deelring van R^I.

(8) $\mathbf{H}(\mathbb{Z})$ is een deelring van $\mathbf{H}(\mathbb{R})$ en $\mathbf{H}(\mathbb{R})$ is een deelring van $\mathbf{H}(\mathbb{C})$. Deze laatst heeft nuldelers.

(9) In $M_2(\mathbb{Q})$ beschouwen wij de volgende deelverzameling

$$\begin{bmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a \in \mathbb{Z},\ b, c \in \mathbb{Q} \right\}$$

[3] Carl Friedrich Gauß, naast Emmy Noether, één van de grondleggers van de algebra

Het is eenvoudig te verifiëren dat dit een deelring is van $M_2(\mathbb{Q})$.

(10) Zij R een ring en

$$Z(R) = \{z \in R \mid zr = rz \text{ voor alle } r \in R\}.$$

Men noemt dit het *centrum* van R. Het centrum is steeds een deelring. De elementen van $Z(R)$ noemt men *centrale elementen*.

Ga na dat $Z(\mathbf{H}(\mathbb{Q})) = \mathbb{Q}$ en

$$Z(M_n(R)) = \{zI \mid z \in Z(R)\},$$

met I de eenheidsmatrix in $M_n(R)$.

2.4 Ringhomomorfismen

Wij introduceren nu terminologie voor afbeeldingen tussen ringen die de structuur bewaren.

Definitie 2.4.1. Zij R en S ringen. Een afbeelding

$$f: \ R \to S$$

noemen we een *ringhomomorfisme* als

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b) \text{ en } \quad f(1_R) = 1_S,$$

voor alle $a, b \in R$. Een ringhomorfisme van R naar zichzelf noemen we een *ringendomorfisme* van R. Een injectief, surjectief, bijectief ringhomorfisme noemen we respectievelijk een *ringmonomorfisme*, een *ringepimorfisme* en een *ringisomorfisme*. Een ringisomorfisme van R naar zichzelf noemen we een *ringautomorfisme*. Als er een ringisomorfisme van R naar S bestaat, dan zeggen we dat R en S isomorf zijn, en we noteren dit door $R \cong S$.

Voorbeelden 2.4.2. (1) Zij n een geheel getal. Dan is

$$f : \mathbb{Z} \to \mathbb{Z} : z \mapsto nz$$

een ringhomomorfisme als en slechts als $n = 1$, d.w.z. f is de identieke afbeelding en een ringautomorfisme.

(2) Zij R_1 en R_2 ringen. Definieer

$$p_1 : R_1 \times R_2 \to R_1 : (r_1, r_2) \mapsto r_1.$$

Dan is p_1 een ringepimorfisme.

(3) De verzameling $S = \mathbb{Z}^3$ voorzien van de volgende bewerkingen

$$(a, b, c) + (d, e, f) = (a + d, b + e, c + f),$$
$$(a, b, c)(d, e, f) = (ad, bd + ce, cf)$$

is een ring. De afbeelding

$$\begin{bmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix} \to S : \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \mapsto (a, b, c)$$

definieert een ringisomorfisme.

(4) De afbeelding

$$\begin{bmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix} \to \mathbb{Z} : \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \mapsto c$$

definieert een ringepimorfisme. Dus de commutatieve ring $\mathbb{Z}$ is een epimorf beeld van een niet-commutatieve ring. Is dit een ringmonomorfisme?

(5) De afbeelding

$$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} : [x]_6 \mapsto ([x]_2, [x]_3)$$

definieert een ringisomorfisme. Met $[x]_n$ noteren wij het element $x+n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$. Bewijs in het algemeen dat de ringen $\mathbb{Z}/nm\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ isomorf zijn als $(n, m) = 1$ $(n, m \in \mathbb{Z})$.

(6) Zij R en S ringen. Bewijs dat $R \times S \cong S \times R$.

Isomorfe ringen voldoen aan dezelfde ringtheoretische eigenschappen. Vandaar dat men in classificatiestellingen geen onderscheid maakt tussen zulke ringen.

Stelling 2.4.3. *Als $f : R \to S$ een ringhomorfisme is, en R' is een deelring van R, dan is $f(R')$ een deelring van S.*

Bewijs. Oefening. □

In Definitie 2.2.3 hebben we de endomorfismering van een abelse groep $R, +$ ingevoerd. Als R ook een ring is, dan beschouwen we de volgende deelring van $\mathrm{End}(R)$.

$$\mathrm{End}_R(R) = \{f \in \mathrm{End}(R) \mid f(xr) = f(x)r, \text{ voor alle } r, x \in R\}.$$

Met andere woorden, $\mathrm{End}_R(R)$ is de deelring van $\mathrm{End}(R)$ bestaande uit alle homomorfismen van $R, +$ die ook R-lineair zijn. Om technische redenen is de voorwaarde met r langs de rechterkant geschreven. Wij tonen nu aan dat dit het typische voorbeeld van een ring is.

Stelling 2.4.4. *Zij R een ring. Dan is R isomorf met* $\mathrm{End}_R(R)$.

Bewijs. Voor $r \in R$ definieer de afbeelding

$$L_r : R \to R : a \mapsto ra.$$

Zij A de commutatieve groep $(R, +)$. Dan volgt er wegens de distributiviteit dat $L_r \in \mathrm{End}(A)$. Bovendien, voor elke $r, s, x \in R$,

$$L_r(xs) = r(xs) = (rx)s = (L_r(x))\, s.$$

Bijgevolg is $L_r \in \mathrm{End}_R(R)$. Definieer dus

$$L : R \to \mathrm{End}_R(R) : r \mapsto L_r.$$

Wij tonen nu aan dat L een ringisomorfisme is. Dit bewijst dan het resultaat.

Zij $r, s, a \in R$, dan

$$L_{rs}(a) = (rs)a = L_r(sa) = L_r(L_s(a)) = (L_r \circ L_s)(a)$$

Dus

$$L(rs) = L_{rs} = L_r \circ L_s = L(r) \circ L(s).$$

Bovendien

$$L_{r+s}(a) = (r + s)a = ra + sa = L_r(a) + L_s(a) = (L_r + L_s)(a),$$

zodat

$$L(r + s) = L_{r+s} = L_r + L_s = L(r) + L(s).$$

Dus is L een ringhomomorfisme.

Veronderstel dat $L(r) = L(s)$. Dan $r = L(r)(1) = L(s)(1) = s$. Dus is L injectief.

Tenslotte tonen wij aan dat L surjectief is. Zij $f \in \mathrm{End}_R(R)$. Stel $r = f(1)$. Dan, voor elke $a \in R$,

$$L(r)(a) = L_r(a) = ra = f(1)a = f(1a) = f(a).$$

Dus $L(r) = f$. Aangezien f willekeurig is, toont dit inderdaad de surjectiviteit van L aan. □

2.5 Idealen

Zij R een ring. Een niet-lege deelverzameling $L \subseteq R$ noemen we een *links ideaal* als $L, +$ een deelgroep is van $R, +$ en als L gesloten is voor vermenigvuldiging met elementen uit R, i.e.

$$\text{voor alle } l \in L \text{ en } r \in R : \ rl \in L \, .$$

Op dezelfde wijze definiëren we een *rechts ideaal*. Een *tweezijdig ideaal* is een links ideaal dat ook een rechts ideaal is. Als R commutatief is, dan vallen de drie begrippen samen. Als het duidelijk is dat we in een commutatieve context werken, dan spreken ook gewoon over een *ideaal*. Als we echter in een algemene, en dus niet noodzakelijk commutatieve context werken, dan zal de notie *ideaal* op een willekeurig ideaal slaan, dat dus links, rechts of tweezijdig kan zijn.

Lemma 2.5.1. *Een niet-lege deelverzameling L van een ring R is een links, respectievelijk rechts; tweezijdig, ideaal als en slechts als voldaan is aan volgende voorwaarden:*

1. *voor alle $l_1, l_2 \in L$, $l_1 - l_2 \in L$,*
2. *voor alle $l \in L$, $r \in R$, $rl \in L$, respectievelijk $lr \in L$; $rl \in L$ en $lr \in L$.*

Bewijs. Het criterium voor deelgroepen levert onmiddellijk (1). De tweede voorwaarde is evident. □

Een ring R is een tweezijdig ideaal van zichzelf. Als L een links ideaal is, en $1 \in L$, dan geldt voor alle $r \in R$ dat $r = r1 \in L$, en dus $L = R$, en analoog voor een rechts ideaal. Een ideaal dat 1 niet bevat, en dus een echt deel is van R, noemen we een *echt* ideaal. Een echt ideaal is dus niet hetzelfde als een deelring. In elke ring R is $\{0\}$ een tweezijdig ideaal. Dit wordt dikwijls het triviaal ideaal genoemd.

Lemma 2.5.2. *Stel $f : R \to S$ is een ringhomomorfisme. Dan is* $\mathrm{Ker}\,(f)$ *een tweezijdig ideaal.*

Bewijs. Stel $a, b \in \mathrm{Ker}\,(f)$. Dan is $f(a-b) = f(a) - f(b) = 0$. Stel $r \in R$ en $a \in Ker(f)$. Dan is $f(ar) = f(a)f(r) = 0 = f(r)f(a) = f(ra)$, dus $ra \in \mathrm{Ker}\,(f)$ en $ar \in \mathrm{Ker}\,(f)$. We mogen besluiten dat $\mathrm{Ker}\,(f)$ een tweezijdig ideaal is. □

Definitie 2.5.3. Zij R een ring en $a \in R$. Dan is $Ra = \{ra \mid r \in R\}$ een links ideaal. Men noemt dit het *linker (hoofd)ideaal voortgebracht door a*. Analoog is $aR = \{ar \mid r \in R\}$ het rechter ideaal voortgebracht door a. Het tweezijdig ideaal voortgebracht door a is

$$RaR = \{\sum_{i=1}^{n} r_i a s_i \mid n \in \mathbf{N},\ r_i, s_i \in R\}\,.$$

Indien R commutatief is, dan wordt dit ideaal dikwijls eenvoudig genoteerd als (a).

In het algemeen is Ra (en ook aR) geen tweezijdig ideaal. Wel is dit linker ideaal bevat in elk links ideaal dat a bevat en dus is Ra het kleinste links ideaal (voor de inclusie relatie) dat a bevat. Dus,

$$Ra = \cap_L L,$$

waarbij de doorsnede genomen wordt over alle linkse idealen L van R die a bevatten. Ook is RaR het kleinste tweezijdig ideaal dat a bevat. Dus

$$RaR = \cap_I I,$$

waarbij de doorsnede genomen wordt over alle tweezijdige idealen I van R die a bevatten.

Definitie 2.5.4. (i) Stel I, J zijn twee respectievelijk linkse, rechtse of tweezijdige idealen in een ring R. Dan is het somideaal, respectievelijk de doorsnede van de idealen

$$I + J = \{a + b | a \in I, b \in J\}\,,$$

respectievelijk,

$$I \cap J = \{a \in I \cap J\}\,.$$

(ii) Stel ofwel I is een links ideaal in een ring R ofwel J is een rechts ideaal in een ring R. Dan is het productideaal

$$IJ = \{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J\}\,.$$

Merk op dat het product van een links ideaal I en een rechts ideaal J dus opnieuw een ideaal is (ga dit zelf na als oefening), en dat $IJ \subset I \cap J$ als I en J tweezijdige idealen zijn. Het volgende voorbeeld toont aan dat deze inclusie niet altijd een gelijkheid is:

$$(4\mathbb{Z})(6\mathbb{Z}) = 24\mathbb{Z} \neq 4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}.$$

Lemma 2.5.5. *De volgende uitspraken zijn equivalent voor een niet triviale ring R.*

(i) R *is een lichaam.*

(ii) De enige linkeridealen zijn R *en* $\{0\}$.

(iii) De enige rechteridealen zijn R *en* $\{0\}$.

Bewijs. Stel R is een lichaam. Stel I is een ideaal verschillend van $\{0\}$. Kies $x \in I$, omdat R een lichaam is, bestaat er een $x^{-1} \in R$. Dus $x^{-1}x \in I$ of $xx^{-1} \in I$. In beide gevallen is $1_R \in I$, dus $I = R$. Stel omgekeerd dat de enige linkeridealen $\{0\}$ en R zijn. Kies $x \in R \setminus \{0\}$. Beschouw $I = Rx$ of $I = xR$. In beide gevallen bestaat er dus een $r \in R$ met $rx = 1$ of $xr = 1$, dus x heeft een inverse in R. □

Voorbeelden 2.5.6.

(1) Voor $n \in \mathbb{Z}$ is $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ een ideaal.

(2) Zij R een ring. Als $X \subseteq R$, dan noteren we (X) (of RXR) voor de doorsnede van alle idealen van R die X omvatten. Dit is het kleinste ideaal van R dat X omvat. Als $X = \{x\}$, dan is

$$(X) = RxR = \{\sum_{i=1}^{n} a_i x b_i \mid n \in \mathbb{N},\ a_1, \ldots, a_n, b_1, \ldots, b_n \in R\}.$$

Als R commutatief is, dan noteren wij (X) ook als RX; er volgt dat als $X = \{r_1, r_2, \ldots, r_n\}$, dan

$$RX = (r_1, r_2, \ldots, r_n) = Rr_1 + Rr_2 + \ldots + Rr_n.$$

In het geval dat $X = \{r_1\}$ en R commutatief is, dan is $(X) = Rr_1$ het hoofdideaal voortgebracht door r_1.

(3) Beschouw de veeltermenring $R[X]$ (R commutatief). De verzameling I van alle veeltermen van de vorm

$$\begin{aligned} r_1X + r_2X^2 + \cdots + r_nX^n &= X(r_1 + r_2X^1 + \cdots + r_nX^{n-1}) \\ &= (r_1 + r_2X^1 + \cdots + r_nX^{n-1})X, \end{aligned}$$

met andere woorden de verzameling der veeltermen die een veelvoud zijn van X, vormen een echt ideaal. Merk op dat $I = R[X]X = XR[X] = R[X]XR[X]$.

(4) In de matrixring $M_2(\mathbb{R})$ is

$$K_1 = \begin{bmatrix} \mathbb{R} & 0 \\ \mathbb{R} & 0 \end{bmatrix} = \left\{ \begin{bmatrix} a_{11} & 0 \\ a_{21} & 0 \end{bmatrix} \mid a_{11}, a_{21} \in \mathbb{R} \right\}$$

een links ideaal. Wij noemen dit eenvoudig de eerste kolom van $M_2(\mathbb{R})$. Analoog is de tweede kolom een links ideaal. Analoog definieert men de eerste rij

$$R_1 = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}$$

en de tweede rij

$$R_2 = \begin{bmatrix} 0 & 0 \\ \mathbb{R} & \mathbb{R} \end{bmatrix}$$

Dit zijn rechtse idealen van $M_2(\mathbb{R})$.

Algemener, voor een ring R en $1 \leq i \leq n$,

$$R_i = \{[a_{kl}] \in M_n(R) \mid a_{kl} = 0 \text{ voor } k \neq i\}$$

is een rechts ideaal in $M_n(R)$ (de i-de rij). De i-de kolom

$$K_i = \{[a_{kl}] \in M_n(R) \mid a_{kl} = 0 \text{ voor } l \neq i\}$$

is een links ideaal.

Merk op dat

$$R_1 + R_2 + \cdots + R_n = M_n(R)$$

en

$$K_1 + K_2 + \cdots + K_n = M_n(R).$$

(5) Beschouw de deelring

$$R = \begin{bmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{bmatrix}$$

van $M_2(\mathbb{Q})$. Verifiëer dat de volgende verzamelingen linkse idealen zijn van R (voor gegeven $k, l \in \mathbb{Z}$):

$$L_1 = \begin{bmatrix} k\mathbb{Z} & \mathbb{Q} \\ 0 & 0 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & \mathbb{Q} \\ 0 & l\mathbb{Z} \end{bmatrix}$$

en

$$L_3 = \begin{bmatrix} k\mathbb{Z} & \mathbb{Q} \\ 0 & l\mathbb{Z} \end{bmatrix}, \quad L_4 = \begin{bmatrix} 0 & k\mathbb{Z} \\ 0 & 0 \end{bmatrix}$$

Definitie 2.5.7. Zij R een ring en $X \subseteq R$, dan is de *rechter annihilator* $\mathrm{ra}(X)$ de verzameling $\{r \in R \mid xr = 0 \text{ voor alle } x \in X\}$. Het is eenvoudig na te gaan dat $\mathrm{ra}(X)$ een rechts ideaal van R is. Analoog definieert men de *linker annihilator* $\mathrm{la}(X)$ van X in R. Als X een rechts ideaal is dan volgt er dat $\mathrm{ra}(X)$ een tweezijdig ideaal is.

2.6 Isomorfismestelling voor ringen

Stelling 2.6.1. *Veronderstel dat $f : R \to S$ een ringhomomorfisme is. Als J een links ideaal (resp. rechts ideaal van S, of deelring van S) is, dan is $f^{-1}(J) = \{a \in R \mid f(a) \in J\}$ een links ideaal (resp. rechts ideaal van R, of deelring van R). In het bijzonder is* $\mathrm{Ker}\,(f) = f^{-1}\{0\}$ *een tweezijdig ideaal.*

Zij I een links, resp. rechts ideaal van R. Als f surjectief is, dan is $f(I) = \{f(i) \mid i \in I\}$ een links, resp. rechts ideaal van S.

Bewijs. Neem een links ideaal J van S, $a, b \in f^{-1}(J)$ en $r \in R$. Dan is $f(a-b) = f(a) - f(b) \in J$, zodat $a - b \in f^{-1}(J)$, en $f(ra) = f(r)f(a) \in J$, zodat $ra \in f^{-1}(J)$. Neem een links ideaal I van R, en $a, b \in I$, dan is $f(a) - f(b) = f(a-b) \in f(I)$, zodat $f(I)$ een abelse groep is voor de optelling. Neem $s \in S$, en $r \in R$ zodat $f(r) = s$ (f is surjectief). Dan is $sf(a) = f(r)f(a) = f(ra) \in f(I)$, zodat $f(I)$ een links ideaal is; zoals gewenst. Het bewijs voor rechtse idealen en deelringen is volkomen analoog. □

Omdat een ringhomomorfisme in de eerste plaats een groephomomorfisme is, verkrijgen wij het volgende resultaat.

Lemma 2.6.2. *Een ringhomomorfisme $f : R \to S$ is injectief als en slechts als* $\mathrm{Ker}\,(f) = \{0\}$.

In groepentheorie bewees men dat de normale deelgroepen overeenstemmen met de kernen van groephomomorfismen. Dat een normale deelgroep de kern is van een groephomomorfisme werd bewezen door het canonieke homomorfisme van een groep naar de quotiëntgroep van de groep met een normale deelgroep te beschouwen. Wij tonen nu de analoge eigenschap aan voor kernen van ringhomomorfismen.

Stelling 2.6.3. *Zij R een ring. De tweezijdige idealen van R zijn precies de kernen van alle ringhomomorfismen van R naar andere ringen.*

Bewijs. Onderstel dat I een tweezijdig ideaal van een ring R is. Beschouw de volgende equivalentierelatie op R:

$$a \sim b \text{ als en slechts als } a - b \in I.$$

De equivalentieklasse die $a \in R$ bevat noteren wij $\overline{a}$ of $a + I$ of $[a]$. Als $a \sim b$, dan schrijven we ook wel eens

$$a \equiv b \pmod{I}.$$

De verzameling van alle equivalentieklassen noteren we R/I:

$$R/I = \{[a] \mid a \in R\}.$$

Omdat R een abelse groep is, en dus I zeker normaal is als deelgroep, weten wij uit de groepentheorie dat R/I een abelse groep is voor de optelling

$$[a] + [b] = [a + b] \qquad (a, b \in R).$$

Op R/I definiëren we een vermenigvuldiging op de voor de hand liggende wijze

$$[a][b] = [ab],$$

waar $a, b \in R$. Deze vermenigvuldiging is welgedefinieerd. Inderdaad, veronderstel $x, y \in I$. Omdat I zowel een links als rechts ideaal is volgt er

$$(a + x)(b + y) - ab = ay + xb + xy \in I.$$

Bijgevolg

$$ab + I = (a + x)(b + y) + I.$$

Dus is $[ab] = [(a + x)(b + y)]$.

Ga zelf na dat deze vermenigvuldiging associatief is, en distributief ten opzichte van de optelling. Bovendien is [1] het eenheidselement. R/I is dus een ring, en we noemen deze een *quotiëntring*. De afbeelding

$$\pi : \ R \to R/I : a \mapsto [a]$$

is een ringepimorfisme met $\mathrm{Ker}\,(\pi) = I$. □

Merk op dat we in het bewijs van Stelling 2.6.3 de quotiëntring R/I gedefinieerd hebben. De quotiëntring is een belangrijk begrip in de ringtheorie. Nu tonen wij de ismorfismestelling aan.

Stelling 2.6.4. (Eerste isomorfismestelling) *Als $f : \ R \to S$ een ringhomomorfisme is, dan is $R/\mathrm{Ker}\,(f)$ isomorf met $f(R)$.*

Bewijs. We definiëren $\tilde{f} : \ R/\mathrm{Ker}\,(f) \to f(R)$ door

$$\tilde{f}([a]) = f(a).$$

Het is welbekend dat deze afbeelding welgedefinieerd is en een groepepimorfisme is. Wij herhalen het bewijs even. Veronderstel $a, b \in R$ en $[a] = [b]$. Dan is $a = b + x$, met

$x \in \mathrm{Ker}\,(f)$. Bijgevolg, $f(a) = f(b+x) = f(b) + f(x) = f(b)$. Bovendien als $a, b \in R$, dan

$$\begin{aligned} \tilde{f}([a]+[b]) &= \tilde{f}([a+b]) \\ &= f(a+b) \\ &= f(a)+f(b) \\ &= \tilde{f}([a])+\tilde{f}([b]) \end{aligned}$$

en

$$\begin{aligned} \tilde{f}([a][b]) &= \tilde{f}([ab]) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \tilde{f}([a])\tilde{f}([b]). \end{aligned}$$

Het is duidelijk dat $\tilde{f}$ surjectief is en dus is het een ringepimorfisme. Bovendien is $\tilde{f}$ injectief. Inderdaad zij $a \in R$ en onderstel dat $\tilde{f}([a]) = f(a) = 0$. Dan is $a \in \mathrm{Ker}\,(f)$, en $[a] = 0$ in $R/\mathrm{Ker}\,(f)$. □

Net zoals voor groepen heeft men ook een tweede en derde isomorfismestelling.

Stelling 2.6.5. *Zij I een tweezijdig ideaal van een ring R.*

1. (Tweede isomorfismestelling) *Er bestaat een bijectief verband tussen de verzameling van deelringen van R die I bevatten en de verzameling van deelringen van R/I. Onder dit bijectief verband corresponderen idealen van R die I bevatten met idealen van R/I.*
2. (Derde isormorfismestelling) *Als S een deelring is van R dan*
   (a) *$I + S = \{i + s \mid i \in I,\ s \in S\}$ is een deelring van R die I bevat,*
   (b) *$I \cap S$ is een ideaal van S, en*
   (c) *$S/(I \cap S) \cong (I + S)/I$.*

Bewijs. De tweede isomorfismestelling volgt eenvoudig uit Stelling 2.6.1. Wij bewijzen nu de derde isomorfismestelling. Beschouw daarom het ringepimorfisme $f : R \to R/I : r \mapsto r + I$. Zij g de beperking van dit homomorfisme tot de deelring S. Dus

$$g : S \to R/I : s \mapsto s + I.$$

Dan is g een ringhomomorfisme. Wegens Stelling 2.4.3 is het beeld $g(S) = \{s + I \mid s \in S\} = (I + S)/I$ een deelring van R/I. Verder

$$\mathrm{Ker}\, g = \{s \in S \mid s + I = I\} = S \cap I.$$

Dus volgt er uit de eerste isomorfismestelling dat $S/\mathrm{Ker}\, g = S/I \cap S \cong g(S) = (I + S)/I$. □

Voorbeelden 2.6.6.
(1) De ring der restklassen modulo n is de verzameling

$$\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},$$

voorzien van de optelling $\overline{i} + \overline{j} = \overline{k}$, waarbij k de rest is bij deling van $i + j$ door n, en, vermenigvuldiging $\overline{ij} = \overline{l}$, waarbij l de rest is bij deling van ij door n. Het is eenvoudig na te gaan dat

$$\mathrm{nat} : \mathbb{Z} \to \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

gedefinieerd door $\mathrm{nat}(z) = \overline{k}$, waarbij k de rest is bij deling van z door n, een ringepimorfisme is met $\mathrm{Ker}\,(\mathrm{nat}) = n\mathbb{Z}$. Dus wegens de isomorfismestelling: $\mathbb{Z}/n\mathbb{Z} \cong \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. In het vervolg maken wij dikwijls geen onderscheid tussen deze twee ringen, en gebruiken dus de notaties door mekaar.

Als n geen priemgetal is, dan bestaan er getallen $1 < r, s < n$ zodat

$$n = rs.$$

Dus $\overline{rs} = \overline{0}$, zodat $\mathbb{Z}/n\mathbb{Z}$ geen domein is. Als n een priemgetal is, dan is dit niet mogelijk, en dan is $\mathbb{Z}/n\mathbb{Z}$ een domein. We besluiten dat $\mathbb{Z}/n\mathbb{Z}$ een domein is als en slechts als n een priemgetal is. Bovendien is $\mathbb{Z}/n\mathbb{Z}$ een veld als n een priemgetal is. Voor dit laatste moeten wij nog aantonen dat $0 \neq \overline{r}$ een multiplicatieve inverse heeft als n priem is. Wel, omdat $\mathrm{ggd}(r, n) = 1$ weten wij dat er $x, y \in \mathbb{Z}$ bestaan zodat

$$xr + yn = 1.$$

Dus

$$\overline{1} = \overline{xr + yn} = \overline{xr} + \overline{yn} = \overline{xr};$$

zodat $\overline{x}$ de inverse is van $\overline{r}$.

(2) Neem een veld k, en $a \in k$. De afbeelding

$$f : \ k[X] \to k : \ P \mapsto P(a)$$

is een ringepimorfisme, en dus is $k \cong k[X]/\mathrm{Ker}\,(f)$. De veelterm P ligt in de kern van f als $P(a) = 0$, of als $(X - a)$ een factor is van P, met andere woorden

$$\mathrm{Ker}\,(f) = \{(X - a)Q(X) \mid Q(X) \in k[X]\} = (X - a).$$

Nemen we $a = 0$ dan volgt er

$$k[X]/k[X]X = k.$$

(3) Zij I een tweezijdig ideaal van een ring R. Stel $\pi : R \to R/I$ het natuurlijk epimorfisme. Dan is de afbeelding

$$f : M_{nn}(R) \to M_{nn}(R/I) : (a_{ij}) \mapsto (\pi(a_{ij}))$$

een ringepimorfisme met $\mathrm{Ker}\,(f) = M_{nn}(I)$. Dus

$$M_{nn}(R)/M_{nn}(I) \cong M_{nn}(R/I).$$

(4) Vrije K-ringen en ringen met generatoren en relaties.
Zij K een veld. De vrije algebra $K\langle X_1, \ldots, X_n\rangle$ in de niet-commuterende veranderlijken $X_1, \ldots, X_n$ is de K-vectorruimte met als basis X^*, de verzameling van alle eindige rijen in de veranderlijken $X_1, \ldots, X_n$ met inbegrip van de lege rij, die wij noteren door het symbool 1.

Een voorbeeld van zo een rij is

$$X_2X_1X_1X_3.$$

In X^* definiëren wij als bewerking (de vermenigvuldiging) de juxtapositie. Vervolgens breiden wij deze vermenigvuldiging via distributiviteit uit tot $K\langle X_1, \ldots, X_n\rangle$. Deze laatste is dan een ring. Merk op dat de elementen van X^* commuteren met de elementen van K. Het element 1 is het eenheidselement. Men noemt $R = K\langle X_1, \ldots, X_n\rangle$ de vrije algebra op $X_1, \ldots, X_n$.

Zij $F = \{f_j \mid j \in J\}$ een deelverzameling van R en zij $I = (F)$ het ideaal van R voortgebracht door F. Wij beschouwen dan de ring $\overline{R} = R/I$. Men noemt dit de K-algebra voortgebracht door $X_1, \ldots, X_n$ met relaties F. Zij $x_i = X_i + I \in \overline{R}$. Dan $f_j(x_1, \ldots, x_n) = 0 \in \overline{R}$.

Wij geven enkele specifieke voorbeelden.

1. Als $F = \{XY - YX\}$ dan $K\langle X, Y\rangle/F \cong K[X, Y]$.

2. Als $F = \{X^2 + 1, Y^2 + 1, XY + YX\}$ dan $\mathbb{R}\langle X, Y\rangle/(F) \cong \mathbf{H}(\mathbb{R})$.

3. Zij K een veld. Als $F = \{XY - YX - 1\}$ dan is $K\langle X, Y\rangle/(F)$ isomorf met de de Weyl algebra over K.

(5) Beschouw in $M_2(\mathbb{Z})$ de volgende deelring

$$\begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z} \right\}$$

Dan is

$$\begin{bmatrix} 0 & 2\mathbb{Z} \\ 0 & 0 \end{bmatrix} = \left\{ \begin{bmatrix} 0 & 2a \\ 0 & 0 \end{bmatrix} \mid a \in \mathbb{Z} \right\}$$

een ideaal van $\begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}$. De quotiëntring

$$\begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix} / \begin{bmatrix} 0 & 2\mathbb{Z} \\ 0 & 0 \end{bmatrix}$$

noteren wij

$$\begin{bmatrix} \mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \\ 0 & \mathbb{Z} \end{bmatrix}$$

Wij schrijven de elementen van deze ring eenvoudig als

$$\begin{bmatrix} a & x \\ 0 & b \end{bmatrix}$$

met $a, b \in \mathbb{Z}$ and $x \in \mathbb{Z}/2\mathbb{Z}$.

Stelling 2.6.7. *Onderstel dat $f : R \to S$ een ringhomomorfisme is, en dat $I \subseteq \mathrm{Ker}\,(f)$ een tweezijdig ideaal is van R. Dan bestaat er een uniek ringhomomorfisme $\tilde{f} : R/I \to S$ zodat*

$$\tilde{f} \circ \pi = f,$$

met andere woorden het volgende diagram commuteert:

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \downarrow{\scriptstyle \pi} & \nearrow \tilde{f} & \\ R/I & & \end{array}$$

Bewijs. Oefening. □

2.7 Priemidealen en maximale idealen

Priemgetallen zijn door de hoofdstelling van de rekenkunde te beschouwen als de bouwstenen van de gehele getallen. Het begrip priemgetal moet worden uitgebreid voor ringen verschillend van $\mathbb{Z}$.

Definitie 2.7.1. Een echt ideaal P van een ring R noemt men een *priemideaal* als, voor alle linkse, respectievelijk rechtse, tweezijdige idealen $I, J \subseteq R$, uit $IJ \subseteq P$ volgt dat $I \subseteq P$ of $J \subseteq P$.

Merk op dat het ideaal P links, rechts of tweezijdig kan zijn, en dit is onafhankelijk van het al dan niet links, rechts of tweezijdig zijn van de idealen I en J.

Definitie 2.7.2. Een ring R noemt men een *priemring* als $\{0\}$ een priemideaal is.

Definitie 2.7.3. Een links, respectievelijk rechts, tweezijdig deaal M van R noemt men een *maximaal links*, respectievelijk *rechts, tweezijdig maximaal ideaal* als er geen echt links, respectievelijk rechts, tweezijdig ideaal I van R bestaat dat M strikt bevat. Een ring R waarin $\{0\}$ een maximaal ideaal is noemt men een *enkelvoudige ring* (Engels: *simple ring*).

Lemma 2.7.4. *Het ideaal P is een priemideaal van de ring R als en slechts als voor alle $a, b \in R$, $aRb \subset P$ impliceert dat $a \in P$ of $b \in P$.*

Bewijs. Stel dat P een priemideaal is in de ring R. Kies $a, b \in R$ en veronderstel dat $aRb \subset P$. Dit laatste betekent dat $arb \in P$ voor alle $r \in R$. Omdat P een ideaal is, geldt dus voor alle $s \in R$, $sarb \in P$ of $arbs \in P$, naargelang P een links of rechts ideaal is. Dus ofwel $RaRb \subset P$ ofwel $aRbR \subset P$. Omdat P een priemideaal is, geldt dus $Ra \subset P$ of $Rb \subset P$ ofwel $aR \subset P$ of $bR \subset P$, m.a.w. $a \in P$ of $b \in P$.

Stel omgekeerd dat voor alle $a, b \in R$, $aRb \subset P$ impliceert dat $a \in P$ of $b \in P$. Stel I, J zijn twee linkse, respectievelijk rechtse, tweezijdige idealen. Kies $a \in I$, $b \in J$ willekeurig. Uit de veronderstellingen volgt $ar \in I$ of $rb \in J$ voor alle $r \in R$, dus $aRb \subset IJ \subset P$, dus $a \in P$ of $b \in P$. Als $a \notin P$, dan volgt, omdat deze redenering waar is voor alle $b \in J$, dat $J \subset P$. Als $a \in P$ voor alle $a \in I$, dan is $I \subset P$. □

Gevolg 2.7.5. *Stel dat R een commutatieve ring is. Dan is P een priemideaal van R als en slechts als voor alle $a, b \in R$, $ab \in P$ impliceert $a \in P$ of $b \in P$. Het ideaal P is een priemideaal als en slechts als $R \setminus P$ is gesloten voor vermenigvuldiging.*

Bewijs. Een ideaal P is een priemideaal als voor alle $r \in R$ en voor alle $a, b \in R$, $abr = arb \in P$ impliceert dat $a \in P$ of $b \in P$. Kiezen we $r = 1$, dan volgt het gestelde. Het tweede gedeelte volgt nu onmiddellijk. □

We hebben nu onmiddellijk het volgende resultaat.

Gevolg 2.7.6. *Een commutatieve ring is een priemring als en slechts als hij een domein is.*

Bewijs. De commutatieve ring R is een priemring als en slechts als $\{0\}$ een priemideaal is. Dit betekent precies dat $ab \in \{0\}$ impliceert dat $a \in \{0\}$ of $b \in \{0\}$ omdat R commutatief is, wat precies betekent dat R een domein is. □

Stelling 2.7.7. *Zij R een ring, en P en M echte idealen.*

1. *Het tweezijdig ideaal M is een maximaal ideaal als en slechts als R/M een enkelvoudige ring is.*
2. *Als R commutatief is, dan*
   (a) *P is een priemideaal als en slechts als R/P is een domein.*
   (b) *M is een maximaal ideaal als en slechts R/M een veld is.*

Bewijs. (1) Veronderstel dat M een maximaal ideaal is van R en veronderstel dat $\overline{J}$ een echt ideaal is van $\overline{R} = R/M$. Zij $\pi : R \to R/M$ het natuurlijk ringepimorfisme. Dan is $J = \pi^{-1}(\overline{J})$ een ideaal van R dat M bevat. Omdat $\pi(\pi^{-1}(\overline{J})) = \overline{J} \neq \overline{R}$, volgt er dat J een echt ideaal is van R. Aangzien M een maximaal ideaal is verkrijgen wij dus dat $M = J$ en dus $\overline{J} = \pi(J) = \pi(M) = \{0\}$. Dus is R/M een enkelvoudige ring.

Omgekeerd, veronderstel dat R/M een enkelvoudige ring is. Als I een echt ideaal is van R dat M bevat, dan is $\overline{I} = I/M$ een echt ideaal van R/M. Bijgevolg is $\overline{I} = \{0\}$. Omdat $I = \pi^{-1}(\overline{I})$ verkrijgen wij aldus dat $I = \pi^{-1}(\{0\}) = M$. Dus is M een maximaal ideaal.

(2) Veronderstel R een commutatieve ring is. Wij weten reeds dat R/P een domein is als en slechts als P een priemideaal is. Wegens gedeelte (1) is M een maximaal ideaal als en slechts als R/M een enkelvoudige ring is. Omdat R/M commutatief is volgt er uit Lemma 2.5.5 dat R/M een enkelvoudige ring is als en slechts als R/M een veld is. Dus volgt het resultaat. □

Gevolg 2.7.8. *Elk maximaal tweezijdig ideaal is een priemideaal.*

Bewijs. Veronderstel dat M een maximaal tweezijdig ideaal is van een ring R. Stel I, J zijn linkse, respectievelijk rechtse, tweezijdige, idealen van R zodat $IJ \subseteq M$. Omdat

R/M een enkelvoudige ring is, zijn de idealen $\pi(I)$ en $\pi(J)$ gelijk aan $\{0\}$ of R/M. Bovendien geldt

$$\pi(I)\pi(J) = \pi(IJ) \subseteq \pi(M) = \{0\}\,.$$

Dus moet $\pi(I) = \{0\}$ of $\pi(J) = \{0\}$. Bijgevolg,

$$I \subseteq \pi^{-1}(\pi(I)) = \pi^{-1}(\{0\}) = M$$

of

$$J \subseteq \pi^{-1}(\pi(J)) = \pi^{-1}(\{0\}) = M\,.$$

Zodat $I \subseteq M$ of $J \subseteq M$, zoals gewenst. □

Voorbeelden 2.7.9.
(1) Onderstel $\{0\} \neq I \subseteq \mathbb{Z}$ een ideaal. Stel

$$n = \min\{|x| \mid x \in I \setminus \{0\}\}$$

Dan is $n \in I$. Neem nu een willekeurige $a \in I$, en bepaal rest en quotiënt bij deling van a door n:

$$a = qn + r, \quad \text{met } 0 \leq r < n.$$

Nu is $r = a - qn \in I$, en dus moet $r = 0$. Hieruit volgt dat $a = qn$, en $I = (n) = n\mathbb{Z}$.

Ook is (0) een priemideaal omdat $\mathbb{Z}$ een domein is.

Zij $n \geq 1$ een geheel getal. Wij weten reeds dat $\mathbb{Z}/n\mathbb{Z}$ een domein is als en slechts n een priemgetal is. Dus is (n) een priemideaal als en slechts als n een priemgetal is. Omdat in dit geval $\mathbb{Z}/n\mathbb{Z}$ een veld is, volgt er dat elk niet-nul priemideaal een maximaal ideaal is.

(2) Zij k een veld, dan is $k[X]/k[X]X \cong k$. Dus is (X) een maximaal ideaal (en dus een priemideaal) van $k[X]$. Nemen wij een polynomenring $k[X, Y]$ in twee commuterende variabelen dan is $(X) = k[X, Y]X$ een priemideaal omdat $k[X, Y]/(X) \cong k[Y]$ een domein is. Omdat $k[Y]$ echter geen veld is, is (X) geen maximaal ideaal.

(3) Beschouw de ring

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

$\mathbb{Z}[\sqrt{2}]$ is een deelring van $\mathbb{R}$, en is dus een domein. We beweren dat

$$(\sqrt{2}) = \{(a + b\sqrt{2})\sqrt{2} = a\sqrt{2} + 2b \mid a, b \in \mathbb{Z}\}$$

een maximaal ideaal is. Immers,

$$\mathbb{Z}[\sqrt{2}]/(\sqrt{2}) \cong \mathbb{Z}/(2)$$

want

$$[a+b\sqrt{2}] = \begin{cases} [0] & \text{als } a \text{ even} \\ [1]+[(a-1)+b\sqrt{2}] = [1] & \text{als } a \text{ oneven} \end{cases} .$$

(4) Zij n een strikt positief geheel getal. Als R een ring is, dan zijn de idealen van $M_{nn}(R)$ precies de deelverzamelingen $M_{nn}(I)$ met I een ideaal van R. Bovendien is $M_{nn}(I)$ een priem- (respectievelijk maximaal) ideaal als en slechts als I een priem- (respectievelijk maximaal) ideaal is van R.

(5) De ring $\begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix}$ bevat het ideaal $\begin{bmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{bmatrix}$. Omdat

$$\begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix} / \begin{bmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{bmatrix} \cong \mathbb{Q} \times \mathbb{Q}$$

nuldelers bevat, volgt er dat $\begin{bmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{bmatrix}$ geen priemideaal is.

(6) We hebben steeds een ringhomomorfisme $f : \mathbb{Z} \to R$, gegeven door $f(n) = n$. In het tweede lid beschouwen we hier n als de som

$$\sum_{i=1}^{n} 1_R.$$

Als ideaal van $\mathbb{Z}$ is $\mathrm{Ker}\,(f) = m\mathbb{Z}$ met $m \in \mathbb{N}$. Men noemt m de *karakteristiek* van R. Als R een domein is (of meer bepaald een veld), dan is $\mathrm{Ker}\,(f)$ een priemideaal, en dan is de karakteristiek ofwel een priemgetal p, ofwel nul.

Er zijn dus eigenlijk twee soorten lichamen. Vooreerst zijn er de lichamen van karakteristiek 0. Dit zijn lichamen die $\mathbb{Z}$ als deelring bevatten, bijvoorbeeld $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. In zo een veld is dus geen enkel natuurlijk getal gelijk aan nul. Bovendien zijn er de lichamen van karakteristiek $p > 0$, waarbij p een priemgetal is. In een veld van karakteristiek p is het getal $p = \sum_{i=1}^{p} 1_R = 0$. Het basisvoorbeeld van zulk een veld is $\mathbb{Z}/p\mathbb{Z}$.

Stelling 2.7.10. *Zij $f : R \to S$ een ringepimorfisme. Dan is voor elk tweezijdig ideaal J van S de verzameling $f^{-1}(J)$ een tweezijdig ideaal van R en*

$$R/f^{-1}(J) \to S/J : [r] \mapsto [f(r)]$$

is een ringisomorfisme.

Bijgevolg, N is een maximaal ideaal van S als en slechts als $f^{-1}(N)$ een maximaal ideaal is van R. Als R en S commutatieve ringen zijn, dan is Q een priemideaal van S als en slechts als $f^{-1}(Q)$ een priemideaal is van R.

Bewijs. Zij J een tweezijdig ideaal van S. Dan weten wij reeds dat $f^{-1}(J)$ een tweezijdig ideaal is van R. Bovendien is de functie

$$\tilde{f} : R \to S/J : r \mapsto [f(r)]$$

een ringhomomorfisme. Omdat f surjectief is, is ook $\tilde{f}$ surjectief. Bovendien,

$$\begin{aligned} \text{Ker}\,(\tilde{f}) &= \{r \in R \mid \tilde{f}(r) = 0\} \\ &= \{r \in R \mid [f(r)] = 0\} \\ &= \{r \in R \mid f(r) \in J\} \\ &= f^{-1}(J) \end{aligned}$$

Wegens de isomorfismestelling verkrijgen wij dus dat

$$R/f^{-1}(J) \cong S/J.$$

Dus is in het bijzonder S/J is priem (respectievelijk enkelvoudig) als en slechts als $R/f^{-1}(J)$ priem (respectievelijk enkelvoudig) is. Het resultaat volgt dan uit Stelling 2.7.7. □

Merk op dat als $f : R \to S$ een willekeurig ringhomomorfisme is en Q een priemideaal van S is, dan is $f^{-1}(Q) = P$ een priemideaal van R op voorwaarde dat ofwel S commutatief is of f surjectief is . Wij bewijzen dit in het geval dat S commutatief is. Zij daarom $a, b \in R$ met $aRb \subseteq P$. Dan $f(a)f(b) = f(ab) \in f(P) \subseteq Q$. Omdat Q een priemideaal in de commutatieve ring S is, volgt er dat $f(a) \in Q$ of $f(b) \in Q$. Dus $a \in P$ of $b \in P$, zoals gewenst.

2.8 Maximale idealen

Een verzameling V is *partieel geordend* als er een orderelatie $\leq$ op V bestaat. Deze moet dus voldoen aan de volgende voorwaarden, voor elke $x,\ y,\ z \in V$:

$$\begin{aligned} x &\leq x, \\ \text{als } x \leq y \text{ en } y \leq x \quad &\text{dan} \quad x = y, \\ \text{als } x \leq y \text{ en } y \leq z \quad &\text{dan} \quad x \leq z. \end{aligned}$$

We noemen V *totaal geordend* als bovendien geldt dat

$$x \leq y \text{ of } y \leq x,$$

voor elke $x, y \in V$.

Een deelverzameling S van een partieel geordende verzameling V heeft een *bovengrens* als er een $x \in V$ bestaat zodat $s \leq x$, voor elke $s \in S$. De verzameling V noemen we *inductief geordend* als elke niet-lege totaal geordende deelverzameling T van V een bovengrens in V heeft. Een element v van V wordt een *maximaal element* genoemd indien de volgende eigenschap geldt:

$$\text{als } x \in V \text{ en } v \leq x \text{ dan } x = v.$$

Een element $x \in V$ wordt een *maximum* genoemd als $v \leq x$ voor alle $v \in V$. In dit geval is x het uniek maximaal element. Indien V totaal geordend is, dan is een element een maximum als en slechts als het het unieke maximaal element is.

Voorbeelden 2.8.1.
(1) $\mathbb{R}, \leq$ is totaal geordend, maar niet inductief geordend. Immers, $\mathbb{R}$ zelf heeft geen bovengrens.

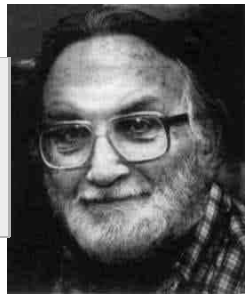
(2) Neem een willekeurige verzameling X, en stel $V = 2^X$, de verzameling van alle deelverzamelingen van X. De inclusie $\subseteq$ definieert een partiële orde op V, maar geen totale orde. V is wel inductief geordend, want X is een bovengrens voor elke $T \subseteq 2^X$.

(3) Een maximaal ideaal (resp. links ideaal) in een ring R is een maximaal element in de partieel geordende verzameling (voor de inclusie relatie) van al de echte idealen (resp. echte linkse idealen) van R.

Het *keuzeaxioma* zegt dat voor elke verzameling $\mathcal{S}$ waarvan de elementen zelf verzamelingen zijn, er een functie $f : \mathcal{S} \to \cup_{X \in \mathcal{S}} X$ bestaat zodat $f(X) \in X$. Men kan aantonen dat dit axioma equivalent is met het Lemma van Zorn.

Lemma 2.8.2. (Lemma van Zorn) *Een niet-lege inductief geordende verzameling heeft steeds een maximaal element.*

Met behulp van het Lemma van Zorn kunnen we het volgende cruciale resultaat bewijzen.



Zorn (1906-1993)

Stelling 2.8.3. *Zij L een echt links ideaal in een ring R. Dan bestaat er een maximaal links ideaal dat L bevat. Analoog is elk rechts (respectievelijk tweezijdig) ideaal bevat in een maximaal rechts (respectievelijk tweezijdig) ideaal.*

Bewijs. Zij L een links ideaal van R. Beschouw

$$V = \{J \mid J \text{ een echt links ideaal van } R \text{ en } L \subseteq J\}.$$

De verzameling V is niet leeg, omdat $L \in V$, en V is partieel geordend door de inclusie. Bovendien is V inductief geordend. Inderdaad, neem een totaal geordend deel $T = \{J_i \mid i \in K\}$ van V. Wij beweren dan dat

$$A = \cup_{i \in K} J_i$$

een links ideaal is. Zij daarom $a, b \in A$, en $r, s \in R$. Dan is $a \in J_i$ en $b \in J_j$ voor zekere indices $i, j \in K$. Omdat T totaal geordend is, is $J_i \subset J_j$ of $J_j \subset J_i$. Onderstel bijvoorbeeld $J_i \subset J_j$, dan is

$$ra + sb \in J_j \subseteq A$$

en A is een links ideaal. Bovendien is A is een echt links ideaal, want anders is $1 \in J_i$ voor een $i \in K$, en dan is J_i geen echt links ideaal.

We hebben dus dat $A \in V$, en A is een bovengrens voor T. Vanwege het Lemma van Zorn bevat V een maximaal element, en dit is noodzakelijk een maximaal links ideaal dat L bevat. □

Voorbeeld 2.8.4. Stel $R = \mathbb{Z}$, en beschouw $I = 6\mathbb{Z}$. Er bestaat dus een maximaal ideaal dat I bevat. In dit geval hebben we er twee: het ideaal $3\mathbb{Z}$ en het ideaal $2\mathbb{Z}$. Voor een willekeurig geheel getal $n \in \mathbb{Z}$ kan men eenvoudig alle maximale idealen vinden die $n\mathbb{Z}$ bevatten. Indien n priem is, dan is $n\mathbb{Z}$ uiteraard zelf maximaal.

2.9 Noetherse Ringen

Een *stijgende keten* in een partieel geordende verzameling V is een oneindige rij van (niet noodzakelijk verschillende) elementen $v_1, v_2, v_3, \ldots$ in V zodat

$$v_1 \leq v_2 \leq v_3 \leq \cdots$$

Wij zeggen dat V voldoet aan de *stijgendeketenvoordevoorwaarde*[4] als elke stijgende keten $v_1 \leq v_2 \leq v_3 \leq \cdots$ in V stationair is, d.w.z. er is een positief geheel getal n bestaat zodat

$$v_n = v_{n+1} = v_{n+2} = \cdots .$$

Lemma 2.9.1. *Zij V een partieel geordende verzameling. Dan voldoet V aan de stijgendeketenvoorwaarde als en slechts als elke niet lege deelverzameling van V een maximaal element heeft (dit noemt men de maximaalvoorwaarde).*

[4]Taalkundig gezien is dit zoals een uniekefactorisatiedomein.

Bewijs. Veronderstel dat V voldoet aan de maximaalvoorwaarde. Zij $v_1 \leq v_2 \leq v_3 \leq \ldots$ een stijgende keten in V. Stel $S = \{v_i \mid i \geq 1\}$. Aangezien S niet leeg is, volgt er dat S een maximaal element heeft, stel het element v_n. Omdat $v_{n+k} \geq v_n$ volgt er dat $v_{n+k} = v_n$, zoals gewenst.

Omgekeerd, veronderstel dat V voldoet aan de stijgende ketenvoorwaarde en stel $S \subseteq V$ met $S \neq \emptyset$. Veronderstel dat S geen maximaal element heeft. Dan is voor elke $s \in S$, de verzameling

$$S(s) = \{t \in S \mid t > s\}$$

niet leeg.

Kies nu $s_1 \in S$. Omdat s_1 niet maximaal is bestaat een $s_2 \in S(s_1)$ zodat $s_1 < s_2$. Omdat s_2 niet maximaal is bestaat $s_3 \in S(s_3)$ zodat $s_3 > s_2$. Wij gaan zo door en verkrijgen aldus een oneindige strikt stijgende keten

$$s_1 < s_2 < s_3 < \ldots,$$

een contradictie. □

De verzameling van de linkse idealen in een ring is partieel geordend voor de inclusie. Indien deze geordende verzameling voldoet aan de stijgendeketenvoorwaarde dan zeggen wij dat de ring voldoet aan de *stijgendeketenvoorwaarde op linkse idealen*.

Definitie 2.9.2. We noemen een ring R *links Noethers* als R voldoet aan de stijgendeketenvoorwaarde op linkse idealen. Analoog definieert men rechts Noetherse ringen. In het geval R commutatief is dan zijn beide voorwaarden dezelfde, en spreken wij eenvoudig over een Noetherse ring.

Stelling 2.9.3. *Een ring R is links Noethers als en slechts als alle linkse idealen van R eindig voortgebracht zijn.*

Bewijs. Onderstel eerst dat R links Noethers is en zij L een links ideaal van R. Als $L = \{0\}$ dan $L = R0$, i.h.b. is L eindig voortgebracht. Indien $L \neq \{0\}$ kies dan $0 \neq l_1 \in L$. Ofwel is $L = Rl_1$, en dus eindig voortgebracht, ofwel bestaat $l_2 \in (L \setminus Rl_1)$. Wij herhalen dit proces. Dus indien l_n gedefinieerd is en $L \neq Rl_1 + \cdots + Rl_n$, dan bestaat $l_{n+1} \in L \setminus (Rl_1 + \cdots + Rl_n)$. Dit proces moet stoppen na een eindig aantal stappen, zoniet krijgen wij een oneindige strikt stijgende keten:

$$Rl_1 \subset Rl_1 + Rl_2 \subset Rl_1 + Rl_2 + Rl_3 \subset \cdots,$$

in contradictie met de stijgendeketenvoorwaarde. Dus is L eindig voortgebracht.

Omgekeerd, veronderstel dat elk links ideaal van R eindig voortgebracht is. Zij

$$L_1 \subseteq L_2 \subseteq L_3 \subseteq \dots$$

een stijgende keten van linkse idealen van R. De unie

$$L = \bigcup_{i=1}^{\infty} L_i$$

is een links ideaal van R, en is dus eindig voorgebracht, door elementen $l_1, \dots, l_m \in R$. Vanaf een zekere index n geldt dat $l_1, \dots, l_m \in L_n$, en dus is $L \subset L_n$, zodat we noodzakelijkerwijs hebben dat

$$L_n = L_{n+1} = L_{n+2} = \dots = L.$$

□

Voorbeelden 2.9.4. (1) Elk veld is Noethers.

(2) $\mathbb{Z}$ is Noethers, want elk ideaal wordt voortgebracht door 1 element (zie Voorbeeld 2.7.9).

(3) Een matrixring $M_{nn}(k)$ over een veld k is links en rechts Noethers. Inderdaad, als wij k identificeren met de scalaire matrices, dan is elk links ideaal van $M_{nn}(k)$ een vectorruimte over k. Aangezien $M_{nn}(k)$ eindig dimensionaal is (van dimensie n^2), is ook elk links ideaal van dimensie ten hoogste n^2. Als nu $L_1 \subset L_2$ twee verschillende linkse ideal zijn, dan is ook $\dim(L_1) < \dim(L_2)$. Er volgt dan dat de stijgendeketenvoorwaarde op linkse idealen voldaan is.

Algemener kan men aantonen dat $M_{nn}(R)$ links Noethers is als R links Noethers is. Dit volgt bijvoorbeeld uit de resultaten die wij later in de theorie van modulen bewijzen.

(4) De veeltermring

$$R = k[X_1, X_2, \dots]$$

in een oneindig aftelbaar aantal variabelen is niet Noethers, aangezien het ideaal $(X_1, X_2, \dots)$ voortgebracht door al de variabelen niet eindig voortgebracht is, of, equivalent, de keten

$$(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \dots$$

niet stationair is.

(5) Beschouw de ring $R = \begin{bmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix}$. Dan is voor elke $n \in \mathbb{Z}$ de verzameling

$$L_n = \begin{bmatrix} 0 & \frac{1}{2^n}\mathbb{Z} \\ 0 & 0 \end{bmatrix}$$

een links ideaal. Omdat

$$L_1 \subset L_2 \subset L_3 \subset \cdots$$

volgt er dat R niet links Noethers is.

(6) Beschouw de ring $R = \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{bmatrix}$. Voor $n \in \mathbb{N}$ is de verzameling

$$R_n = \begin{bmatrix} 0 & \frac{1}{2^n}\mathbb{Z} \\ 0 & 0 \end{bmatrix}$$

een rechts ideaal in R. Bovendien is

$$R_1 \subset R_2 \subset R_3 \subset \ldots$$

een strikt stijgende rij van rechts idealen in R. Dus is R niet rechts Noethers. Toon aan dat de linkse idealen (verschillend van $\{0\}$ of R) van de volgende vorm zijn:

$$\begin{bmatrix} \mathbb{Q} & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & 0 \end{bmatrix},$$

of

$$\begin{bmatrix} 0 & \mathbb{Q} \\ 0 & n\mathbb{Z} \end{bmatrix}, \begin{bmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & n\mathbb{Z} \end{bmatrix},$$

voor een $n \in \mathbb{Q}$. Er volgt dat R wel links Noethers is.

Stelling 2.9.5. *Zij R een links Noetherse ring. Als I een tweezijdig ideaal is van R, dan is R/I ook links Noethers. M.a.w. elk homomorf beeld van een links Noetherse ring is zelf links Noethers.*

Bewijs. Zoals gewoonlijk schrijven we $\pi : R \to R/I$ voor het canonieke epimorfisme. Als L een links ideaal is van R/I, dan is $\pi^{-1}(L)$ een links ideaal van R. Wegens de veronderstelling is $\pi^{-1}(L)$ eindig voortgebracht. Zij $x_1, x_2, \cdots, x_n$ een stel voortbrengers van dit linker ideaal. De beelden $[x_1], [x_2], \ldots, [x_n]$ brengen L voort. □

Stelling 2.9.6. (Hilberts basisstelling) *Als R links Noethers is, dan is ook $R[X]$ links Noethers.*

Bewijs. Onderstel dat $L \subseteq R[X]$ een links ideaal is. Voor een veelterm $P(X) = r_0 + r_1X + \cdots + r_dX^d$, met $r_d \neq 0$, noemen we r_d de hoogstegraadscoëfficiënt. Neem de verzameling $h(L)$ van alle hoogstegraadscoëfficiënten van veeltermen in L, aangevuld met 0.

We beweren dat $h(L)$ een links ideaal van R is. Onderstel dat $a, b \in h(L)$, en onderstel $a, b, a-b \neq 0$. Dus er zijn veeltermen $P = aX^d + \cdots$ en $Q = bX^e + \cdots$ in L. Onderstel bijvoorbeeld dat $d \leq e$. Dan is $X^{e-d}P = aX^e + \cdots$ in L, en ook $X^{e-d}P - Q = (a-b)X^e + \cdots$. Dus is $a-b \in h(L)$. Als $r \in R$, dan is $rP = raX^d + \cdots \in L$, en dus $ra \in h(L)$.

Wegens de veronderstelling is $h(L)$ eindig voortgebracht. Neem veeltermen $F_1, F_2, \ldots, F_n \in L$ waarvan de hoogstegraadscoëfficiënten $h(L)$ voortbrengen. Neem N zo dat $N > \mathrm{gr}(F_i)$, voor elke $1 \leq i \leq n$. Voor elke $m \leq N$ beschouwen we de verzameling L_m van de hoogstegraadscoëfficiënten van de veeltermen in L die graad ten hoogste m hebben. Elke L_m is dan een links ideaal van R, en is dus eindig voortgebracht. Voor elke $m \leq N$ bestaat er dus een eindig stel veeltermen

$$F_{m_1}, F_{m_2}, \ldots, F_{m_{n_m}} \in L$$

waarvan de hoogstegraadscoëffiënten L_m voortbrengen. Beschouw nu het links ideaal L' in $R[X]$ dat voortgebracht wordt door al de F_i en F_{m_j}. Het is duidelijk dat L' eindig voortgebracht is, en dat $L' \subseteq L$. De stelling is bewezen als we kunnen aantonen dat $L' = L$.

Onderstel dat L' een echt deel van L is, en neem $G \in (L \setminus L')$ van minimale graad. Er zijn twee gevallen: ofwel is $\mathrm{gr}(G) = M > N$, ofwel is $\mathrm{gr}(G) = M \leq N$.

We beschouwen het eerste geval: $\mathrm{gr}(G) > N$. We schrijven

$$\begin{aligned} G &= bX^M + \cdots \\ F_i &= a_i X^{d_i} + \cdots \end{aligned}$$

$b \in h(L)$, het links ideaal voortgebracht door $a_1, a_2, \ldots, a_n$, en er zijn dus elementen $r_1, r_2, \ldots, r_n \in R$ zodat

$$b = \sum_{i=1}^{n} r_i a_i$$

en stel

$$F = \sum_{i=1}^{n} r_i X^{M-d_i} F_i = bX^M + \cdots \in L'.$$

Hieruit volgt dat $\mathrm{gr}(G-F) < M$, en dus $G - F \in L'$, door de minimaliteit van de graad van G. Maar nu volgt dat ook $G \in L'$, een contradictie.

Onderstel tenslotte dat $\mathrm{gr}(G) = m \leq N$. We schrijven

$$\begin{aligned} G &= bX^m + \cdots \\ F_{m_i} &= a_{m_i} X^{d_{m_i}} + \cdots \end{aligned}$$

waarbij we weten dat de graad van F_{m_i} ten hoogste m is. Nu is $b \in L_m$, het ideaal voortgebracht door $a_{m_1}, a_{m_2}, \ldots, a_{m_{n_m}}$, en dus

$$b = \sum_{i=1}^{n_m} r_i a_{m_i}$$

en

$$F = \sum_{i=1}^{n_m} r_i X^{m-d_{m_i}} F_{m_i} = bX^m + \cdots \in L'$$

Hieruit volgt dat $\mathrm{gr}(G-F) < m$, en dus $G - F \in L'$, door de minimaliteit van de graad van G. Hieruit volgt dat $G \in L'$, weerom een contradictie. □

2.10 De Chinese reststelling

Zij R een ring, en zij I en J twee linkse (respectievelijk rechtse, tweezijdige) idealen in R. Herinner dat de volgende verzamelingen opnieuw linkse (respectievelijk rechtse, tweezijdige) idealen van R zijn:

$$\begin{aligned} I + J &= \{a + b \mid a \in I,\ b \in J\} \\ IJ &= \{a_1 b_1 + \cdots + a_n b_n \mid a_1, \ldots, a_n \in I,\ b_1, b_2, \ldots, b_n \in J\} \\ I \cap J &= \{a \mid a \in I \text{ en } a \in J\} \end{aligned}$$

In de rest van dit hoofdstuk zullen wij ons beperken tot commutatieve ringen.

In een commutatieve ring noemen we twee idealen I en J *comaximaal* als $I + J = R$.

Stelling 2.10.1. *Zij R een commutatieve ring. Veronderstel dat I en J idealen zijn van R. Als I en J comaximaal zijn, dan is $IJ = I \cap J$.*

Bewijs. $(I \cap J) = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subseteq JI + IJ = IJ$. □

Een andere belangrijke eigenschap van comaximale idealen is de volgende stelling, bekend onder de naam "Chinese reststelling".

Stelling 2.10.2. (Chinese reststelling) *Onderstel dat $I_1, I_2, \ldots, I_n$ idealen zijn in de commutatieve ring R, die twee aan twee comaximaal zijn. Voor elk n-tal $(x_1, x_2, \cdots, x_n)$ in R^n bestaat er een $x \in R$ zodat*

$$x \equiv x_i \pmod{I_i} \quad (d.w.z.\ x - x_i \in I_i),$$

voor elke index i.

Bewijs. Wij behandelen eerst het geval $n = 2$. Omdat $I_1 + I_2 = R$ bestaan er $a_1 \in I_1$ en $a_2 \in I_2$ zodat $a_1 + a_2 = 1$. Stel $x = a_2x_1 + a_1x_2$, zodat

$$x - x_1 = (a_2 - 1)x_1 + a_1x_2 = a_1(x_2 - x_1) \in I_1.$$

Op analoge wijze vinden we dat $x - x_2 \in I_2$.

Vervolgens behandelen we het algemene geval. Dus, n is willekeurig. Voor elke $i \neq 1$ passen we het geval $n = 2$ toe op de idealen I_1 en I_i en met $x_1 = 0$, $x_i = 1$. We vinden aldus een stel elementen $y_2, y_3, \ldots, y_n$ in R, zodat

$$y_i \equiv 0 \pmod{I_1} \text{ en } y_i \equiv 1 \pmod{I_i}.$$

M.a.w.

$$y_i \in I_1 \text{ en } y_i + z_i = 1 \text{ met } z_i \in I_i.$$

In het produkt

$$1 = \prod_{i=2}^{n} (y_i + z_i)$$

zijn alle termen, op $z_2 \cdots z_n$ na, een veelvoud van een der y_i, en dus gelegen in I_1. We vinden dus dat

$$1 = z_2 \cdots z_n + a_1,$$

met $a_1 \in I_1$. Hieruit volgt dat $1 \in I_1 + I_2I_3 \cdots I_n$, zodat I_1 en $I_2I_3 \cdots I_n$ comaximaal zijn. Op deze twee idealen kunnen we het geval $n = 2$ toepassen, en we vinden een $t_1 \in R$ zodat

$$t_1 \equiv 1 \pmod{I_1} \text{ en } t_1 \equiv 0 \pmod{I_2I_3 \cdots I_n}$$

Aangezien $I_2I_3 \cdots I_n \subseteq I_2 \cap I_3 \cap \cdots \cap I_n$, volgt hieruit dat $t_1 \equiv 0 \pmod{I_j}$, voor elke $j \neq 1$, of met andere woorden

$$t_1 \equiv \delta_{1j} \pmod{I_j}$$

voor elke j. Op dezelfde wijze vinden we $t_2, t_3, \ldots, t_n \in R$ zodat

$$t_i \equiv \delta_{ij} \pmod{I_j}$$

Stel nu $x = x_1t_1 + x_2t_2 + \cdots + x_nt_n$. Dan is

$$\begin{aligned} x &\equiv \sum_{i=1}^{n} x_i t_i \pmod{I_j} \\ &\equiv \sum_{i=1}^{n} x_i \delta_{ij} \pmod{I_j} \\ &\equiv x_j \pmod{I_j} \end{aligned}$$

en dit bewijst onze stelling. □

Opmerking. In het bewijs van de Chinese reststelling bewezen wij dat als $I_1, I_2, \ldots, I_n$ twee aan twee comaximale idealen zijn in een commutatieve ring, dan zijn I_1 en $I_2 \cdots I_n$ ook comaximaal.

Veronderstel, zoals in de stelling, dat de idealen $I_1, I_2, \ldots, I_n$ twee aan twee comaximaal zijn. Bekijk de afbeelding

$$f: \ R \to R/I_1 \times R/I_2 \times \cdots R/I_n$$

gegeven door

$$f(r) = (r + I_1, \ r + I_2, \ldots, \ r + I_n)$$

Het is gemakkelijk in te zien dat f een ringhomomorfisme is, en dat

$$\text{Ker}\,(f) = \cap_{i=1}^{n} I_i = I_1 I_2 \ldots I_n$$

Uit de Chinese reststelling volgt dat f surjectief is. Als we dit combineren met Stelling 2.6.4, dan vinden we volgend resultaat.

Gevolg 2.10.3. *Zij R een commutatieve ring. Als de idealen $I_1, I_2, \ldots, I_n$ twee aan twee comaximaal zijn, dan hebben we een isomorfisme*

$$R/\bigcap_{i=1}^{n} I_i \cong \prod_{i=1}^{n} R/I_i$$

Voorbeeld 2.10.4. (1) Neem $R = \mathbb{Z}$, $I_1 = (2)$, $I_2 = (3)$ en $I_3 = (25)$. Deze idealen zijn twee aan twee comaximaal. Kies bijvoorbeeld $x_1 = 1$, $x_2 = 4$ en $x_3 = 3$. Het element x waarvoor het bestaan uit de Chinese reststelling volgt, is bijvoorbeeld $x = 103$.

(2) Neem $R = \mathbb{Z}$, en $n > 1$ een natuurlijk getal. Het getal n kan ontbonden worden in priemfactoren p_i:

$$n = p_1^{r_1} p_2^{r_2} p_3^{r_3} \ldots p_l^{r_l},$$

met $p_i \neq p_j$ voor $i \neq j$, en $r_i > 0$. Stel $I_i = (p_i^{r_i})$ in Gevolg 2.10.3. Omdat de I_j twee per twee comaximaal zijn, geldt wegens Stelling 2.10.1 en de opmerking na de Chinese reststelling dat

$$n\mathbb{Z} = \bigcap_{i=1}^{l} I_i = \cap_{i=1}^{l} p_i^{r_i}\mathbb{Z}$$

en dus

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \mathbb{Z}/p_2^{r_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_l^{r_l}\mathbb{Z} \tag{2.3}$$

2.11 Breukenlichamen, breukenringen en lokale ringen

De rationale getallen $\mathbb{Q}$ kunnen geconstrueerd worden door aan de gehele getallen $\mathbb{Z}$ de inverse "toe te voegen" van elk van nul verschillend getal:

$$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0\}.$$

In feite kunnen we $\mathbb{Q}$ definiëren als de equivalentieklassen van $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ voor de equivalentierelatie $\sim$, gegeven door

$$(m, n) \sim (m', n') \text{ als en slechts als } mn' = m'n.$$

In deze paragraaf veralgemenen we deze constructie naar willekeurige commutatieve ringen.

Definitie 2.11.1. Veronderstel dat R een commutatieve ring is. Een deelverzameling $S \subset R$ is een *multiplicatief gesloten deel* als $1 \in S$ en voor alle $s_1, s_2 \in S$, $s_1 s_2 \in S$.

Beschouw een willekeurige commutatieve ring R en een multiplicatief gesloten deel S. Op $R \times S = \{(a, s) \mid a \in R,\ s \in S\}$ definiëren we een equivalentierelatie als volgt:

$$(a, s) \sim (a', s') \text{ als en slechts als } s''(as' - a's) = 0 \text{ voor een } s'' \in S.$$

Wij tonen nu aan dat $\sim$ een equivalentierelatie is. Omdat $1(as - as) = 0$, volgt er $(a, s) \sim (a, s)$. Dus is de relatie reflexief. Om de symmetrie aan te tonen, onderstel $(a, s) \sim (a', s')$, zodat $s''(as' - a's) = 0$. Dan is $s''(a's - as') = 0$, zodat $(a', s') \sim (a, s)$. Tenslotte, voor de transitiviteit, onderstel $(a, s) \sim (a', s')$ en $(a', s') \sim (b, t)$. Er bestaan dan $s'', t'' \in S$ zodat $s''(as' - a's) = 0$ en $t''(a't - bs') = 0$. Vermenigvuldig beide vergelijkingen met respectievelijk tt'' en ss'', dan

$$\begin{aligned} tt''s''as' - tt''s''a's &= 0, \\ ss''t''a't - ss''t''bs' &= 0. \end{aligned}$$

Optellen van beide vergelijkingen geeft

$$tt''s''as' - ss''t''bs' = s''t''s'(ta - sb) = 0,$$

zodat $(a, s) \sim (b, t)$.

Op de verzameling van de equivalentieklassen $(R \times S)/\sim$ definiëren we een optelling en een vermenigvuldiging als volgt:

$$\begin{aligned} (a, s) + (a', s') &= (s'a + sa', ss'), \\ (a, s)(a', s') &= (aa', ss'). \end{aligned}$$

Ga zelf na dat deze definities onafhankelijk zijn van de gekozen representanten. De verzameling $(R \times S)/\sim$ noteren we ook door $S^{-1}R$, en deze is een commutatieve ring voor deze optelling en vermenigvuldiging. We noemen $S^{-1}R$ de *breukenring* (of *quotiëntring*) ten opzichte van het multiplicatief deel S, of ook de *lokalisatie* van R aan S. De equivalentieklasse waartoe (a, s) behoort noteren we door $\frac{a}{s}$ of a/s, of as^{-1}. Het nul-element is $\frac{0}{1} = \frac{0}{s}$ (voor elke $s \in S$), en het eenheidselement is $\frac{1}{1}$.

Stelling 2.11.2. *Zij S een multiplicatief gesloten deel van de commutatieve ring R. Dan is de afbeelding*

$$f : \ R \to S^{-1}R : a \mapsto \frac{a}{1}$$

een ringhomomorfisme met kern

$$K = \{a \in R \mid as = 0 \text{ voor een } s \in S\}.$$

Bewijs. Het eerste deel van de stelling is triviaal. Voor het tweede gedeelte, onderstel dat

$$f(a) = \frac{a}{1} = \frac{0}{s}$$

Dan bestaat er een $s' \in S$ zodat $s'(as - 0) = ass' = 0$. Omdat $ss' \in S$, volgt er dat $a \in \{a \in R \mid as = 0 \text{ voor een } s \in S\}$. Omgekeerd, als $sa = 0$ met $s \in S$ en $a \in R$, dan is $s(a1 - 0) = 0$ en dus

$$f(a) = \frac{a}{1} = \frac{0}{1}.$$

Bijgevolg $a \in \text{Ker}\,(f)$. □

Gevolg 2.11.3. *Als R een domein is, en $0 \notin S$, dan is $f: R \to S^{-1}R$ injectief.*

Voorbeelden 2.11.4. (1) Zij R een domein. Dan is $S = R \setminus \{0\}$ multiplicatief gesloten. In $S^{-1}R$ is elk van nul verschillend element inverteerbaar, en we noemen $Q(R) = S^{-1}R$ het *breukenveld* van R. Uit Gevolg 2.11.3 volgt dat $R \to Q(R)$ injectief is. Het breukenveld van $\mathbb{Z}$ is $\mathbb{Q}$, en voor elk veld k is het breukenveld van de veeltermenring $k[X]$ het veld der rationale vormen $k(X) = \{\frac{f(X)}{g(X)} \mid f(X), g(X) \in k[X],\ 0 \neq g(X)\}$.

(2) Zij R een commutatieve ring. Neem $f \in R$, en stel

$$S = \{1, f, f^2, f^3, \ldots\}.$$

We noteren nu

$$R_f = S^{-1}R = \{\frac{a}{f^i} \mid a \in R, i \in \mathbb{N}\}$$

Merk op dat er ringen bestaan zodat f *nilpotent* is, d.w.z. er bestaat een natuurlijk getal $n > 0$ zodat $f^n = 0$. In dit geval is de natuurlijke afbeelding van R naar $S^{-1}R$ niet injectief.

(3) Als $0 \in S$, dan geldt voor alle $a \in R$ en $s \in S$ dat

$$\frac{a}{s} = \frac{0}{1}$$

aangezien $0(a1 - s0) = 0$. Derhalve is $S^{-1}R = \{0\}$ de triviale ring.

(4) Neem twee lichamen k_1 en k_2, en beschouw de productring $R = k_1 \times k_2$. Stel $S = \{(0, x) \mid x \neq 0 \in k_2\} \cup \{(1, 1)\}$. Uit Stelling 2.11.2 volgt dat

$$\mathrm{Ker}\,(f) = k_1 \times \{0\}.$$

Daarnaast is

$$S^{-1}R \cong \{0\} \times k_2 \cong k_2$$

We hebben dus een situatie waar de canonieke afbeelding $f: R \to S^{-1}R$ niet injectief is, maar wel surjectief.

(5) Onderstel dat P een priemideaal is in een commutatieve ring R. Dan is $S = R \setminus P$ multiplicatief gesloten. De breukenring $(R \setminus P)^{-1}R = R_P$ zullen we hierna bestuderen.

Definitie 2.11.5. Een commutatieve ring R noemen we een lokale ring als R precies één maximaal ideaal heeft.

Een veld heeft slechts één echt ideaal, en is dus een lokale ring. Vooraleer we nog meer voorbeelden van lokale ringen geven, formuleren we eerst het volgend criterium.

Stelling 2.11.6. *Een commutatieve ring R is lokaal als en slechts als de niet inverteerbare elementen van R een ideaal vormen. Dit ideaal is dan het unieke maximale ideaal (en dus het maximum ideaal).*

Bewijs. Onderstel eerst dat R een lokale ring is, met uniek maximaal ideaal M. Zij $a \in R \setminus M$. Als a niet inverteerbaar is, dan is het ideaal (a) een echt ideaal, en dus bevat in een maximaal ideaal N. Omdat $N \neq M$ zijn er dus twee maximale idealen. Dit is in tegenspraak met de onderstelling dat R lokaal is. Dus alle niet inverteerbare elementen zitten in M. Omgekeerd zijn alle elementen van M niet inverteerbaar (omdat $1 \notin M$). Dus M is een ideaal dat bestaat uit alle niet inverteerbare elementen.

Onderstel omgekeerd dat de verzameling der niet inverteerbare elementen van R een ideaal M vormen. Neem nu een willekeurig ander echt ideaal J van R. Omdat J alleen niet inverteerbare elementen bevat, is $J \subseteq M$, en dus is M het enige maximale ideaal. Bijgevolg is R lokaal. □

Stelling 2.11.7. *Onderstel dat P een priemideaal is in een commutatieve ring R, en stel $S = R \setminus P$. De ring $S^{-1}R = R_P$ is een lokale ring, en het unieke maximale ideaal is het ideaal PR_P voortgebracht door het beeld van P in R_P onder het natuurlijke homomorfisme. De ring R_P noemen we de gelokaliseerde ring aan het priemideaal P.*

Bewijs. Zij $r \in R$ en $s \in S$. We beweren dat $r/s \in R_P$ inverteerbaar is als en alleen als $r \in S$. Onderstel eerst dat r/s inverteerbaar is met inverse t/u, $t \in R$ en $u \in S$. Omdat

$$\frac{r}{s}\frac{t}{u} = \frac{rt}{su} = 1$$

bestaat een $s' \in S$ zodat

$$s'(rt - su) = 0.$$

Hieruit volgt dat

$$s'rt = s'su \in S\,.$$

Stel $rt \notin S$, dan is $rt \in P$, en dus ook $s'rt \in P$, maar $S = R \setminus P$. Dus $rt \in S$. Het zelfde argument levert ook dat $r \in S$ en $t \in S$. Omgekeerd, als $r \in S$, dan is s/r het invers van r/s.

De verzameling der niet inverteerbare elementen van R_P is dus

$$\{\frac{r}{s} \mid r \in P,\ s \in S\}$$

en dit is juist het ideaal PR_P voortgebracht door (het beeld van) P in R_P. De niet-inverteerbare elementen vormen dus een ideaal, en R_P is een lokale ring. □

Voorbeelden 2.11.8. (1) Neem een domein R. Het triviale ideaal (0) is dan een priemideaal, en de gelokaliseerde ring $R_{(0)}$ is het breukenveld van R.

(2) Neem een priemgetal p. De gelokaliseerde van $\mathbb{Z}$ aan het priemideaal (p) is

$$\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} \mid m \in \mathbb{Z} \text{ en } n \text{ is geen veelvoud van } p\}.$$

(3) Zij K een veld. De ring van de *machtreeksen* over K, genoteerd $K[[X]]$, is per definitie de verzameling van alle formele (oneindige) sommen

$$\sum_{i\in\mathbb{N}} k_i X^i,$$

met alle $k_i \in K$, en voorzien van de volgende bewerkingen:

$$\sum_{i\in\mathbb{N}} k_i X^i + \sum_{i\in\mathbb{N}} l_i X^i = \sum_{i\in\mathbb{N}} (k_i + l_i) X^i$$

(de componentsgewijze optelling), en

$$\left(\sum_{i\in\mathbb{N}} k_i X^i\right)\ \left(\sum_{j\in\mathbb{N}} l_j X^j\right) = \sum_{u\in\mathbb{N}} m_u X^u,$$

met

$$m_u = \sum_{i=0}^{u} k_i l_{u-i} \in K.$$

Ga na dat $K[[X]]$ inderdaad een commutatieve ring is, en dat $K[X]$ een deelring is van $K[[X]]$. Toon ook aan dat een element $\sum_{i\in\mathbb{N}} k_i X^i$ inverteerbaar is in $K[[X]]$ als en slechts als $k_0 \neq 0$. Bewijs vervolgens dat $K[[X]]$ een lokale ring is.

2.12 Hoofdideaal- en Euclidische ringen

In deze paragraaf beschouwen wij veralgemeningen van de aritmetische structuur van de ring van de gehele getallen $\mathbb{Z}$. Zoals eerder gezegd beperken wij ons tot commutatieve ringen.

Definitie 2.12.1. Een commutatieve ring R noemen we een hoofdideaalring als elk ideaal een hoofdideaal is, dit wil zeggen dat elk ideaal voortgebracht wordt door één element.

Een hoofdideaalring zonder nuldelers noemen we een hoofdideaaldomein (Eng. principal ideal domain, PID).

In Voorbeeld 2.7.9 hebben we gezien dat $\mathbb{Z}$ een hoofdideaaldomein is. Vooraleer andere voorbeelden te bekijken voeren wij het begrip deelbaarheid in voor een willekeurig domein.

Definitie 2.12.2. Zij $a, b \in R$. Wij definiëren

$$a|b \text{ (lees, } a \text{ deelt } b) \quad \text{als en slechts als} \quad b = ac \text{ voor een } c \in R.$$

Uiteraard geldt dan ook

$$a|b \quad \text{als en slechts als } b \in (a).$$

Definitie 2.12.3. Een element $d \in R$ is een *grootste gemene deler* van a en b (wij noteren dit $d = \text{ggd}(a, b)$) als aan de volgende voorwaarden voldaan is:

1. $d|a$ en $d|b$,
2. voor $e \in R$, als $e|a$ en $e|b$ dan $e|d$.

Als c en d twee grootste gemene delers zijn van a en b, dan volgt uit voorwaarden (1) en (2) dat $c|d$ en $d|c$. Omdat R een domein is, volgt hieruit dat $c = ud$, met $u \in R$ inverteerbaar. Dus, grootste gemene delers zijn uniek op een eenheid na.

We tonen nu aan dat de *formule van Bézout* geldt in elk hoofdideaaldomein.

Stelling 2.12.4. *Zij R een hoofdideaaldomein. Als a en b niet-nul elementen zijn van R en $d = \text{ggd}(a, b)$ (een grootste gemene deler), dan $(a, b) = (d)$.*

BÉZOUT (1730-1783)

Bewijs. We weten dat (a, b) een hoofdideaal is, m.a.w. $(a, b) = (c)$, voor een $c \in R$. We zullen bewijzen dat c een grootste gemene deler van a en b is. Omdat $a, b \in (c)$ is het duidelijk dat $c|a$ en $c|b$. Als $e|a$ en $e|b$, dan zijn $a, b \in (e)$, en $(c) = (a, b) \subseteq (e)$. Hieruit volgt dat $c \in (e)$, en $e|c$.

Uit de bovenstaande opmerking volgt nu dat $d = uc$, met $u \in U(R)$. Maar dan is $(d) = (c) = (a, b)$. □

Gevolg 2.12.5. *Stel $d = \text{ggd}(a, b)$. Dan bestaan er elementen $x, y \in R$ zodat $ax + by = \text{ggd}(a, b)$.*

In een domein is niet elk (niet-nul) priemideaal een maximaal ideaal. Doch in hoofdideaaldomeinen is dit wel zo.

Stelling 2.12.6. *Onderstel dat R een hoofdideaaldomein is. Dan is elk van (0) verschillend priemideaal P maximaal.*

Bewijs. Veronderstel dat M een echt ideaal is dat P bevat. Omdat R een hoofdideaalring is, bestaan er $p \in P$ en $m \in M$ zodat

$$P = (p) \subseteq M = (m).$$

Dus is $p = am \in P$, met $a \in R$. Omdat P een priemideaal is volgt er dat $a \in P$ of $m \in P$. Als $m \in P$, dan is $M = (m) \subset P$, dus is $P = M$. Stel daarom $a \in P$. Dan is $a = xp$ voor een zekere $x \in R$. Bijgevolg is $p = am = xmp$. Omdat R is een domein is, volgt dat m inverteerbaar is. Maar dan is $M = R$. We besluiten dus dat $P = M$ of $M = R$, dus. het ideaal P is maximaal. □

Wij bekijken nu een speciale klasse van hoofdideaaldomeinen.

Definitie 2.12.7. We noemen een domein R Euclidisch als er een afbeelding $g : R \setminus \{0\} \to \mathbb{N}$ bestaat die voldoet aan de volgende voorwaarden:

1. voor niet-nul elementen $a, b \in R$ geldt dat $g(ab) \geq g(a)$,
2. voor alle $a, b \in R$ met $a \neq 0$ bestaan er $q, r \in R$ zodat $b = qa + r$ met $g(r) < g(a)$ of $r = 0$. Men noemt r de rest bij deling van b door a.

De afbeelding g wordt ook wel *Euclidische norm* genoemd.

Voorbeelden 2.12.8. (1) Stel $R = \mathbb{Z}$ en $g(m) = |m|$. De tweede voorwaarde uit de definitie is het gewone delingsalgoritme.

(2) Neem een veld k, en stel $R = k[X]$, en $g(P) = \mathrm{gr}(P)$. Nu is de tweede voorwaarde niets anders dan de quotiëntstelling voor veeltermen.

(3) De verzameling $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ is een deelring van $\mathbb{C}$. Men noemt dit de *ring der gehelen van Gauß*. Deze ring is een Euclidisch domein, en $g(a+bi) = |a+bi| = a^2+b^2$.

Stelling 2.12.9. *Elk Euclidisch domein R is een hoofdideaaldomein.*

Bewijs. Neem een willekeurig niet-nul ideaal $I \subset R$, en neem $x \in I \setminus \{0\}$ zodat $g(x)$ minimaal is. Neem $y \in I$. Uit de definitie weten we dat er $q, r \in R$ bestaan zodat $y = qx + r$, met $r = 0$ of $g(r) < g(x)$. Als $r \neq 0$, dan is $r = y - qx \in I$, en $g(r) < g(x)$ wat strijdig is met de minimaliteit van $g(x)$. Dus is $r = 0$, en $y = qx$. Elk element van I is dus een veelvoud van x, en $I = (x)$. □

Men kan bewijzen dat $R = \{a + b\frac{1+\sqrt{19}i}{2} \mid a, b \in \mathbb{Z}\}$ een hoofdideaaldomein is, maar geen Euclidisch domein.

Gevolg 2.12.10. *$\mathbb{Z}$, $k[X]$ en $\mathbb{Z}[i]$ zijn hoofdideaaldomeinen.*

Stelling 2.12.11. *Elke hoofdideaalring R is Noethers.*

Bewijs. Neem een stijgende keten idealen

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

in R. Dan is $I = \cup_i I_i$ een ideaal van R, en dus is $I = (a)$ voor een zekere $a \in R$. Zij n zodat $a \in I_n$. Dan,

$$I = (a) \subseteq I_n \subseteq I_{n+1} \subseteq \cdots \subset I = (a)$$

en bijgevolg is $I_n = I_{n+1} = \cdots$. Wij hebben dus aangetoond dat elke stijgende keten idealen stationair is. □

We keren nu onze aandacht naar de belangrijke bouwelementen van de rekenkunde. De inverteerbare elementen zijn "te goed", dus spenderen wij daar geen of weinig aandacht aan.

Definitie 2.12.12. Een niet-inverteerbaar element a in een domein R wordt irreducibel genoemd als en slechts als aan de volgende eigenschap voldaan is:

$$\text{als } a = bc, \text{ met } b, c \in R \text{ dan } b \in U(R) \text{ of } c \in U(R).$$

Het is duidelijk dat de irreducibele elementen van $\mathbb{Z}$ juist de priemgetallen zijn. Meer algemeen hebben we

Stelling 2.12.13. *Onderstel dat R een domein is. Als het hoofdideaal (a) een niet-nul priemideaal is, dan is a irreducibel.*

Bewijs. Veronderstel dat $a = bc$. Omdat $bc \in (a)$ moet $b \in (a)$ of $c \in (a)$, want (a) is een priemideaal. Veronderstel bijvoorbeeld dat $b \in (a)$. Dit betekent dat er een $x \in R$ bestaat zodat $b = ax$. Bijgevolg $a = bc = axc$. Omdat R een domein is volgt hieruit dat $xc = 1$, en dus is c inverteerbaar, dus a is irreducibel. □

Als k een veld is dan zijn de inverteerbare elementen van $k[X]$ de niet-nul constante polynomen. Dus zijn de irreducibele elementen de niet-constante polynomen die niet

kunnen gefactoriseerd worden in een product waarvan elke factor een niet constante polynoom is.

Wij kunnen evenwel meer zeggen voor elk hoofdideaaldomein.

Gevolg 2.12.14. *Zij R een hoofdideaaldomein en $0 \neq a \in R$. De volgende voorwaarden zijn equivalent:*

1. *(a) is een priemideaal,*
2. *a is irreducibel,*
3. *(a) is een maximaal ideaal.*

Bewijs. Wegens Stelling 2.12.13, (1) $\Rightarrow$ (2). Wegens Stelling 2.12.6 zijn (1) en (3) equivalent. Wij bewijzen nu (2) $\Rightarrow$ (3). Veronderstel dus dat a irreducibel is. Omdat a niet inverteerbaar is, is (a) een echt ideaal. Om aan te tonen dat het een maximaal ideaal is, veronderstal dat $(a) \subseteq (b) \subset R$. Dan $a = bx$ voor een $x \in R$. Omdat a irreducibel is moet b of x een inverteerbaar element zijn. Het eerste is onmogelijk omdat $(b) \neq R$. Dus is x een eenheid. Bijgevolg $b = ax^{-1} \in (a)$, en dus $(a) = (b)$, zoals gewenst. □

2.13 Uniekefactorisatiedomeinen

De hoofdstelling van de rekenkunde garandeert dat elk geheel getal op een unieke wijze, op de volgorde van de factoren na, en op eventuele mintekens van de factoren na, geschreven kan worden als het product van priemgetallen, eventueel met mintekens. Deze eigenschap maakt dat $\mathbb{Z}$ een zogenaamd uniekefactorisatiedomein[5] is. De equivalentie van (1) en (2) in Gevolg 2.12.14 blijft gelden voor de deze rijkere klasse van ringen, zoals zal blijken uit de uit Stelling 2.13.4.

[5]Een domein waar unieke factorisatie geldt, wordt in het Nederlands wel degelijk tot één woord samengevoegd. Vergelijk met "langeafstandsloper", "geroosterdecourgettetapenade" en "Turksepizzabakker". Aan de hand van dit laatste voorbeeld kan men ook het verschil inzien tussen een Turkse pizzabakker en een Turksepizzabakker.

Definitie 2.13.1. Een domein R noemen we een uniekefactorisatiedomein (Eng. unique factorization domain, UFD) als aan de volgende voorwaarden voldaan is:

1. als $0 \neq x \in R$ en als x geen inverteerbaar element is, dan is x een product van irreducibele elementen,
2. als $p_1 \cdots p_n = q_1 q_2 \cdots q_m$, met elke p_i en q_i een irreducibel element, dan $n = m$ en $q_i = u_i p_{\sigma(i)}$, waarbij u_i inverteerbaar is, en σ een permutatie is van $\{1, 2, \ldots, n\}$.

Het eerste gedeelte van het bewijs van de volgende stelling toont aan dat in een Noethers domein elk niet nul element ofwel inverteerbaar is ofwel een product is van irreducibele elementen. In het algemeen is zo een product echter niet uniek (in de zin van de vorige definitie).

Stelling 2.13.2. *Elk hoofdideaaldomein is een uniekefactorisatiedomein.*

Bewijs. Zij S de verzameling van alle hoofdidealen voorgebracht door de niet-nul elementen a van R die niet inverteerbaar zijn en die ook niet kunnen geschreven worden als een product van irreducibele elementen. Onderstel dat S niet leeg is. Wegens Stelling 2.12.11 is R Noethers. Bijgevolg voldoet de verzameling S aan de maximaalvoorwaarde. Zij $a \in R$ zodat (a) een maximaal is onder de idealen $(s) \in S$. Het element a is uiteraard reducibel, dus $a = bc$, b en c niet inverteerbare elementen van R. Maar dan zijn (b) en (c) echte idealen die (a) strikt bevatten. Uit de maximaliteit van (a) (voor $a \in S$) leiden we af dat $b, c \notin S$. Dus zijn b en c te ontbinden tot een produkt van irreducibele elementen, en a fortiori geldt hetzelfde voor $a = bc$. Dus $a \notin S$, een contradictie. We concluderen dat $S = \emptyset$. M.a.w., elk niet-nul element en niet-inverteerbaar element van R is te ontbinden in irreducibele elementen. Dit bewijst de existentie van de ontbinding.

We kunnen nu de uniciteit van de ontbinding in irreducibele factoren bewijzen. Wij gebruiken hiervoor dat elk irreducibel element een priemideaal voortbrengt (Gevolg 2.12.14). Onderstel dat

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

met p_i, q_i irreducibel. Hieruit volgt dat $p_1 | q_1 q_2 \cdots q_m$. Omdat (p_1) een priemideaal is volgt dat $p_1 | q_i$ voor een zekere q_i. Dus $q_i = u_i p_1$ voor een $u_i \in R$. Omdat q_i irreducibel is, volgt dat u_i inverteerbaar is. Herhaaldelijk toepassen van deze redenering geeft ons de uniciteit van de ontbinding. □

Men kan aantonen dat het domein $\mathbb{Z}[\sqrt{10}]$ een Noethers domein is. Dus wegens de opmerking voor Stelling 2.13.2 is elk niet-nul element dat niet inverteerbaar is een

product van irreducibele elementen. Doch deze ontbinding is hier in het algemeen niet uniek. Dit is bijvoorbeeld het geval voor het element $9 = 3 \cdot 3 = (\sqrt{10}+1)(\sqrt{10}-1)$.

Als R een uniekefactorisatiedomein is, dan is ook de veeltermring $R[X]$ een uniekefactorisatiedomein De rest van deze paragraaf wijden we aan het bewijs van deze stelling. Daarvoor hebben we een aantal hulpstellingen nodig. Na een voorbeeld beginnen we met een soort omgekeerde van Stelling 2.12.13.

Voorbeeld 2.13.3. $k[X,Y]$ en $\mathbb{Z}[X]$ zijn uniekefactorisatiedomeinen, maar geen hoofdideaalringen, en dus ook geen Euclidische ringen. Immers, de idealen $(X,Y) \subset k[X,Y]$ en $(p,X) \subset \mathbb{Z}[X]$ zijn geen hoofdidealen.

Stelling 2.13.4. *Onderstel dat R een domein is waarin elk niet nul element dat niet inverteerbaar is kan geschreven worden als een product van irreducibele elementen. Dan is R een uniekefactorisatiedomein als en alleen als elk ideaal voortgebracht door een irreducibel element een priemideaal is.*

Bewijs. Zij R een UFD en $a \in R$ irreducibel. Wij tonen aan dat (a) een priemideaal is. Veronderstel daarom dat $bc \in (a)$. Dan bestaat er een $x \in R$ zodat $bc = xa$. Schrijf nu de irreducibele ontbinding uit van b en c. Uit de uniciteit van de ontbinding van $bc = xa$, en uit het feit dat a irreducibel is, volgt dat a een irreducibele factor is van b of c, met andere woorden $b \in (a)$ of $c \in (a)$. Dit bewijst dat (a) inderdaad een priemideaal is.

Omgekeerd, onderstel dat elk ideaal voortgebracht door een irreducibel element een priemideaal is. Elke $x \in R \setminus U(R)$ heeft een factorisatie in irreducibele elementen, en we hoeven dus enkel te bewijzen dat die factorisatie uniek is. Onderstel dat

$$a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m, \tag{2.4}$$

met elke a_i, b_j irreducibel. Dan is

$$b_1 b_2 \cdots b_m \in (a_n),$$

en dus moet minstens één der $b_i \in (a_n)$, want (a_n) is bij onderstelling een priemideaal. Dus $b_i = w a_n$ voor een $w \in R$. Omdat b_i irreducibel is, en a_n niet inverteerbaar, is noodzakelijk w inverteerbaar. We "delen" nu (2.4) door b_i, en vinden

$$w^{-1} a_1 a_2 \cdots a_{n-1} = b_1 b_2 \cdots \hat{b}_i \cdots b_m$$

Als we deze redenering herhalen, dan vinden we $n = m$ en de uniciteit van de ontbinding. □

Definitie 2.13.5. Neem een uniekefactorisatiedomein R met breuken-veld K. Een veelterm

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in R[X]$$

noemt men een primitieve veelterm als elke deler in R van $P(X)$ een inverteerbaar element is, of m.a.w. als elke gemene deler in R van de coëfficiënten $a_0, a_1, \ldots, a_n$ inverteerbaar is.

Lemma 2.13.6. *We gebruiken dezelfde notaties als in Definitie 2.13.5. Zij P een veelterm in $K[X]$. Dan,*

1. *bestaan $c \in K$ en $P_0 \in R[X]$ primitief zodat $P(X) = cP_0(X)$;*
2. *bovendien zijn c en P_0 uniek op eenheid na, d.w.z., als*

   $$P = cP_0 = c'P_0'$$

   met $P_0, P_0' \in R[X]$ primitief, en $c, c' \in K$, dan bestaat er een inverteerbaar element $u \in R$ zodat $c = uc'$ en $P_0' = uP_0$;
3. *$P \in R[X]$ als en alleen als $c \in R$ en c is een grootste gemene deler van $a_0, a_1, \ldots, a_n$.*

Bewijs. (1) Omdat K het breukenveld is van R, bestaat een $0 \neq d \in R$ zodat $dP = P_1 \in R[X]$. Neem nu voor e een grootste gemene deler van de coëffiënten van P_1 (dit bestaat omdat R een UFD is). Dan is $dP = P_1 = eP_0$ met P_0 primitief, en

$$P = \frac{e}{d} P_0 = cP_0.$$

(2) Stel $c = \frac{e}{d}$ en schrijf $c' = \frac{e'}{d'}$, met $e', d' \in R$ en $0 \neq d'$. Uit $cP_0 = c'P_0'$ volgt dat

$$d'eP_0 = de'P_0'.$$

Schrijf

$$P_0(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

en

$$P_0'(X) = a_n' X^n + a_{n-1}' X^{n-1} + \cdots + a_0',$$

met alle $a_i, a_i' \in R$. Dan geldt voor elke index i dat $d'ea_i = de'a_i'$. Nu is $d'e$ een grootste gemene deler van $\{d'ea_0, d'ea_1, \ldots, d'ea_n\}$ en de' een grootste gemene deler van

$\{de'a'_0, de'a'_1, \ldots, de'a'_n\}$. Omdat deze twee verzamelingen aan elkaar gelijk zijn volgt hieruit dat $e'd = ud'e$, met u een inverteerbaar element van R, en

$$c = \frac{d}{e} = u\frac{d'}{e'} = uc'.$$

(3) Als $P \in R[X]$, dan kunnen wij in (1) d gelijk aan 1 nemen, en dus is $e = c \in R$ is een grootste gemene deler van $\{a_0, a_1, \ldots, a_n\}$. De omgekeerde bewering is triviaal. □

Stelling 2.13.7. (Lemma van Gauß) *Zij R een uniekefactorisatiedomein. Als $P, Q \in R[X]$ primitief zijn, dan is ook $F = PQ$ primitief.*

Bewijs. Onderstel dat $c \in R$, irreducibel en niet inverteerbaar, alle coëfficiënten van $F = PQ$ deelt, en bekijk het natuurlijk epimorfisme

$$\pi : \ R[X] \to (R/(c))[X] : P \mapsto \overline{P}.$$

Omdat c irreducibel is, is (c) een priemideaal (Stelling 2.13.4), en dus zijn $R/(c)$ en $(R/(c))[X]$ domeinen. Omdat P en Q primitief zijn, zijn $\overline{P}$ en $\overline{Q}$ verschillend van 0 in $(R/(c))[X]$ (anders is c een gemene deler van elk van de coëfficiënten). Maar $\overline{F} = \overline{PQ} = \overline{P}\,\overline{Q} = 0$, en dit is strijdig met het feit dat $(R/(c))[X]$ een domein is. □

Stelling 2.13.8. *Zij R een uniekefactorisatiedomein.*

1. *Zij $P, Q \in R[X]$ en onderstel dat P primitief is. Als $Q = FP$ voor een $F \in K[X]$, dan is $F \in R[X]$. M.a.w., als P een primitieve deler is van Q in $K[X]$, dan ook in $R[X]$.*
2. *Zij $P, Q \in K[X]$. Als $P \mid Q$ in $K[X]$, dan is $P_0 \mid Q_0$ in $R[X]$ (waarbij P_0 en Q_0 zijn zoals in Lemma 2.13.6).*
3. *Zij $P, Q \in R[X]$. Als P en Q een gemene niet-constante deler in $K[X]$ hebben, dan ook in $R[X]$.*
4. *Als $P \in R[X]$ niet constant en irreducibel is in $R[X]$, dan ook in $K[X]$.*

Bewijs. (1) Schrijf $F = cF_0$, met F_0 primitief en $c \in K$ (zoals in Lemma 2.13.6). Dan is $Q = cF_0P$, en uit Stelling 2.13.7 volgt dat F_0P primitief is. Omdat $Q \in R[X]$ volgt uit deel (3) van Lemma 2.13.6 dat $c \in R$, en dus is $F = cF_0 \in R[X]$.

(2) Schrijf $P = cP_0$, $Q = dQ_0$ en $Q = FP$ met $F \in K[X]$. Dan is

$$Q_0 = \frac{c}{d} F P_0.$$

Bijgevolg is P_0 is een deler van Q_0 in $K[X]$, en ook in $R[X]$, vanwege deel 1).

(3) Als $F \in K[X]$ een gemene deler is van P en Q, dan is ook $F_0 \in R[X]$ een gemene deler van P en Q in $K[X]$. Uit deel 1) volgt dat F_0 de veeltermen P en Q deelt in $R[X]$.

(4) Schrijf $P = cP_0$. Omdat P irreducibel is, is c of P_0 inverteerbaar. Het laatste is onmogelijk, want P (en P_0) is niet constant. Dus is c inverteerbaar, en P is primitief. Onderstel dat $P = FQ$ in $K[X]$. Dan $F|P$ in $K[X]$, dus, door 2), $F_0|P$ in $R[X]$. Omdat P irreducibel is, zijn er twee mogelijkheden: ofwel is F_0 constant, en dan is ook F constant, ofwel is $P = kF_0$, met $k \in R$ inverteerbaar. In dit laatste geval is $kF_0 = FQ$, en dan is Q een constante. Dit bewijst dat P irreducibel is in $K[X]$. □

Stelling 2.13.9. *Zij R een uniekefactorisatiedomein. Een veelterm $P \in R[X]$ is irreducibel als en alleen als een van de volgende twee voorwaarden geldt:*
a) P is een constante veelterm, en is irreducibel als element van R;
b) P is primitief en irreducibel in $K[X]$.

Bewijs. Onderstel eerst dat $P \in R[X]$ irreducibel is. Schrijf $P = cP_0$, met P_0 primitief en $c \in R$. Omdat P irreducibel is, is ofwel c ofwel P_0 inverteerbaar.

Als P_0 inverteerbaar is, dan is P_0 een constante veelterm, en dan is $P = cP_0$ ook een constante veelterm, m.a.w. $P \in R$. Uiteraard is P ook irreducibel in R.

Als c inverteerbaar is (en dus P_0 geen constante), dan is P primitief in $R[X]$. Uit deel 4) van vorige stelling volgt dat P ook irreducibel is in $K[X]$.

De omgekeerde eigenschap is triviaal. □

Stelling 2.13.10. *Onderstel dat R een uniekefactorisatiedomein is. Als $F \in R[X]$ irreducibel is, dan is (F) een priemideaal.*

Bewijs. Veronderstel dat $F \in R[X]$ irreducibel is. Onderstel dat $PQ \in (F)$, met $P, Q \in R[X]$. We zullen aantonen dat $P \in (F)$ of $Q \in (F)$. Rekening houdend met Stelling 2.13.9 zijn er twee gevallen.

Wij beschouwen eerst het geval dat $F = f \in R$ is irreducibel. Schrijf $P = cP_0$ en $Q = dQ_0$, met $c, d \in R$ en P_0 en Q_0 primitieve veeltermen in $R[X]$. Dan is ook P_0Q_0

primitief, en er is dus een coëfficiënt van P_0Q_0 die niet deelbaar is door f. We noemen deze coëfficiënt a. Omdat f wel een deler is van PQ ($PQ \in (f)$), is f een deler van cda. Bijgevolg is

$$f \mid c \quad \text{of} \quad f \mid d.$$

Dus

$$f \mid P = cP_0 \quad \text{of} \quad f \mid Q = dQ_0$$

en bijgevolg

$$P \in (f) \quad \text{of} \quad Q \in (f).$$

Wij behandelen nu het tweede geval. Zij dus F primitief en irreducibel in $K[X]$. Nu is $K[X]$ een Euclidisch domein (Voorbeeld 2.12.8) en dus een hoofdideaaldomein (Stelling 2.12.9 en Gevolg 2.12.14). Bijgevolg is (F) een priemideaal in $K[X]$. Dus is

$$F \mid P \quad \text{of} \quad F \mid Q$$

in $K[X]$, en vanwege deel 1) van Stelling 2.13.8 ook in $R[X]$. □

Stelling 2.13.11. *Als R een uniekefactorisatiedomein is, dan is ook de veeltermring $R[X]$ een uniekefactorisatiedomein. Bijgevolg is de veeltermring $K[X_1, X_2, \ldots, X_n]$ een uniekefactorisatiedomein voor elk veld K.*

Bewijs. Onderstel dat R een uniekefactorisatiedomein is, en $0 \neq P \in R[X]$. Veronderstel ook dat P geen inverteerbaar element is. Schrijf $P = cP_0$, met P_0 primitief. Omdat R een uniekefactorisatiedomein is, kan c geschreven worden als een product van irreducibele elementen, ofwel is c inverteerbaar.

Wij tonen nu aan dat elke primitieve veelterm P_0 kan ontbonden worden tot een product van irreducibele elementen. Dit kan gemakkelijk gedaan worden per inductie op de graad van P_0. Voor $\mathrm{gr}(P_0) = 1$ is de eigenschap evident: elke primitieve veelterm van graad 1 is irreducibel. Onderstel nu dat elke primitieve veelterm van graad strikt kleiner dan n kan ontbonden worden, en neem een primitieve veelterm P_0 van graad n. Er zijn twee mogelijkheden. Ofwel bestaan er geen veeltermen van graad kleiner dan n die P_0 delen. Dan is P_0 irreducibel, en is dus een product van irreducibelen. Ofwel is P_0 het product van twee veeltermen van een lagere graad. Door de inductiehypothese kunnen deze geschreven worden als een product van irreducibele veeltermen, en hetzelfde geldt dus ook voor P_0.

Er volgt dat P ofwel een eenheid is ofwel een product is van irreducibele elementen.

De uniciteit van de factorisatie volgt nu uit de Stellingen 2.13.4 en 2.13.10. □

Hoofdstuk

3 Modulen

3.1 Inleiding

Het concept moduul is een veralgemening van vectorruimte. De *scalairen* behoren nu tot een ring. Men zou kunnen zeggen dat een moduul is "zoals" een vectorruimte: het is een additieve abelse groep en er is een product van elementen van een ring met de moduulelementen. Deze vermenigvuldiging is distributief en gemengd associatief.

Modulen zijn zeer nauw verbonden met representatietheorie van groepen en zijn van groot belang in andere takken van de wiskunde (zoals o.a. homologische algebra, algebraïsche meetkunde en algebraïsche topologie).

Modulen zijn echter veel ingewikkelder dan vectorruimten. Bijvoorbeeld, niet elk moduul heeft een basis, en als zij dit wel hebben dan is het aantal elementen in een basis niet noodzakelijk invariant. Als de scalairen tot een ring behoren met "goede eigenschappen" (bijvoorbeeld een hoofideaaldomein) dan gelden die eigenschappen soms wel.

3.2 Modulen en deelmodulen

Definitie 3.2.1. Zij R een ring. Een (links) *R-moduul* is een abelse groep $M, +$ met een afbeelding

$$R \times M \to M : \ (r, x) \mapsto rx$$

waarvoor

$$\begin{aligned} 1x &= x, \qquad (rs)x = r(sx) \\ (r+s)x &= rx + sx \\ r(x+y) &= rx + ry \end{aligned}$$

voor alle $x, y \in M$ en $r, s \in R$.

Stel dat M een links R-moduul is. Toon aan als oefening dat voor alle $x \in M$ geldt dat $0x = 0$, dat voor alle $a \in R$ geldt $a0 = 0$, en dat $a(-x) = -ax$ en $(-a)x = -ax$.

Voorbeelden 3.2.2.
(1) Als k een veld is, dan is een k-moduul hetzelfde als een k-vectorruimte.

Een belangrijke klasse van ringen zijn de algebra's A over een veld k. D.w.z. A is een ring die ook een (linkse) vectorruimte is over k zodat bovendien

$$(\alpha a)b = \alpha(ab) = a(\alpha b),$$

voor alle $\alpha \in k$ en $a, b \in A$. Voorbeelden zijn matrixringen $M_{nn}(k)$ (of meer algemeen $\mathrm{End}_k(V)$, de ruimte van de k-lineaire functies op een vectorruimte V) en polynoomringen $k[X]$ over een veld k.

(2) Zij M een abelse groep (additief genoteerd). Dan is M is een $\mathbb{Z}$-moduul voor de bewerking

$$mx = \sum_{i=1}^{m} x \quad ; \quad (-m)x = -(mx) \quad ; \quad 0x = 0,$$

voor elke $x \in M$ en $m \in \mathbb{N}$. Omgekeerd is elk $\mathbb{Z}$-moduul automatisch ook een abelse groep. Een abelse groep is dus net hetzelfde als een $\mathbb{Z}$-moduul.

(3) Een ring R is een (links) R-moduul voor de natuurlijke bewerking

$$R \times R \to R : (r, m) \mapsto rm.$$

Dit moduul noemt men het *regulier* links R-moduul. Later noemen wij dit moduul ook het vrij links R-moduul van rang 1.

Wij veralgemenen nu deze definitie als volgt. Voor een geheel getal $n \geq 1$, zij

$$R^n = \{(r_1, r_2, \cdots, r_n) \mid r_1, \cdots, r_n \in R\}.$$

Dan is R^n een links R-moduul voor de volgende bewerkingen:

$$(r_1, \cdots, r_n) + (r'_1, \cdots, r'_n) = (r_1 + r'_1, \cdots, r_n + r'_n),$$

$$r(r_1, \cdots, r_n) = (rr_1, \cdots, rr_n),$$

voor $r, r_i, r'_i \in R$, $1 \leq i \leq n$. Later noemen wij dit het vrije links R-moduul van rang n.

(4) Zij K een veld en V een K-vectorruimte. Zij verder g een K-linaire transformatie van V. Voor elke polynoom $f \in K[X]$ definiëren wij een K-lineaire transformatie $f(g)$ als volgt: als

$$f = k_n x^n + k_{n-1} x^{n-1} + \cdots + k_1 x + k_0,$$

met alle $k_i \in K$, dan definiëren wij

$$f(g) = k_n g^n + k_{n-1} g^{n-1} + \cdots + k_1 g + k_0 1_V \,.$$

Door de volgende bewerking

$$K[X] \times V \to V : (f(x), v) \mapsto f(g)(v)$$

wordt V een links $K[X]$-moduul.

(5) Zij A een commutatieve groep, dan is A een links $\mathrm{End}(A)$-moduul voor de bewerking

$$\mathrm{End}(A) \times A \to A : (f, a) \mapsto f(a) \,.$$

Definitie 3.2.3. Stel dat M een links R-moduul is, en $N \leqslant M$. Als N een links R-moduul is voor dezelfde vermenigvuldiging van elementen van M met elementen van R, dan is N een *deelmoduul* van M.

De deelmodulen van het regulier R-moduul R, zijn de linkse idealen van R.

Lemma 3.2.4. *Een niet-lege deelverzameling N van een links R-moduul M is een deelmoduul als en slechts als $r_1 n_1 + r_2 n_2 \in N$ voor alle $n_1, n_2 \in N$ en $r_1, r_2 \in R$.*

Bewijs. Bewijs dit als oefening. □

Gevolg 3.2.5. *Als N en N' deelmodulen zijn van een R-moduul M, dan is ook $N \cap N'$ en $N + N' = \{n + n' \mid n \in N,\ n' \in N'\}$ een deelmoduul van M.*

Als $N \cap N' = \{0\}$, dan schrijven we $N \oplus N'$ in plaats van $N + N'$ (dit wordt de *directe som* van N en N' genoemd). In dit geval is elk element van $N \oplus N'$ op een unieke manier te schrijven als de som van één element in N en één in N'.

Een links moduul M over een ring R is niet noodzakelijk een rechts moduul. Wel is het zo dat M een rechts moduul wordt voor de *tegengestelde ring* R^{op} van R (Eng. *opposite ring*). Deze ring is als additieve groep R, maar het product rs in R^{op} is het element sr van R.

3.3 Homomorfismen en quotiëntmodulen

Een aantal begrippen en eigenschappen zijn volledig analoog aan die uit de theorie der vectorruimten over een veld.

Definitie 3.3.1. Zij R een ring en M en N twee R-modulen. Een afbeelding $f : M \to N$ noemen we een *R-lineaire afbeelding* of *R-homomorfisme*, of *R-moduulhomomorfisme*, als

$$f(rx + sy) = rf(x) + sf(y),$$

voor alle $r, s \in R$ en $x, y \in M$. Een homomorfisme dat ook bijectief is noemen we een *isomorfisme* van R-modulen.

Op dezelfde manier voeren we *endo-*, *epi-*, *mono-*, en *automorfismen* van modulen in. Bewijs als oefening het volgende lemma.

Lemma 3.3.2. *Als $f : M \to N$ een homomorfisme is van modulen, dan zijn* $\mathrm{Ker}\,(f) = \{m \in M \mid f(m) = 0\}$ *en* $\mathrm{Im}\,(f) = \{f(m) \mid m \in M\}$ *deelmodulen van respectievelijk M en N.*

Net zoals voor groepen noteren wij met $M \cong N$ dat de twee modulen M en N isomorf zijn. Omdat een moduulhomomorfisme een groephomomorfisme is (tussen abelse groepen) volgt er dat een moduulhomomorfisme $f : M \to N$ injectief (respectievelijk surjectief) is als en slechts als $\mathrm{Ker}\,(f) = \{0\}$ (respectievelijk $\mathrm{Im}\,(f) = N$).

Als M en N R-modulen zijn, dan is

$$\mathrm{Hom}_R(M, N) = \{f : M \to N \mid f \text{ is } R - \text{lineair}\}$$

een additieve groep. Dit is een R-moduul voor de bewerking

$$R \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N) : (r, f) \mapsto rf,$$

met

$$rf : M \to N : m \mapsto rf(m).$$

Wel is, voor een willekeurige ring R,

$$\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$$

een ring (en een deelring van $\mathrm{End}(M)$). De vermenigvuldiging wordt gegeven door de samenstelling. In het vorige hoofdstuk hebben wij hiervan een voorbeeld gezien, namelijk $\mathrm{End}_R(R)$ (waar R het regulier links moduul was).

Als N een deelmoduul is van M, dan kunnen we het quotiënt M/N zoals gebruikelijk definiëren als de verzameling van equivalentieklassen ten opzichte van de equivalentierelatie $\sim$ op M:

$$x \sim y \iff x - y \in N\,.$$

Deze quotiëntstructuur erft de R-moduulstructuur van M door de gebruikelijke definities van de bewerkingen. We noteren een equivalentierelatie met representant x zoals gebruikelijk als $[x]_\sim$.

(i) De optelling op M/N is de groepsbewerking in M/N beschouwd als quotiëntgroep

(ii) De operatie $R \times M/N \to M/N$, $(r, [x]_\sim) \mapsto r[x]_\sim = [rx]_\sim$. Dit is goed gedefinieerd. Immers, $[x]_\sim$ is in een additieve nevenklasse $x + N$ van de deelgroep N van M. Als $y \in x + N$, dan is $y - x \in N$, wegens de moduulstructuur van N is dus $a(y - x) = ay - ax \in N$, dus $[ax]_\sim = [ay]_\sim$.

(iii) Men kan nu eenvoudig nagaan dat M/N met deze bewerkingen een R-moduul is.

Zoals gebruikelijk noteren we $[x]_\sim$ ook als $\overline{x}$. De moduuloperatie op $R \times M/N$ is dus $r\overline{x} = \overline{rx}$.

Definitie 3.3.3. Beschouw een R-moduulhomomorfisme $f : M \to N$. We noemen

$$\mathrm{Coker}\,(f) = N/\mathrm{Im}\,(f)$$

de *cokern* van f.

Stelling 3.3.4. *Beschouw een R-moduul homomorfisme $f : M \to N$. Dan is*

$$M/\mathrm{Ker}\,(f) \cong \mathrm{Im}\,(f)\,.$$

Bewijs. Uit de groepentheorie weten we dat als additieve groepen, $M/\mathrm{Ker}\,(f) \cong \mathrm{Im}\,(f)$. Noem ϕ het canonisch isomorfisme, i.e. $\phi(\overline{m}) = f(m)$. We moeten in feite enkel nog aantonen dat ϕ ook de moduulstructuur bewaart. Beschouw daarom $r\overline{m} + s\overline{n}$, $\overline{m}, \overline{n} \in M/\mathrm{Ker}\,(f)$, $r, s \in R$. Dan geldt

$$\phi(r\overline{m} + s\overline{n}) = \phi(\overline{rm + sn}) = f(rm + sn) = rf(m) + sf(n) = r\phi(\overline{m}) + s\phi(\overline{n})\,,$$

de eerste gelijkheid door de R-moduulstructuur op de quotiëntmodule, de tweede door het canonisch groepisomorfisme, de derde doordat f een groephomomorfisme is, en de laatste opnieuw door het groepisomorfisme. □

3.4 Modulen en groeprepresentaties

Zij G een eindige groep en R een ring. Beschouw de groepring RG, zie Definitie 2.2.5, en beschouw een (links) RG-moduul M. Definieer de afbeelding

$$G \times M \to M : \ (g, m) \mapsto gm = u_g m.$$

Wij verkrijgen aldus een *actie* van de groep G op de verzameling M, immers

$$(gh)m = g(hm) \tag{3.1}$$
$$e_G m = m \tag{3.2}$$

voor alle $g, h \in G$ en $m \in M$. Bewijs als oefening dat de actie van elke g op M R-lineair is:

$$g(m+n) = gm + gn \tag{3.3}$$
$$g(rm) = rg(m) \tag{3.4}$$

voor alle $g \in G \subset RG$[1], $m, n \in M$ en $r \in R \subset RG$.

Lemma 3.4.1. *Als M een links R-moduul is, waarop een G-actie gedefinieerd is die voldoet aan (3.1-3.4), dan is M een links RG-moduul via de formule*

$$\left(\sum_{g \in G} r_g u_g \right) m = \sum_{g \in G} r_g gm.$$

Bewijs. Bewijs als oefening. □

Dus, indien $R = K$ een veld is dan is een KG-moduul een K-vectorruimte waarop een G-actie gedefinieerd is die K-lineair is (en omgekeerd).

Lemma 3.4.2. *Veronderstel dat M en N twee RG-modulen zijn. Een afbeelding $f : M \to N$ is RG-lineair als en slechts als f een R-lineaire afbeelding is die ook voldoet aan $f(gm) = gf(m)$, voor elke $g \in G$ en $m \in M$.*

Bewijs. Bewijs als oefening. □

[1] hier bekijken we de precieze eigenschappen van de vermenigvuldiging van elementen uit het moduul M met elementen uit de ring RG. Zie opnieuw Definitie 2.2.5 en verder, waaruit volgt dat in de groepring RG, de elementen van $R \subset RG$ commuteren met de elementen van $G \subset RG$

Veronderstel nu dat G een eindige groep is en ρ een representatie van G. Dan definieert

$$G \times V \to V : \qquad (g, v) \mapsto g \cdot v := \rho(g)(v) \tag{3.5}$$

een G-actie op de vectorruimte V. Omdat $\rho(g) \in \mathrm{GL}(V)$ is deze actie K-lineair, en voldoet dus aan de voorwaarden van Lemma 3.4.1. Dus V is ook een KG-moduul. We noemen dit KG-moduul $V = M(\rho)$ het *representatiemoduul* behorend bij de representatie ρ. We hebben met een representatie ρ een matrixvoorstelling R geassocieerd, in functie van een basis voor de vectorruimte V (het zogenaamde geassocieerd groephomomorfisme). Als ρ een representatie van graad n is, dan is $R(g)$ een matrix uit $\mathrm{GL}(n, K)$. Aldus is ook K^n een KG-moduul. De actie is dan

$$G \times K^n \to K^n : \qquad (g, v) \mapsto g \cdot v := R(g)v\,, \tag{3.6}$$

en g werkt op een vector v door linkse vermenigvuliding met de matrix $R(g)$.

De volgende stelling toont het omgekeerde aan: elk KG-moduul is het representatiemoduul van een representatie.

Stelling 3.4.3. *Veronderstel K een veld en G een eindige groep. Veronderstel dat M een KG-moduul is, van dimensie n als K-vectorruimte. Dan bestaat er een representatie ρ van G van graad n naar een K-vectorruimte waarvoor $M = M(\rho)$.*

Bewijs. Merk op dat in het KG-moduul M geldt dat

$$g(av + bw) = g(av) + g(bw) = (ga)v + (gb)w = (ag)v + (bg)w = a(gv) + b(gw)\,,$$

voor alle $a, b \in K$, alle $g \in G$, en alle $v, w \in M$, precies omdat in de groepring KG geldt dat $ga = ag$, voor alle $a \in K$ en $g \in G$. Dus voor elke $g \in G$ is de afbeelding $\phi_g : M \to M : \; v \mapsto \phi_g(v) := gv$, K-lineair. Dit definieert een afbeelding $\rho : \; G \to \mathrm{End}_K(M)$[2]: $g \mapsto \phi_g$. Nu geldt voor alle v in het KG-moduul M en voor alle $g \in G$:

$$g^{-1}(gv) = (g^{-1}g)v = v\,,$$

dus $\rho(g^{-1}) = \rho(g)^{-1}$, of nog, $\rho(g) \in \mathrm{GL}(M)$ voor alle $g \in G$. Beschouw nu $g, h \in G$. Omdat in het KG-moduul M geldt dat

$$(gh)v = g(hv)\,,$$

voor alle $v \in M$, is $\rho(gh) = \rho(g) \circ \rho(h)$. Met andere woorden, ρ is een representatie van G, in de K-vectorruimte M, dus van graad n. Het is duidelijk dat $M = M(\rho)$. □

[2]Hier is M een n-dimensionale K-vectorruimte

Representaties van een groep in een K-vectorruime en KG-modulen zijn dus equivalente objecten. De volgende stelling zegt dat isomorfe representaties overeenkomen met isomorfe modulen. Aldus is representatietheorie volledig vertaald in moduultheorie. Dit laatste is de moderne manier om groeprepresentaties te bestuderen.

Stelling 3.4.4. *Veronderstel dat G een eindige groep is. Twee K-representaties ρ en τ van G zijn equivalent als en slechts als $M(\rho) \cong M(\tau)$.*

Bewijs. Beschouw de representaties $\rho : G \to \mathrm{GL}(V_1)$ en $\tau : G \to \mathrm{GL}(V_2)$, V_1 en V_2 beide K-vectorruimten. Veronderstel dat de representaties ρ en τ equivalent zijn. Dit betekent per definitie (Definitie 1.3.3) dat er een vectorruimte-isomorfisme $\psi : V_1 \to V_2$ bestaat zodat $\psi \circ \rho(g) \circ \psi^{-1} = \tau(g)$ voor alle $g \in G$. Beide representaties definiëren acties van G op V_1, respectievelijk V_2 (zie (3.5)): $g \cdot v = \rho(g)(v)$ voor $v \in V_1$ en $g \cdot v = \tau(g)(v)$ voor $v \in V_2$. Door Lemma 3.4.1 zijn V_1 en V_2 ook KG-modulen. omdat ρ en τ equivalente representaties zijn, is de dimensie van V_1 en V_2 als K-vectorruimte uiteraard gelijk, en uiteraard $V_1 = M(\rho)$ en $V_2 = M(\tau)$. We moeten aantonen dat V_1 en V_2 ook als KG-moduul isomorf zijn. Definieer daartoe de afbeelding

$$\phi : V_1 \to V_2 : v \mapsto \phi(v) := \psi(v)$$

Deze afbeelding is K-linear (nu beschouwen we V_1 en V_2 als KG-moduul), omdat ψ K-linear is. Kies $g \in G$ en $v \in V_1$ willekeurig. Dan is

$$\phi(gv) = \phi(\rho(g)(v)) = \psi(\rho(g)(v) = \tau(g)(\psi(v)) = g\psi(v) = g\phi(v)\,.$$

De afbeelding ϕ is dus ook G-linear, en door Lemma 3.4.2 ook KG-lineair, dus een moduulhomomorfisme, en een isomorfisme omdat ψ dat ook is.

Omgekeerd, veronderstel dat $M_1 = M(\rho) \cong M_2 = M(\tau)$. Noem $\phi : M_1 \to M_2$ het moduulisomorfisme. Omdat de afbeelding ϕ KG-lineair is, is ze ook K-lineair en G-linear. De eerste eigenschap maakt dat ϕ ook een vectorruimte-isomorfisme is. De tweede eigenschap geeft precies $\phi(gv) = g\phi(v)$, maar in de vectorruimte M_1 is gv precies de actie $\rho(g)(v)$ van g op v, in de vectorruimte M_2 is $g\phi(v)$ precies de actie $\tau(g)(\phi(v))$ van g op $\phi(v)$. Met andere woorden, de afbeelding ϕ is ook een vectorruimte-isomorfisme zodat $\phi \circ \rho(g) \circ \phi^{-1} = \tau(g)$ voor alle $g \in G$. □

Gevolg 3.4.5. *Een K-invariante deelruimte van een representatie is dus equivalent met een KG-deelmoduul.*

Bewijs. Bewijs als oefening. □

Definitie 3.4.6. Zij R een ring. Men noemt een niet-nul (links) R-moduul M *enkelvoudig* of *irreducibel* indien $\{0\}$ en M de enige deelmodulen van M zijn, met andere woorden als M geen niet-triviale deelmodulen heeft.

Gevolg 3.4.7. *Een K-representatie ρ van een groep G is irreducibel als en slechts het KG-moduul $M(\rho)$ een irreducibel KG-moduul is.*

Definitie 3.4.8. Zij R een willekeurige ring, en M een links R-moduul. Een keten deelmodulen

$$0 \subset M_1 \subset M_2 \subset \ldots \subset M_k = M$$

waarbij alle inclusies echt zijn en waarbij alle M_{i+1}/M_i enkelvoudig zijn noemen we een *compositierij* voor M.

Een enkelvoudig moduul heeft enkel de triviale compositierij $\{0\} \subset M$. Het andere uiterste, namelijk dat er compositierijen bestaan van oneindige lengte, is ook mogelijk. Wel geldt de volgende stelling voor eindige compositierijen.

Stelling 3.4.9. *Zij M een links R-moduul. Als*

$$0 \subset M_1 \subset M_2 \subset \ldots \subset M_k = M$$

en

$$0 \subset N_1 \subset N_2 \subset \ldots \subset N_l = M$$

compositierijen zijn van M, dan is $k = l$, en de enkelvoudige quotiënten zijn uniek op de volgorde na.

Bewijs. Kies de minimale index r waarvoor geldt dat $N_1 \subseteq M_r$, en beschouw het R-moduul $M_{r-1} \cap N_1 \subseteq N_1$. Aangezien N_1 enkelvoudig is, zijn er dus maar twee mogelijkheden, ofwel $M_{r-1} \cap N_1 = N_1$, ofwel $M_{r-1} \cap N_1 = \{0\}$. Het eerste is onmogelijk, omdat dan $N_1 \subseteq M_{r-1}$, en dit is strijdig met de minimaliteit van r. Dus $M_{r-1} \cap N_1 = \{0\}$ en bijgevolg $M_{r-1} + N_1 = M_{r-1} \oplus N_1$. Aangezien

$$M_{r-1} \subseteq M_{r-1} \oplus N_1 \subseteq M_r$$

en $N_1 \neq \{0\}$ vinden we dat $M_{r-1} \oplus N_1 = M_r$. Hieruit volgt dat

$$M_r/M_{r-1} \cong N_1.$$

Bovendien, voor M/N_1 vinden we daarom de volgende twee compositierijen:

$$\{0\} = N_1/N_1 \subset M_1 + N_1/N_1 \subset \cdots M_{r-1} + N_1/N_1 = M_r/N_1$$

$$\subset M_{r+1}/N_1 \subset \cdots M_k/N_1$$

en

$$\{0\} \subset N_2/N_1 \subset N_3/N_1 \subset \ldots \subset N_l/N_1$$

We herhalen deze redenering nu inductief. □

Lemma 3.4.10. *Veronderstel dat G een eindige groep is, en K een veld. Elk KG-moduul dat eindig dimensionaal is als K-vectorruimte, heeft een eindige compositierij.*

Bewijs. Een KG-moduul is het representatiemoduul $M(\rho)$ voor een representatie van de groep G. Als ρ irreducibel is, dan is M irreducibel en dan bestaat alleen de triviale compositierij. Als ρ reducibel is, dan bestaat er een echt deelmoduul $M_1 \subset M$. Het deelmoduul M_1 is opnieuw een representatiemoduul, van een representatie ρ_1. Ook het quotiëntmoduul M/M_1 is een representatiemoduul, van de representatie ρ_2. Mogelijks zijn ρ_1 en/of ρ_2 opnieuw reducibel, en vinden we opnieuw echte deelmodulen in M_1 en/of M/M_1. De dimensie van M_1 en M/M_1 als vectorruimten is kleiner dan de dimensie van M. Men kan dus hoogstens nog een eindig aantal deelmodulen vinden in M_1 en M/M_1. Indien alle deelrepresentaties irreducibel zijn, dan zijn alle quotiëntmodulen M_{i+1}/M_i in de keten irreducibel, dus M heeft een eindige compositierij. Door Stelling 3.4.9 zijn de deelmodulen en deelrepresentaties uniek op volgorde en equivalentie na. □

Stelling 3.4.11. *Elke K-representatie ρ van een eindige groep G heeft een matrixvoorstelling van de volgende vorm:*

$$\begin{pmatrix} R_{11}(g) & R_{12}(g) & \cdots & R_{1k}(g) \\ 0 & R_{22}(g) & \cdots & R_{2k}(g) \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & R_{kk}(g) \end{pmatrix},$$

waarbij de R_{ii} de geassocieerde groephomomorfismen zijn van irreducibele representaties ρ_{ii}. Bovendien zijn deze representaties uniek op volgorde en equivalentie na.

Bewijs. Beschouw de compositierij $M_1 \subset M_2 \subset \ldots \subset M_k = M$, M het representatiemoduul van ρ. Stel $U_1 \subset U_2 \subset \ldots \subset U_k$ is een rij van verzamelingen $U_i \subset M$, zodat elke U_i precies een K-basis is van elk moduul M_i. Stel $U_j = \{u_1, \ldots u_{m_j}\}$, en dus $0 < m_1 < m_2 < \ldots < m_k = n$. De i-de kolom van de matrix $R(g)$ bestaat uit de coördinaten van $\rho(g)u_i$ ten opzichte van de basis U_k. Omdat $\rho(g)u_i \in M_j$ voor $i \leq m_j$, zijn de elementen op de rijen $m_j + 1$ tot en met n gelijk aan nul. Dit toont aan dat ten opzichte van de gekozen basis, de matrixvoorstelling $R(g)$ gelijk is aan

$$\begin{pmatrix} R_{11}(g) & R_{12}(g) & \cdots & R_{1k}(g) \\ 0 & R_{22}(g) & \cdots & R_{2k}(g) \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & R_{kk}(g) \end{pmatrix}, \tag{3.7}$$

Voor elke $g \in G$ is $R_{ii}(g)$, de matrixvoorstelling van $\rho_{ii}(g)$, de irreducibele representatie die correspondeert met het irreducibel KG-moduul M_{i+1}/M_i. □

De matrix (3.7) is bijna een bovendriehoeksmatrix. Als $R_{ij}(g) = 0$ voor $i \neq j$ voor alle $g \in G$ dan zal het KG-moduul een extra eigenschap hebben. We geven eerst de volgende definitie. Vergelijk deze definitie met de uitkomst van Stelling 1.4.7.

Definitie 3.4.12. Een representatie ρ van een groep G noemen we volledig reducibel indien de matrixvoorstelling van $\rho(g)$ na een geschikte basiskeuze onder de vorm

$$\begin{pmatrix} R_{11}(g) & 0 & \cdots & 0 \\ 0 & R_{22}(g) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & R_{kk}(g) \end{pmatrix} \tag{3.8}$$

kunnen gebracht worden, waarbij de R_{ii} de geassocieerde groephomomorfismen zijn van irreduciebele representaties ρ_{ii} van G. Wij schrijven $\rho = \rho_{11} \oplus \cdots \oplus \rho_{kk}$.

Stelling 3.4.13. *Een representatie ρ van G is volledig reducibel als en alleen als het bijhorend representatiemoduul M de directe som is van irreducibele kG-modulen.*

Bewijs. Onderstel eerst dat ρ volledig reducibel is, m.a.w., de matrixvoorstelling voor $\rho(g)$ is van de vorm (3.8) voor elke $g \in G$. Beschouw de bijhorende compositierij

$$0 \subset M_1 \subset M_2 \subset \ldots \subset M_k = M$$

van het representatiemoduul M. Stel $U_1 \subset U_2 \subset \ldots \subset U_k$ is een rij van verzamelingen $U_i \subset M$, zodat elke U_i precies een K-basis is van elk moduul M_i. Stel $U_k = \{u_1, u_2, \ldots, u_n\}$, en we veronderstellen dat de dimensie van M_i gelijk is aan n_i, dan is $U_i = \{u_1, \ldots, u_{n_i}\}$. Definieer nu N_i als de deelruimte van M met basis $\{u_{n_{i-1}+1}, u_{n_{i-1}+2}, \ldots, u_{n_i}\}$. Uiteraard is

$$M = N_1 \oplus N_2 \oplus N_3 \oplus \cdots \oplus N_k$$

als K-vectorruimte. Uit de matrix (3.8) blijkt bovendien dat $gN_i \subseteq N_i$ voor elke $g \in G$ en $i = 1, \ldots, k$. Dit betekent dat elke N_i een KG-moduul is, en dus is M ook de directe som van de N_i als KG-modulen.

Omgekeerd, onderstel dat M de directe som is van irreduciebele KG-deelmodulen $N_1, N_2, \ldots, N_k$. Neem basissen van elk van de N_i, en schrijf deze achter elkaar tot een basis $\{u_1, u_2, \cdots, u_n\}$ van M. Ten opzichte van deze basis is de matrixvoorstelling van $\rho(g)$ van de vorm (3.8), waarbij ρ_{ii} de representatie is met representatiemoduul N_i, zodat ρ_{ii} irreduciebel is. □

Opmerkingen 3.4.14. 1) Uiteraard is het representatiemoduul M steeds de som van ééndimensionale vectorruimten. Deze vectorruimten zijn echter niet noodzakelijk KG-modulen. Het is dus cruciaal in Stelling 3.4.13 dat de directe som een directe som is van KG-modulen (en niet alleen van K-vectorruimten).

2) Niet elke representatie is volledig reduciebel. Als voorbeeld nemen we $G = \mathbb{Z}$, $K = \mathbb{Q}$ en $n = 2$. De afbeelding

$$\rho : \ \mathbb{Z} \to \mathrm{Gl}_2(\mathbb{Q}) : \ n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

is een (reduciebele) representatie, aangezien

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$$

en $\left\{ \begin{pmatrix} k \\ 0 \end{pmatrix} \mid k \in \mathbf{Q} \right\}$ een echt deelmoduul is van $\mathbf{Q}^2$. De representatie is echter niet volledig reducibel, want voor geen enkele $n \neq 0$ bestaat er een reguliere matrix S zodat

$$S^{-1} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} S$$

een diagonaalmatrix is.

3) In sommige omstandigheden heeft men wel dat elke representatie volledig reducibel is. Bijvoorbeeld in de Stelling van Maschke (Stelling 1.4.7) hebben wij aangetoond dat als G een eindige groep is zodat de karakteristiek van K geen deler is van $|G|$ (d.w.z. $0 \neq |G| \in K$) dan is elke representatie van G volledig reduciebel.

Als de karakteristiek van K geen deler is van van $|G|$, dan spreken we van een *gewone* representatie. In het andere geval spreken we van een *modulaire* representatie.

De reguliere K-representatie van een eindige groep heeft als representatiemoduul de volledige groepring KG. Met $Z(KG)$ noteren we het centrum van de groepring, d.i. de verzameling van alle elementen van KG die met alle elementen commuteren ten opzichte van de vermenigvuldiging.

Zoals wij eerder aangetoond hebben is elke irreduciebele $\mathbb{C}$-representatie een directe sommand van de reguliere representatie van G. Deze laatste heeft als representatiemoduul de groepalgebra KG. Bijgevolg bevat deze ring alle informatie over K-representaties van G. De algebraïsche structuur van KG is dus zeer belangrijk. Zo kan men onder andere een K-basis van het centrum beschrijven via de conjugatieklassen van een eindige groep.

Stelling 3.4.15. *Zij G een eindige groep en zij $C_1, \ldots, C_k$ de conjugatieklassen van G. Dan is*

$$\{\hat{c_i} = \sum_{g \in C_i} u_g \mid 1 \leq i \leq k\}$$

een K-basis voor $\mathrm{Z}(KG)$.

Bijgevolg is de dimensie van $Z(\mathbb{C}G)$ gelijk aan het aantal irreduciebele $\mathbb{C}$ representaties van G.

Bewijs. We bewijzen eerst dat $\hat{c_i} \in \mathrm{Z}(KG)$. Omdat $\{u_h \mid h \in G\}$ een K-basis is voor KG volstaat het om aan te tonen dat $\hat{c_i}$ commuteert met elke u_h. Dit kan men eenvoudig narekenen:

$$u_h \hat{c_i} = \sum_{g \in C_i} u_h u_g = \sum_{g \in C_i} u_{hgh^{-1}} u_h = \sum_{x \in C_i} u_x u_h = \hat{c_i} u_h$$

Vervolgens tonen we aan dat $\{\hat{c_1}, \ldots, \hat{c_k}\}$ het centrum van KG voortbrengen. Neem $u = \sum_{g \in G} r_g u_g \in \mathrm{Z}(KG)$. Dus voor elke $h \in G$ hebben we $u = u u_h^{-1} u_h = u_{h^{-1}} u u_h$. Dus

$$\sum_{g \in G} r_g u_g = u_{h^{-1}} (\sum_{g \in G} r_g u_g) u_h = \sum_{g \in G} r_g u_{h^{-1}} u_g u_h = \sum_{g \in G} r_g u_{h^{-1}gh} = \sum_{x \in G} r_{hxh^{-1}} u_x$$

Aangezien $\{u_g | g \in G\}$ een K-basis is voor KG is $r_{hgh^{-1}} = r_g$, dus $r_g = r^i$ constant voor alle $g \in C_i$. Dus kunnen we u schrijven als een lineaire combinatie van de $\hat{c_i}$'s:

$$u = \sum_{i=1}^{k} r^i \hat{c_i}$$

Bewijs zelf dat de $\{\hat{c_i} \mid i = 1, \cdots, t\}$ lineair onafhankelijk zijn. □

Voorbeeld 3.4.16. Als G een abelse groep is, dan zijn alle C_i singletons. In dit geval is $\{u_g \mid g \in G\}$ een basis van $\mathrm{Z}(KG)$, en $\mathrm{Z}(KG) = KG$. Dit is evident, aangezien KG commutatief is.

Men kan aantonen dat $\mathbb{C}G$ een directe som is van matrices

$$M_{n_1}(\mathbb{C}), \cdots, M_{n_k}(\mathbb{C}),$$

waarbij k het aantal irreduciebele niet-isomorfe complexe representaties is van G en $n_1, \ldots, n_k$ de graden zijn van deze representaties.

3.5 Vrije Modulen

Definitie 3.5.1. Zij M een R-moduul, en $X \subseteq M$. Het *moduul voortgebracht door* X is

$$(X) = \bigcap_{X \subseteq N} N,$$

de doorsnede van alle deelmodulen N van M die X bevatten.

Het is duidelijk dat (X) een moduul is dat X bevat en dat $(\emptyset) = \{0\} = (0)$.

Lemma 3.5.2. *Als $X \neq \emptyset$ dan is*

$$(X) = \{\sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N},\ r_i \in R,\ x_i \in X\}.$$

Bewijs. Bewijs als oefening. □

Als M en N R-modulen zijn, dan is $M \times N$ ook een R-moduul via

$$(m, n) + (m', n') = (m + m', n + n') \quad ; \quad r(m, n) = (rm, rn).$$

Als M en N deelmodulen zijn van een gegeven R-moduul, en $M \cap N = \{0\}$, dan is het duidelijk dat $M \oplus N \cong M \times N$.

Definitie 3.5.3. Zij M een links R-moduul. Een verzameling $B \subset M$ is een *basis* als $M = (B)$ en als de elementen van B R-lineair onafhankelijk zijn. Een *vrij moduul* is een moduul waarvoor er een basis $B \subset M$ bestaat. Als B eindig is, dan is M *eindig voortgebracht*.

Uit de definitie volgt dat als B een basis is voor M, elk element op een unieke wijze geschreven kan worden als een R-lineaire combinatie van elementen van B. Een ring R als links R-moduul heeft $\{1_R\}$ als basis.

Opmerking 3.5.4. Een vrij links R-moduul M heeft dus een basis, maar twee basissen voor M hoeven niet noodzakelijk evenveel elementen te bevatten. De rang van M is dus niet uniek. Wel is het zo dat als M een R-basis heeft van kardinaliteit $n \in \mathbb{N} \setminus \{0\}$, dat M isomorf is met het vrij R-moduul R^n.

Een ring R voldoet aan de zogenaamde *invariant basis number* voorwaarde als elk vrij links R-moduul M een unieke rang heeft, dus als elke twee basissen voor M dezelfde kardinaliteit hebben. In dat geval wordt de rang soms de dimensie van M genoemd. Men kan aantonen dat commutatieve ringen en links Noetherse ringen aan de invariant-basis-number-voorwaarde voldoen. We weten al uit de theorie van de vectorruimten dat velden (en uiteraard ook lichamen) aan deze voorwaarde voldoen.

Er bestaan ringen die niet aan de invariant-basis-number-voorwaarde. Voor een dergelijke ring R is het dus mogelijk dat de vrije modulen R^m en R^n, $n \neq m$, isomorf zijn. Een voorbeeld van een dergelijke ring R wordt gegeven door de endomorfismering van een vrij moduul van aftelbare rang over een ring.

Lemma 3.5.5. *Zij M een links R-moduul en $B \subset M$ een basis voor M. Noteer $B = \{x_i\}_{i\in I}$ en stel N is een links R-moduul. Voor elke familie van elementen $\{y_i\}_{i\in I}$, $y_i \in N$ bestaat er een uniek moduulhomomorfisme $f : M \to N$ zodat $f(x_i) = y_i$ voor alle $i \in I$. Als $\{y_i\}_{i\in I}$ een basis is van N, dan is f een moduulisomorfisme*

Bewijs. Stel $x \in M$. Dan bestaat er een unieke familie van elementen $\{a_i\}_{i\in I}$ zodat $x = \sum_{i\in I} a_i x_i$. Definieer

$$f(x) = \sum_{i\in I} a_i y_i \,,$$

dan is f het unieke moduulhomomorfisme dat aan de opgave van het lemma voldoet.

Als $\{y_i\}_{i\in I}$ een basis is voor N, dan bestaat er een uniek moduulhomomorfisme $g : N \to M$ zodat $g(y_i) = x_i$ voor alle $i \in I$, en $f \circ g = g \circ f$. □

Gevolg 3.5.6. *Als twee linkse R-modulen basissen met gelijke kardinaliteit hebben, dan zijn ze isomorf.*

Voorbeeld 3.5.7. In het bijzonder is R^n een R-moduul, en het is eindig voortgebracht door

$$\{(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}.$$

Een n-dimensionale K-vectorruimte is een K-moduul en heeft steeds een basis, en is isomorf met K^n. Het is dus uiteraard ook een vrij K-moduul. Over een (commutatieve) ring R liggen de zaken minder eenvoudig. Stel $R = \mathbb{Z}$, en beschouw R zelf als $\mathbb{Z}$-moduul en beschouw ook $\mathbb{Z}/n\mathbb{Z}$ als $\mathbb{Z}$-moduul. Dit laatste wordt voorgebracht door $\overline{1}$. Duidelijk is $\mathbb{Z}/n\mathbb{Z}$ eindig, en dus niet isomorf met een $\mathbb{Z}$. Het $\mathbb{Z}$-moduul $\mathbb{Z}/n\mathbb{Z}$ is dus eindig voortgebracht maar niet vrij. Men ziet trouwens ook eenvoudig in dat $\{\overline{1}\}$ niet $\mathbb{Z}$-lineair onafhankelijk is.

Overzicht van eigenschappen

Een aantal eigenschappen van eindigdimensionale vectorruimten gelden ook voor eindig voortgebrachte vrije modulen over een *commutatieve* ring. Zonder in details te treden geven we een overzicht. Zij $M \cong R^m$ en $N \cong R^n$ vrije modulen. Neem basissen $E = \{e_1, e_2, \ldots, e_m\}$ en $F = \{f_1, f_2, \ldots, f_n\}$ voor respectievelijk M en N. Zij $f : M \to N$ een homomorfisme van modulen. Schrijf

$$f(e_i) = \sum_{j=1}^{n} a_{ji} f_j,$$

met elke $a_{ji} \in R$. Wij noteren de $n \times m$-matrix $A = (a_{ji})$ als $[f]_{FE}$. Beschouw de coördinaatafbeeldingen

$$[\bullet]_E : M \to R^m \quad : \quad \sum_{i=1}^{m} a_i e_i \mapsto (a_1, a_2, \ldots, a_m)^\tau,$$
$$[\bullet]_F : N \to R^n \quad : \quad \sum_{j=1}^{n} b_j f_j \mapsto (b_1, b_2, \ldots, b_n)^\tau.$$

Dan geldt voor elke $x \in M$ dat

$$[f(x)]_F = A[x]_E = [f]_{FE}\,[x]_E.$$

De afbeelding

$$[\bullet]_{FE} : \mathrm{Hom}_R(M, N) \to \mathrm{M}_{nm}(R) : f \mapsto [f]_{FE}$$

is een isomorfisme van R-modulen. Bovendien is

$$[\bullet]_{EE} : \mathrm{End}_R(M) \to \mathrm{M}_{mm}(R) : f \mapsto [f]_{EE}$$

een isomorfisme van ringen.

Voor $A \in \mathrm{M}_{mm}(R)$ kunnen we de *determinant* definiëren:

$$\det(A) = \sum_{\sigma \in S_m} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{m\sigma(m)},$$

met S_m de symmetrische groep van graad m en $\varepsilon(\sigma)$ is het teken van σ. De regel van Cramer blijft gelden:

$$A\ (\mathrm{adj}\ A) = (\mathrm{adj} A)\ A = \det(A) I_m.$$

Als $\det(A)$ inverteerbaar is in R, dan heeft de matrix A dus een (tweezijdige) inverse in $\mathrm{M}_{mm}(R)$, namelijk

$$A^{-1} = \det(A)^{-1} \mathrm{adj} A. \tag{3.9}$$

De verzameling van de inverteerbare matrices in $\mathrm{M}_{mm}(R)$ is

$$\mathrm{GL}_m(R) = \{A \in \mathrm{M}_{mm}(R) \mid \det(A) \text{ is inverteerbaar in } R\} = U(M_{mm}(R)).$$

Neem nu andere basissen $E' = \{e'_1, e'_2, \ldots, e'_m\}$ en $F = \{f'_1, f'_2, \ldots, f'_n\}$ voor respectievelijk M en N. Dan bestaan er unieke inverteerbare matrices $P \in \mathrm{GL}_m(R)$ en $Q \in \mathrm{GL}_n(R)$ zodat

$$[x]_{E'} = P[x]_E \quad \text{en} \quad [y]_{F'} = Q[y]_F$$

voor alle $x \in M$ en $y \in N$. We verifiëren gemakkelijk dat

$$A' = [f]_{F'E'} = QAP^{-1}$$

Als $A' = QAP^{-1}$, dan zijn A' en A dus de matrices van eenzelfde lineaire afbeelding, maar genomen ten opzichte van verschillende basissen. We bekijken enkele speciale gevallen.

1a) Verwissel in de basis E de vectoren e_i en e_j. De matrix A' is dan juist de matrix A met de i-de en de j-de kolom verwisseld.

1b) Verwissel in de basis F de vectoren f_i en f_j. De matrix A' is dan juist de matrix A met de i-de en de j-de rij verwisseld.

2a) Vervang e_i door $e'_i = e_i + re_k$ $(k \neq i,\ r \in R)$. Dan is

$$f(e'_i) = \sum_{j=1}^{n} a_{ji} f_j + r a_{jk} f_j = \sum_{j=1}^{n} (a_{ji} + r a_{jk}) f_j$$

en we zien dat de matrix A' bekomen wordt door in A de i-de kolom te vervangen door de i-de kolom met daarbij opgeteld r maal de k-de kolom.

2b) Vervang nu f_k door $f'_k = f_k - rf_l$ $(k \neq l)$. Nu is

$$f(e_i) = \sum_{j=1}^{n} a_{ji} f_j = \sum_{j=1, j\neq k}^{n} a_{ji} f_j + a_{ki}(f'_k + rf_l)$$

en we zien dat de matrix A' bekomen wordt door in A de l-de rij te vervangen door de l-de rij met daarbij opgeteld r maal de k-de rij.

3a) Vervang e_i door $e'_i = re_i$, waarbij r inverteerbaar is in R. Dan is

$$f(e'_i) = \sum_{j=1}^{m} r a_{ji} f_j$$

en dus ontstaat A' uit A door de i-de kolom met r te vermenigvuldigen.

3b) Vervang f_k door $r^{-1} f_k = f'_k$, waarbij r omkeerbaar in R. Nu ontstaat A' uit A door de k-de rij met r te vermenigvuldigen.

De operaties beschreven in 1a, 2a en 3a noemt men *elementaire kolomoperaties*. Die in 1b, 2b en 3b noemt men *elementaire rijoperaties*. Als men op een matrix A elementaire rij- en kolomoperaties toepast, dan verkrijgt men een matrix van dezelfde lineaire afbeelding, maar genomen ten opzichte van andere basissen.

3.6 Eindig voortgebrachte modulen

Zoals we reeds opmerkten is een eindig voortgebracht R-moduul M niet altijd vrij. In deze paragraaf zullen we een structuurstelling bewijzen voor eindig voortgebrachte modulen over een Euclidische ring. In het bijzonder zal hieruit een structuurstelling volgen voor eindig voortgebrachte abelse groepen.

Lemma 3.6.1. *Zij R een ring en $\varphi : M \to N$ een R-lineaire afbeelding. Als* $\operatorname{Ker}\varphi$ *en* $\operatorname{Im}\varphi$ *eindig voortgebracht zijn, dan is ook M eindig voortgebracht.*

Bewijs. Kies generatoren $m_1, m_2, \ldots, m_k$ voor $\operatorname{Ker}\varphi$, en $\varphi(v_1)$, $\varphi(v_2)$, $\ldots$, $\varphi(v_l)$ voor $\operatorname{Im}\varphi$. Zij $x \in M$. Dan is

$$\varphi(x) = \sum_{i=1}^{l} r_i \varphi(v_i)$$

waarbij $r_1, \ldots, r_l \in R$. Hieruit volgt dat

$$x - \sum_{i=1}^{l} r_i v_i \in \operatorname{Ker} \varphi.$$

Dus bestaan $s_1, \ldots, s_k \in R$ zodat

$$x = \sum_{i=1}^{l} r_i v_i + \sum_{j=1}^{k} s_j m_j.$$

Wij hebben aangetoond dat M voorgebracht wordt door

$$\{m_1, m_2, \ldots, m_k, v_1, v_2, \ldots, v_k\}.$$

□

Stelling 3.6.2. *(1) Zij R een ring en M een eindig voortgebracht R-moduul. Dan is elk homomorf beeld van M ook eindig voortgebracht.*

(2) Als bovendien R een links Noetherse ring is, dan is ook elk deelmoduul N van M eindig voortgebracht.

Bewijs. De eerste bewering is triviaal. Wij tonen de tweede bewering aan. Veronderstel dus dat R links Noethers is. Zij N een deelmoduul van het eindig voortgebracht R-moduul M. We bewijzen de bewering eerst in het geval waarin $M \cong R^n$ vrij is. We gaan te werk per inductie op n. Als $n = 1$, dan is N een links ideaal van R. Omdat R links Noethers is, volgt er dan uit Stelling 2.9.3 dat N een eindig voortgebracht links ideaal is, en dus een eindig voortgebracht R-moduul. Onderstel dat de bewering waar is voor $n-1$, en bekijk de projectie

$$\pi : \ R^n \to R^{n-1} : \ (a_1, \ldots, a_{n-1}, a_n) \mapsto (a_1, \ldots, a_{n-1}).$$

Zij N een deelmoduul van M, en beschouw de beperking

$$\pi_{|N} : \ N \to R^{n-1}.$$

Dan $\operatorname{Ker}(\pi_{|N}) \subseteq \operatorname{Ker}(\pi) \cong R$ en $\operatorname{Im}(\pi_{|N}) \subseteq R^{n-1}$. Vanwege de inductiehypothese zijn dan $\operatorname{Ker}(\pi_{|N})$ en $\operatorname{Im}(\pi_{|N})$ eindig voortgebracht. Wegens Lemma 3.6.1 volgt dan dat ook N eindig voortgebracht is.

Onderstel nu dat $M = (m_1, m_2, \ldots, m_n)$ een willekeurig eindig voortgebracht R-moduul. Beschouw de lineaire afbeelding

$$\pi : \ R^n \to M : \ (r_1, r_2, \ldots, r_n) \mapsto \sum_{i=1}^{n} r_i m_i$$

Het is duidelijk dat π surjectief is en dat $\pi^{-1}(N)$ een deelmoduul is van R^n. Wegens het vorige gedeelte is $\pi^{-1}(N)$ eindig voortgebracht. Daar $N = \pi(\pi^{-1}(N))$ volgt dat N ook eindig voortgebracht is. □

In het algemeen is een deelmoduul van een eindig voortgebracht moduul zelf niet eindig voortgebracht. Dit is slechts zo als aan de stijgendeketenvoorwaarde voldaan is.

Stelling 3.6.3. *Zij R een ring. De volgende voorwaarden zijn equivalent voor een R-moduul M:*

1. *elk deelmoduul van M is eindig voortgebracht,*
2. *M voldoet aan de stijgende ketenvoorwaarde (of M is een Noethers moduul); d.w.z. er bestaat geen oneindig strikt stijgende keten $M_1 \subset M_2 \subset \ldots$ van deelmodulen van M.*

Bewijs. Bewijs dit als oefening. □

3.7 Modulen over Euclidische domeinen

Wij tonen nu eerst aan dat een grote klasse van modulen over een commutatieve Noetherse ring R kan beschreven worden door een matrix.

Zij M een eindig voortgebracht moduul over R. Dan bestaat er een epimorfisme

$$\pi : \ R^n \to M.$$

Wegens Stelling 3.6.2 is $\mathrm{Ker}\,(\pi)$ een eindig voortgebracht deelmoduul van R^n. Bovendien

$$R^n/\mathrm{Ker}\,(\pi) \cong M.$$

We nemen een basis $\{e_1, e_2, \ldots, e_n\}$ van R^n, en noteren $\pi(e_i) = f_i$. Dan is $\{f_1, f_2, \ldots, f_n\}$ een stel generatoren voor M. Neem een stel generatoren $\{g_1, g_2, \ldots, g_m\}$ voor $\mathrm{Ker}\,(\pi)$, en schrijf

$$g_i = \sum_{j=1}^{n} a_{ji} e_j.$$

Zij $A = (a_{ji})$, een $n \times m$-matrix. Aangezien $\pi(g_i) = a_i = 0$ in M, geldt voor elke $i \in \{1, \ldots, m\}$ dat

$$\sum_{j=1}^{n} a_{ji} f_j = 0 \tag{3.10}$$

in M. Beschouw nu het homomorfisme

$$\chi : R^m \to R^n : (x_1, \cdots, x_m) \mapsto \sum_{i=1}^{m} x_i g_i.$$

Het is duidelijk dat $\mathrm{Im}\,(\chi) = \mathrm{Ker}\,(\pi)$.

Aldus verkrijgen wij een homomorfisme, de samenstelling van g met de inclusie $\mathrm{Ker}\,(\pi) \subseteq R^n$:

$$\chi : R^m \to R^n.$$

Omdat R een commutatieve ring is, kan men nu eenvoudig nagaan dat χ gegeven wordt door linkse vermenigvuldiging met de $n \times m$-matrix A. Er volgt dat

$$M \cong R^n/\mathrm{Ker}\,(\pi) \cong R^n/AR^m = R^n/\mathrm{Im}\,(\chi).$$

Als we op A elementaire rij- of kolomoperaties toepassen, dan is de nieuwe matrix A' de matrix van dezelfde lineaire afbeelding, maar ten opzichte van andere basissen. Daarom is het moduul M dat we verkrijgen met behulp van de matrix A isomorf met hetgeen we verkrijgen met de matrix A'.

Het moduul M is dus bepaald door de matrix A. Wij noemen dit een *presentatiematrix* voor M. De betrekkingen (3.10) noemen we een *volledig stel relaties* van M. Een kolomvector die een lineaire combinatie is van de kolommen van A noemen we een *relatievector* .

Hoe "eenvoudiger" we de presentatiematrix A kunnen kiezen, hoe "eenvoudiger" de beschrijving van het bijhorende R-moduul M. Voor een Euclidische ring hebben we de volgende stelling.

Stelling 3.7.1. *Zij R een Euclidische ring R. Zij M en N vrije modulen en $f : M \to N$ een lineaire afbeelding. Dan bestaan er basissen $E = \{e_1, \ldots, e_m\}$ en $F = \{f_1, \ldots, f_n\}$ van respectievelijk M en N zodat*

$$[f]_{F,E} = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

waarbij D een diagonaalmatrix is (met elementen op de diagonaal verschillend van 0), en waarbij de nullen in de matrix nulmatrices voorstellen van de gepaste dimensie.

Bewijs. Beschouw een Euclidische norm $g : R \setminus \{0\} \to \mathbb{N}$ (zie Definitie 2.12.7). Kies willekeurige basissen van M en N en noem $A \in M_{nm}(R)$ de matrix van f ten opzichte van deze basissen. Als $A = 0$, dan is de stelling bewezen.

Veronderstel dat $A \neq 0$. Het volstaat om aan te tonen dat A in de gewenste vorm kan gebracht worden door elementaire rij- en kolomoperaties toe te passen. Door rijen en kolommen te verwisselen kunnen we ervoor zorgen dat het element a_{11} in de linkerbovenhoek verschillend van nul is. Door vervolgens rijen te verwisselen kunnen we ervoor zorgen dat

$$g(a_{11}) = \min\{g(a_{i1}) \mid i = 1, \ldots, n \text{ met } a_{i1} \neq 0\}. \tag{3.11}$$

Veronderstel nu dat er een $i > 1$ bestaat met $a_{i1} \neq 0$. Als we het delingsalgoritme uitvoeren krijgen we

$$a_{i1} = a_{11}q + r,$$

waarbij $r = 0$ of $g(r) < g(a_{11})$. We trekken nu q maal de eerste rij af van de i-de rij. Op plaats $(i, 1)$ in de nieuwe matrix verschijnt nu r. Als $r = 0$ dan zijn we tevreden. Als $r \neq 0$, dan verwisselen we de eerste en de i-de rij, zodat opnieuw (3.11) geldt, en we herhalen onze redenering. Bij elke stap wordt

$$\sum_{i=1}^{n} g(a_{i1})$$

kleiner. Na een eindig aantal stappen krijgen we daarom een matrix van de vorm

$$\begin{pmatrix} a_{11} & A' \\ 0 & A'' \end{pmatrix}.$$

We herhalen nu de hele redenering, maar met kolomoperaties in plaats van rijoperaties (eventueel moeten wij ook het eerste gedeelte herhalen). Nu krijgen we een matrix van de vorm

$$\begin{pmatrix} a_{11} & 0 \\ 0 & A_1 \end{pmatrix}.$$

Als $A_1 = 0$, dan is de matrix van de gewenste vorm. Anders herhalen we de hele redenering, maar nu voor de matrix A_1. Na een eindig aantal stappen vinden wij een matrix van de gewenste vorm. □

Definitie 3.7.2. Zij R een ring en M een R-moduul. Het moduul wordt *cyclisch* genoemd als er een $m \in M$ bestaat zodat $M = Rm$.

Er volgt dat M cyclisch als en slechts als $M \cong R/L$, met L een links ideaal van R. Indien R een hoofideaalring is (bijvoorbeeld een Euclidisch domein) dan zijn de cyclische modulen, op isomorfisme na, de modulen $R/(a)$ met $a \in R$. In het geval van $R = \mathbb{Z}$ komen cyclische modulen dus overeen met cyclische groepen.

Stelling 3.7.3. *Zij R een Euclidisch domein. Elk eindig voortgebracht R-moduul M is isomorf met een product van de vorm*

$$R/(d_1) \times \ldots R/(d_s) \times R^r$$

en is dus het product van een vrij moduul, en een eindig aantal cyclische modulen.

Bewijs. Als $M = \{0\}$ dan is het resultaat evident. Veronderstel dus dat M niet triviaal is. We hebben reeds aangetoond dat M isomorf is met de cokern van een lineaire afbeelding $\chi : \ R^m \to R^n$. Gebruik makend van Stelling 3.7.1 kunnen we basissen van R^n en R^m vinden zodat de matrix van χ van de vorm is

$$[\chi] = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix},$$

met D een diagonaalmatrix. Rangschik de basisvectoren zodanig dat de eerste s diagonaalelementen $d_1, d_2, \ldots, d_s$ van D niet inverteerbaar zijn, en de volgende l, $d_{s+1}, \ldots, d_{s+l}$ wel. We mogen nog steeds elementaire rij- en kolomoperaties op A toepassen. Als we de i-de rij $(s+1 \leq i \leq s+l)$ delen door d_i, dan wordt de matrix van χ:

$$[\chi] = \begin{pmatrix} D_s & 0 & 0 \\ 0 & I_l & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Zij $\{E_1, E_2, \ldots, E_m\}$ de gevonden basis van R^m en $\{E'_1, \cdots, E'_n\}$ de gevonden basis van R^n. Dan is het R-moduul $[\chi]R^m$ voortgebracht door de elementen

$$d_1E'_1, \ d_2E'_2, \ \ldots, \ d_sE'_s,$$

en

$$E'_{s+1}, \ E'_{s+2}, \ \ldots, \ E'_{s+l}.$$

Bijgevolg

$$\begin{aligned} M &\cong R^n/[\chi]R^m \\ &\cong R^n/(d_1) \times \cdots \times (d_s) \times R^l \times \{0\}^{n-(s+l)} \\ &\cong (R/(d_1) \times R/(d_2) \times \cdots \times R/(d_s)) \times R^{n-(s+l)} \end{aligned}$$

□

Omdat $\mathbb{Z}$ een Euclidisch domein is, en omdat $\mathbb{Z}$-modulen precies de abelse groepen zijn, vinden we nu onmiddellijk de volgende stelling.

Stelling 3.7.4. (Hoofdstelling van abelse groepen)
Elke eindig voortgebrachte abelse groep A is het product van een vrije abelse groep F en een eindig aantal cyclische groepen. Dus

$$A = F \times T,$$

met

$$F = \mathbb{Z} \times \cdots \times \mathbb{Z}$$

(het aantal oneindig cyclische factoren van F noemt men de torsie vrije rang van A) en T een direct product van eindig cyclische groepen (merk op dat T precies bestaat uit de elementen van eindige orde in A). In het bijzonder is elke eindige abelse groep het product van cyclische groepen.

Omdat een Euclidisch domein R ook een UFD is kan men elk element schrijven als het product van machten van irreducibele elementen. Zoals in Voorbeeld 2.10.4 is dan elk cyclisch R-moduul $R/(d)$, met $d \neq 0$, isomorf met een product van de vorm $R/(d) = R/(p_1^{n_1}) \times \cdots \times R/(p_k^{n_k})$, met elke p_i irreducibel en elke $n_i > 0$. Wij verkrijgen aldus

Gevolg 3.7.5. *Een eindig voortgebracht R-moduul over een Euclidisch domein is isomorf met een product van de vorm*

$$R/(p_1^{n_1}) \times \cdots \times R/(p_n^{n_k}) \times R^r,$$

met elke p_i irreducibel en elke $n_i > 0$, en $r \in \mathbb{N}$.

Met een beetje meer werk kan men het gevolg bewijzen voor eindig voortgebrachte modulen over een willekeurig hoofdideaaldomein. Het is bovendien zo dat de machten $p_i^{n_i}$ uniek zijn op inverteerbare elementen na. Voor abelse groepen is dit vrij eenvoudig te bewijzen (via combinatorische argumenten).

Hoofdstuk

4 Toepassingen

4.1 Velden en velduitbreidingen

Algebraïsche uitbreidingen

Beschouw een veld K. We hebben de precieze definitie gezien van een irreducibel element in een ring, meer bepaald in een polynomenring $K[X]$. We hebben ook gezien dat een irreducibel polynoom $f(X)$ een maximal ideaal $I = (f(X))$ bepaalt. De quotiëntring $E = K[x]/(f(X))$ is dus een veld. Omdat $K[X]$ een Euclidisch domein is, kunnen we de formule van Bézout gebruiken (of in de praktijk het uitgebreid algoritme van Euclides) om de multiplicatieve inverse van een element $a \in E \setminus \{0\}$ te berekenen, immers, voor een element $x \in E$, voorgesteld door een polynoom $g(X) \in K[x]$, geldt $\text{ggd}(f(X), g(X)) = 1$, en er bestaan elementen $r(X), s(X) \in K[X]$ waarvoor

$$1 = r(X)f(X) + s(X)g(X)\,.$$

Dus modulo $f(X)$ geldt $s(X)g(X) = 1$. De theorie van algebraïsche uitbreidingen van lichamen, komt in zeer ruime mate aan bod in het vak Galoistheorie. Hier zullen we ons beperken tot voorbeelden en enkele van hun eigenschappen.

Een belangrijke klasse van voorbeelden zijn de *eindige lichamen*. Deze kunnen allemaal geconstrueerd worden door bovenstaande procedure te gebruiken, startend van een veld met p elementen, p priem, en een irreducibel polynoom van graad h.

Stel bijvoorbeeld $p = 2$, dan is $K = \mathbb{Z}/2\mathbb{Z}$. Het is duidelijk dat $f(X) = X^2 + X + 1$ irreducibel is in $K[x]$. De elementen van $E = K[x]/(f(X))$ zijn polynomen van $K[X]$ modulo $f(X)$, dus $E = \{0, 1, X, X + 1\}$. In dit geval is het heel eenvoudig na te gaan dat $X(X+1) \equiv 1 \pmod{f}$. Dus X en $X+1$ zijn elkaars multiplicatieve inverse. Verder geldt ook dat $X^2 = X + 1$ en $X^3 = X^2 + X = 1$ in E. De inverteerbare elementen zijn dus $\{1, X, X^2\}$, en de multiplicatieve groep is cyclisch met X als voortbrenger. We vermelden een aantal stellingen over eindige lichamen zonder bewijs.

Stelling 4.1.1. *Voor elk priemgetal p en elk natuurlijk getal $h \geq 1$, bestaat er een eindig veld van orde $q = p^h$. Elk eindig veld is op isomorfisme na gelijk aan de bovenstaande constructie.*

We noteren een eindig veld van orde q vaak als $\mathbb{F}_q$ of $\mathrm{GF}(q)$.

Stelling 4.1.2. *Elk eindig veld heeft $q = p^h$ elementen, p priem, $h \geq 1$. De multiplicatieve groep is een cyclische groep van orde $q - 1$.*

Gevolg 4.1.3. *Veronderstel dat K een eindig veld is met q elementen. Dan geldt in $K[X]$*

$$X^q - X = \prod_{a \in K} X - a \,.$$

Stelling 4.1.4. *Een eindig veld van de orde $q = p^h$, heeft een cyclische automorfismegroep van orde h, voortgebracht door het* Frobenius-*automorfisme:*

$$\phi : \mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^p \,.$$

Het is eenvoudig na te gaan dat ϕ een automorfisme van $\mathbb{F}_q$ is.

Een veld K is *algebraïsch gesloten* als de irreducibele elementen van $K[X]$ precies de monische veeltermen van graad 1 zijn, dus als elk polynoom uit $K[X] \setminus K$ te schrijven is als product van lineaire factoren. Een algebraïsche sluiting van een veld K is een algebraïsch gesloten veld E dat K bevat. Ook de volgende stelling is een klassieker uit de algebra. Het bewijs steunt onder andere op het Lemma van Zorn.

Stelling 4.1.5. *Voor elk veld K bestaat er een algebraïsche sluiting $\overline{K}$. Deze is echter niet uniek bepaald, maar slechts op een automorfisme na.*

Het bekendste voorbeeld van een algebraïsch gesloten veld is wellicht het veld der complexe getallen $\mathbb{C}$. Men kan $\mathbb{C}$ beschouwen als een veldsuitbreiding van $\mathbb{R}$: $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$. De complexe toevoeging is een veldautomorfisme van $\mathbb{C}$, dat $\mathbb{R}$ elementsgewijze fixeert. Er bestaan verschillende bewijzen van de volgende stelling. Eén van de gebruikelijke bewijzen is analytisch, het maakt gebruikt van de topologische eigenschappen van $\mathbb{R}$ en $\mathbb{C}$. Men kan echter in het kader van Galoistheorie ook een *zuiver algebraïsch* bewijs geven.

Stelling 4.1.6. *Het veld der complexe getallen is algebraïsch gesloten.*

Het veld der p-adische getallen

Veronderstel dat K een veld is, en noteer $\mathbb{R}^+ := \{x \in \mathbb{R}, x \geq 0\}$.

Definitie 4.1.7. Een absolute waarde op K is een afbeelding $|\,| : K \to \mathbb{R}^+$ die voldoet aan

(i) $|x| = 0 \iff x = 0$

(ii) $|xy| = |x||y|$ voor alle $x, y \in K$

(iii) $|x + y| \leq |x| + |y|$, voor alle $x, y \in K$

Een absolute waarde is niet-Archimediaans als $|x+y| \leq \max\{|x|, |y|\}$, voor alle $x, y \in K$.

Het volgende lemma beschrijft een zeer belangrijke eigenschap van niet-Archimediaanse absolute waarden.

Lemma 4.1.8. *Zij $|\,|$ een niet-Archimediaanse absolute waarde op een veld K. Stel $x, y \in K$. Als $|x| \neq |y|$, dan is $|x + y| = \max\{|x|, |y|\}$.*

Bewijs. Stel $|x| \neq |y|$. Zonder verlies van algemeenheid mogen we veronderstellen dat $|x| > |y|$. Dus $|x + y| \leq \max\{|x|, |y|\} = |x|$. Omdat $x = (x + y) - y$, geldt ook $|x| = |x + y - y| \leq \max\{|x + y|, |y|\}$. Als $|x + y| < |y|$, dan is $|x| \leq |y|$, een contradictie. Dus $\max\{|x + y|, |y|\} = |x + y|$, dus $|x| \leq |x + y| \leq |x|$. Dus $|x| = |x + y|$. □

We zullen een niet-Archimediaanse absolute waarde op $K = \mathbb{Q}$ definiëren aan de hand van de zogenaamde p-adische valuatie. Stel $p \in \mathbb{N}$ is een priemgetal. De *p-adische valuatie op $\mathbb{Z}$* is de afbeelding $v_p : \mathbb{Z} \to \mathbb{N}$: $v_p(x) = n$ als en slechts als $p^n | x$ en $p^{n+1} \nmid x$. Het is duidelijk dat $\mathrm{Im}\,(v_p) = \mathbb{N}$. Met breidt het definitiegebied van v_p eenvoudig uit tot $\mathbb{Q}$ door $v_p(\frac{a}{b}) := v_p(a) - v_p(b)$ te stellen, en dan wordt $\mathrm{Im}\,(v_p) = \mathbb{Z}$.

Lemma 4.1.9. *Voor alle $x, y \in \mathbb{Q}$ geldt*

(i) $v_p(xy) = v_p(x) + v_p(y)$,

(ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Bewijs. Bewijs deze eigenschap als oefening. □

Definitie 4.1.10. Stel $p \in \mathbb{N}$ is een priemgetal. De p-adische absolute waarde op $\mathbb{Q}$ is de afbeelding $|\ |_p : \mathbb{Q} \to \mathbb{R}^+$: $|x|_p := p^{-v_p(x)}$ als $x \neq 0$ en $|x|_p = 0$ als $x = 0$.

Het is eenvoudig in te zien dat $|\ |_p$ een niet-Archimediaanse absolute waarde is, en dat $\mathrm{Im}\,(|\ |_p) = \{p^n | n \in \mathbb{Z}\}$.

Definitie 4.1.11. Veronderstel dat K een veld is en $|\ |$ een absolute waarde op K.

(i) Een rij (x_n) van elementen in K is een *Cauchyrij* als voor elke $\epsilon \in \mathbb{R}^+ \setminus \{0\}$ er een $M \in \mathbb{N}$ bestaat met de eigenschap $|x_n - x_m| < \epsilon$ van zodra $m, n > M$.

(ii) Een veld K is *compleet* ten opzichte van een absolute waarde $|\ |$ als en slechts als elke Cauchyrij een limiet heeft in K.

De lichamen $\mathbb{R}$ en $\mathbb{C}$ zijn compleet ten opzichte van de gebruikelijke absolute waarde. Het is precies deze eigenschap dat deze lichamen geschikt maakt om analyse te doen. Het volgende lemma is een typische eigenschap van een niet-Archimediaanse absolute waarde. Het is dan ook helemaal niet geldig voor de gewone absolute waarde op de lichamen $\mathbb{R}$ en $\mathbb{C}$.

Lemma 4.1.12. *Een rij (x_n) in $\mathbb{Q}$ is een Cauchyrij ten opzichte van een niet Archimediaanse absolute waarde $|\ |$ als en slechts als $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.*

Bewijs. Stel $m = n + r > n$. Dan is

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - \cdots + x_{n+1} - x_n| \\ &\leq \max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|\} \end{aligned}$$

Dus $\lim_{n\to\infty} |x_{n+1} - x_n| = 0 \implies |x_m - x_n| < \epsilon$ als $m, n > M$. De omgekeerde implicatie is triviaal. □

We zullen nu aantonen dat $\mathbb{Q}$ niet compleet is ten opzichte van de absolute waarde $|\ |_p$. Merk op dat $\mathbb{Q}$ ook niet compleet is ten opzichte van de gebruikelijke absolute waarde. Het is eenvoudig om een Cauchyrij te construeren ten opzichte van $|\ |$ die niet convergeert naar een rationaal getal. Denk bijvoorbeeld aan $\sqrt{2}$, en de opeenvolgende rationale benaderingen ervan. Het volgende resultaat gebruikt in feite hetzelfde idee: we construeren een algebraïsch element, i.e. een oplossing van een polynoom, waarvan we zeker weten dat het geen rationaal getal is. Het tweede belangrijke idee in het bewijs is de zogenaamde "lifting" van elementen modulo p naar elementen modulo p^n, voor willekeurige n. Daardoor kunnen we als het ware elementen uit het eindig veld $\mathbb{Z}/p\mathbb{Z}$ liften naar p-adische getallen.

Lemma 4.1.13. *Stel $p \in \mathbb{N}$ priem en $l \in \mathbb{N}$, $p \nmid l$, en $l \geq 2$. Stel $n \in \mathbb{N} \setminus \{0\}$ en $a \in \mathbb{Z}$, $p \nmid a$. Stel dat er een $\alpha_n \in \mathbb{Z}$ bestaat zodat $\alpha_n^l \equiv a \pmod{p^n}$. Dan bestaat er een $\alpha_{n+1} \in \mathbb{Z}$ zodat $\alpha_{n+1}^l \equiv \alpha \pmod{p^{n+1}}$ en $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$.*

Bewijs. Stel $\alpha_{n+1} := \alpha_n + kp^n$, $k \in \mathbb{Z}$. Dan moet

$$\alpha_{n+1}^l = \sum_{i=0}^{l} \binom{l}{i} \alpha_n^{l-i} k^i p^{ni} \equiv a \pmod{p^{n+1}}.$$

Daaruit volgt

$$\alpha_n^l + l\alpha_n^{l-1} kp^n \equiv a \pmod{p^{n+1}}.$$

Omdat $\alpha_n^l \equiv a \pmod{p^n}$, is $\alpha_n^l - a = mp^n$ voor een welbepaalde $m \in \mathbb{Z}$. Dus

$$mp^n + l\alpha_n^{l-1} kp^n \equiv 0 \pmod{p^{n+1}}$$

waaruit volgt dat $l\alpha_n^{l-1} k \equiv -m \pmod{p}$. Omdat $p \nmid l\alpha_n^{l-1}$, bestaat er een inverse voor $l\alpha_n^{l-1} \pmod{p}$, dus er is een unieke oplossing voor $k \in \{0, 1, \ldots, p-1\}$. □

Voorbeelden 4.1.14. Stel $\alpha_1^2 \equiv 2 \pmod{7}$. Er zijn 2 oplossingen voor α_1: $\alpha_1 \in \{-4, 4\}$. Kiezen we $\alpha_1 = 4$, en passen we de procedure uit het bewijs toe, dan vinden we $\alpha_2 = 39$, $\alpha_3 = 235$, $\alpha_4 = 235$, $\alpha_5 = 12240$, ... We moeten uiteraard niet met $l = 2$ werken, en we kunnen ook starten met $\alpha_n^l = a \pmod{p^n}$ voor eender welke $n \geq 1$. Een dergelijk voorbeeld gaan we gebruiken in het bewijs van volgende lemma.

Definitie 4.1.15. Stel $(x_n) \in C_p(\mathbb{Q})$. Dan zeggen we dat $\lim\limits_{n\to\infty} x_n = x$ als en slechts als $\lim\limits_{n\to\infty} |x_n - x|_p = 0$.

Lemma 4.1.16. *Het veld $\mathbb{Q}$ is niet compleet ten opzichte van de p-adische absolute waarde.*

Bewijs. Stel p is een priemgetal verschillend van 2. Men vindt eenvoudig een element $a \in \mathbb{Z}$ dat geen kwadraat is in $\mathbb{Z}$ maar wel een kwadraat modulo p. Dus er bestaat een α_1 zodat $\alpha_1^2 \equiv a \pmod{p}$. Er bestaat dus voor alle $n \in \mathbb{N} \setminus \{0\}$ een $\alpha_n \in \mathbb{Z}$, met $\alpha_n^2 \equiv a \pmod{p^n}$ en $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$. Beschouw nu de rij (α_n), dan geldt $p^n \mid (\alpha_{n+1} - \alpha_n)$. Dus $v_p(\alpha_{n+1} - \alpha_n) \geq n$, dus $|\alpha_{n+1} - \alpha_n|_p \leq p^{-n}$. Dus $\lim_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p = 0$, m.a.w. de rij (α_n) is een Cauchyrij. Stel nu $\lim_{n\to\infty} \alpha_n = \alpha \in \mathbb{Q}$.

Er geldt ook dat $p^n \mid (\alpha_n^2 - a)$. Dus $|\alpha_n^2 - a|_p =\leq p^{-n}$, dus $\lim_{n\to\infty} |\alpha_n^2 - a|_p = 0$. Dus $\alpha^2 = \lim_{n\to\infty} \alpha_n^2 = a$, maar $a \in \mathbb{Z}$, een contradictie want a is geen kwadraat.

Stel nu $p = 2$. Kies $\alpha_3 = 3$. Er geldt dat $\alpha_3^3 \equiv 3 \pmod{2^3}$. We vinden dus opnieuw een rij $(\alpha_n)_{n\geq 3}$ zodat $\alpha_{n+1}^3 \equiv 3 \pmod{2^{n+1}}$ en $\alpha_{n+1} \equiv \alpha_n \pmod{2^n}$, dus deze rij is een Cauchyrij, en als deze naar $\alpha \in \mathbb{Q}$ convergeert dan is $\alpha^3 = 3$, een contradictie.

We besluiten dat voor elk priemgetal p, het veld $\mathbb{Q}$ niet compleet is ten opzichte van de p-adische absolute waarde. □

We noteren de verzameling van alle Cauychyrijgen in $\mathbb{Q}$ ten opzichte van de p-adische absolute waarde als $C_p(\mathbb{Q})$. Op deze verzameling definiëren we zoals verwacht een puntsgewijze optelling en vermenigvuldiging.

$$(x_n) + (y_n) := (x_n + y_n)\,,$$
$$(x_n) \cdot (y_n) := (x_n y_n)\,.$$

Lemma 4.1.17. *Beschouw een Cauchyrij $(x_n) \in C_p(\mathbb{Q}) \setminus \mathcal{N}$. Dan is de rij $|x_n|_p$ stationair, i.e. $|x_n|_p = \lambda \in \mathbb{Q}$ voor $n \geq N$, voor een zekere $N \in \mathbb{N}$.*

Bewijs. Omdat $(x_n) \notin \mathcal{N}$ bestaat er een $N \in \mathbb{N}$ en een $c > 0$ zodat $|x_n|_p \geq c > 0$ van zodra $n \geq N$. Omdat (x_n) een Cauchyrij is, bestaat er een N' zodanig dat $|x_n - x_m|_p < c$ van zodra $n, m > N'$. Stel $M = \max\{N, N'\}$, dan geldt

$$n, m \geq M \implies |x_n - x_m|_p < c \leq \max\{|x_n|_p, |x_m|_p\}\,.$$

Door Lemma 4.1.8 volgt nu dat $|x_n|_p = |x_m|_p$ als $n, m \geq M$. □

Gevolg 4.1.18. *Beschouw een Cauchyrij $(x_n) \in C_p(\mathbb{Q}) \setminus \mathcal{N}$. Dan is de rij $(|x_n|_p)$ begrensd.*

Lemma 4.1.19. *De verzameling $C_p(\mathbb{Q})$ is een commutatieve ring. Het eenheidselement voor de optelling is de rij (0), het eenheidselement voor de vermenigvuldiging is de rij (1).*

Bewijs. Het is duidelijk dat

$$\lim_{n\to\infty} |x_{n+1} + y_{n+1} - x_n - y_n|_p \leq \lim_{n\to\infty} \max\{|x_{n+1} - x_n|_p, |y_{n+1} - y_n|_p\} = 0\,.$$

Voor het product van twee Cauchyrijen geldt

$$\begin{aligned}\lim_{n\to\infty} |x_{n+1}y_{n+1} - x_n y_n|_p &= \lim_{n\to\infty} |x_{n+1}(y_{n+1} - y_n) - y_n(x_{n+1} - x_n)|_p \\ &\leq \lim_{n\to\infty} \max\{|x_{n+1}|_p|y_{n+1} - y_n|_p, |y_n|_p|x_{n+1} - x_n|_p\} = 0\,,\end{aligned}$$

omwille van Gevolg 4.1.18. □

We noteren de verzameling van alle Cauchyrijen die naar $0 \in \mathbb{Q}$ convergeren als $\mathcal{N} := \{(x_n) | \lim_{n\to\infty} x_n = 0\} = \{(x_n) | \lim_{n\to\infty} |x_n|_p = 0\}$.

Lemma 4.1.20. *De verzameling $\mathcal{N}$ is een maximaal ideaal in $C_p(\mathbb{Q})$.*

Bewijs. Het bewijs steunt andermaal op het niet-Archimediaans zijn van $|\,|_p$. Voor $(x_n), (y_n) \in \mathcal{N}$ geldt duidelijk

$$\lim_{n\to\infty} |x_n - y_n|_p \leq \lim_{n\to\infty} \max\{|x_n|_p, |y_n|_p\} = 0\,,$$

Voor het product van een rij $(x_n) \in \mathcal{N}$ met een rij $(y_n) \in C_p(\mathbb{Q})$ geldt

$$\lim_{n\to\infty} |x_n y_n|_p = \lim_{n\to\infty} |x_n|_p |y_n|_p = 0\,,$$

omdat $|y_n|_p$ begrensd is en (x_n) een nulrij. Dus $\mathcal{N}$ is een ideaal van $C_p(\mathbb{Q})$.

Beschouw nu een element $(x_n) \in C_p(\mathbb{Q}) \setminus \mathcal{N}$. We noemen I het ideaal voortgebracht door (x_n) en $\mathcal{N}$, en we zullen aantonen dat $(1) \in I$. Omdat $(x_n) \notin \mathcal{N}$, bestaat er een $c > 0$, en een $N \in \mathbb{N}$ met $x_n > c$ als $n \geq N$. Dus vanaf $n \geq N$, is $x_n \neq 0$. We definiëren $y_n := \frac{1}{x_n}$, als $n \geq N$ en $y_n := 0$ als $n < N$. Dan is $(y_n) \in C_p(\mathbb{Q})$. Immers,

$$\left|\frac{1}{x_n} - \frac{1}{x_{n+1}}\right|_p = \frac{|x_{n+1} - x_n|_p}{|x_n x_{n+1}|_p} \leqslant \frac{|x_{n+1} - x_n|_p}{c^2}\,,$$

hetgeen naar nul convergeert omdat (x_n) een Cauchyrij is. Het is daarenboven duidelijk dat $(x_n)(y_n)$ op de eerste N termen na gelijk is aan (1), dus $(1) - (x_n)(y_n) \in \mathcal{N}$. Tellen we bij (1) het veelvoud $(x_n)(y_n)$ op, dat besluiten we dat $(1) \in I$. Dus $\mathcal{N}$ is maximaal. □

Definitie 4.1.21. Voor een priemgetal $p \in \mathbb{N}$ is $\mathbb{Q}_p = C_p(\mathbb{Q})/\mathcal{N}$ het veld der p-adische getallen.

Het is duidelijk dat de rationale getallen $\mathbb{Q}$ gemakkelijk ingebed kunnen worden in $\mathbb{Q}_p$. Het volstaat om elk getal $x \in \mathbb{Q}$ te identificeren met de stationaire rij (x). Vanaf nu zullen we de elementen van $\mathbb{Q}_p$ noteren als $x \in \mathbb{Q}_p$, en $\mathbb{Q}$ als echte deelverzameling van $\mathbb{Q}_p$ beschouwen.

Als $x \in \mathbb{Q}_p$ dus voorgesteld wordt door de Cauchyrij (x_n), dan definiëren we $|x|_p := \lim_{n\to\infty} |x_n|_p$, en $v_p(x) := -\log_p(|x|_p)$ als $x \neq 0$. Dat $|x|_p := \lim_{n\to\infty} |x_n|_p$ altijd bestaat, volgt uit Lemma 4.1.17.

Lemma 4.1.22. *De afbeelding $|\,|_p$ is goed gedefinieerd op $\mathbb{Q}_p$ en $|\,|_p$ is een niet-Archimediaanse absolute waarde die een uitbreiding is van $|\,|_p$ op $\mathbb{Q}$.*

Bewijs. Bewijs als oefening. □

Gevolg 4.1.23. *Het beeld van $|\,|_p$ op $\mathbb{Q}_p$ is de verzameling $\{0\} \cup \{p^n | n \in \mathbb{Z}\}$.*

Het is nu eenvoudig om in te zien dat $|\,|_p$ een niet-Archimediaanse absolute waarde op $\mathbb{Q}_p$ is, die beperkt tot $\mathbb{Q}$ volledig samenvalt met de gedefinieerde absolute waarde $|\,|_p$ op $\mathbb{Q}$. We kunnen nu dezelfde procedure herhalen en trachten om $\mathbb{Q}_p$ opnieuw uit te breiden. De volgende stelling toont echter aan dat deze procedure niets meer toevoegt aan $\mathbb{Q}_p$, namelijk dat $\mathbb{Q}_p$ een zogenaamde topologische completering is van $\mathbb{Q}$ ten opzichte van de absolute waarde $|\,|_p$[1]

Stelling 4.1.24. *De verzameling $\mathbb{Q}_p$ is compleet ten opzichte van $|\,|_p$, i.e. elke Cauchyrij van elementen uit $\mathbb{Q}_p$ convergeert naar een element uit $\mathbb{Q}_p$.*

Bewijs. Het bewijs van deze stelling is op zich niet moeilijk, maar steunt voornamelijk op analytische argumenten. Daarom laten we het hier achterwege. □

We beschikken door de topologische constructie over voldoende gereedschap om de *algebraïsche* eigenschappen van $\mathbb{Q}_p$ te bespreken.

Definitie 4.1.25. voor een priemgetal $p \in \mathbb{N}$ is de *ring der p-adische gehele getallen* de ring

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p | |x|_p \leq 1\}.$$

Dat $\mathbb{Z}_p$ gesloten is onder optelling en vermenigvuldiging, volgt uit het feit dat $|\,|_p$ een niet-Archimediaanse absolute waarde is. Het is dus inderdaad zo dat de verzameling $\mathbb{Z}_p$ een ring is. Merk op dat $\mathbb{Z} \subset \mathbb{Z}_p$.

Stelling 4.1.26. *De ring $\mathbb{Z}_p$ is een lokale ring. Haar unieke maximale ideaal is het hoofdideaal voortgebracht door p. Verder geldt $\mathbb{Q} \cap \mathbb{Z}_p = \{\frac{a}{b} \in \mathbb{Q} | p \nmid b\} = \mathbb{Z}_{(p)}$*

Bewijs. Beschouw de verzameling $M := \{x \in \mathbb{Z}_p | |x|_p < 1\}$. Het is duidelijk dat M een ideaal is in $\mathbb{Z}_p$. Het is ook duidelijk dat de elementen van $\mathbb{Z}_p$ die inverteerbaar zijn,

[1] Nog iets correcter: ten opzichte van de afstand op $\mathbb{Q}$ gedefinieerd door $|\,|_p$.

precies de elementen van $\mathbb{Z}_p \setminus M$ zijn. Elk ideaal dat minstens één inverteerbaar element bevat, bevat ook 1 en is dus de volledige ring. Dus M is een maximaal ideaal.

Stel nu dat I een willekeurig maximaal ideaal is van $\mathbb{Z}_p$. Kies $x \in \mathbb{Z}_p \setminus I$. Omdat I maximaal is, bestaat er een $y \in I$, en $r, s \in \mathbb{Z}_p$, zodat $1 = rx + sy$. Nu geldt $1 = |1|_p = |rx + sy|_p \leq \max\{|rx|_p, |sy|_p\}$. Maar $|sy|_p < 1$ en $|r|_p \leq 1$, dus moet $|x|_p = |r|_p = 1$, dus x is inverteerbaar in $\mathbb{Z}_p$ en $I = M$.

Het ideaal M is dus het unieke maximale ideaal in $\mathbb{Z}_p$. Stel nu $x \in M$. Dan volgt uit $|x|_p < 1$ dat $|x|_p \leq \frac{1}{p}$. Omdat $|p|_p = \frac{1}{p}$, volgt dus dat $|\frac{x}{p}|_p \leq 1$, dus $\frac{x}{p} \in \mathbb{Z}_p$, dus $x \in p\mathbb{Z}_p$. Er volgt dus dat $M \subset p\mathbb{Z}_p$, maar omdat M maximaal is, is er gelijkheid.

De laatste uitspraak in de stelling volgt nu onmiddellijk uit de definitie van $\mathbb{Z}_p$ en de p-adische absolute waarde. □

Het veld $\mathbb{Q}$ is *dicht* in $\mathbb{R}$. Hetzelfde geldt voor $\mathbb{Q}$ in $\mathbb{Q}_p$, en ook voor $\mathbb{Z}$ in $\mathbb{Z}_p$. Omdat we vooral de algebraïsche eigenschappen van $\mathbb{Z}_p$ willen kennen, is enkel dit laatste van belang.

Stelling 4.1.27. *De verzameling $\mathbb{Z}$ is dicht in $\mathbb{Z}_p$.*

Bewijs. We moeten aantonen dat voor een willekeurige $a \in \mathbb{Z}_p$ en een willekeurige $\epsilon \in \mathbb{R}^+$, er steeds een $A \in \mathbb{Z}$ bestaat zodat $|A - a|_p < \epsilon$, of, equivalent, voor een willekeurige $n \geq 1$, moet er steeds een $A_n \in \mathbb{Z}$ bestaan met $v_p(a - A_n) \geq n$.

Het element $a \in \mathbb{Z}_p$ kan voorgesteld worden door een Cauchyrij $(a_n) \in C_p(\mathbb{Q})$. Omdat $v_p(a) \geq 0$, weten we zeker dat er slechts een eindig aantal elementen uit de rij (a_n) zijn met $v_p(a_n) < 0$. Na weglating, mogen we dus veronderstellen dat $v_p(a_n) \geq 0$ voor alle $n \in \mathbb{N}$. Omdat (a_n) een Cauchyrij is, mogen we, opnieuw na eventueel weglaten van een eindig aantal termen, veronderstellen dat $v_p(a_i - a_j) \geq n$, voor alle $i, j \in \mathbb{N}$. Stel nu $a_i = \frac{c_i}{d_i}$, $c_i \in \mathbb{Z}$, $d_i \in \mathbb{N}$, $p \nmid d_i$.

Omdat $p \nmid d_1$ bestaat een inverse voor d_1 in $\mathbb{Z}/p^n\mathbb{Z}$. Daarom kunnen we voor elke $n \in \mathbb{N}$ een getal $A_n \in \mathbb{Z}$ vinden waarvoor

$$d_1 A_n \equiv c_1 \pmod{p^n}.$$

Voor een willekeurige $i \in \mathbb{N}$ geldt nu

$$a_i - a_1 = \frac{c_i}{d_i} - \frac{c_1}{d_1} = p^n \frac{c}{d}, \qquad c \in \mathbb{Z}, d \in \mathbb{N}, p \nmid d.$$

Dus $d(c_i d_1 - c_1 d_i) = p^n c d_1 d_i$, en omdat $p \nmid d$ volgt $p^n \mid c_i d_1 - c_1 d_i$. Door de keuze van A_n geldt $p^n \mid (c_i d_1 - d_1 A_n d_i)$. Omdat $p \nmid d_1$ kunnen we ook een $b \in \mathbb{Z}$ vinden

waarvoor $p^n b = c_i - A_n d_i$. Dus $a_i - A_n = p^n \frac{b}{d_i}$, dus $v_p(a_i - A_n) \geq n$. Met $v_p(a - A_n) = v_p(a - a_i + a_i - A_n) \geq \min\{v_p(a - a_i), v_p(a_i - A_n)\} \geq n$, volgt dat $\lim_{n\to\infty} A_n = a$. □

We bestuderen eerst de idealen voortgebracht door p^n, $n \in \mathbb{N} \setminus \{0\}$.

Merk op dat $|p^n|_p = p^{-n} < 1$, dus $p^n \in \mathbb{Z}_p$. Dit wisten we in feite ook al uit het bewijs van Stelling 4.1.26, en we gebruiken nu hetzelfde argument om de idealen (p^n) te karakteriseren. Stel $x \in \mathbb{Z}_p$ en $|x|_p \leq \frac{1}{p^n}$. Dan is $|\frac{x}{p^n}|_p \leq 1$, dus $\frac{x}{p^n} \in \mathbb{Z}_p$, of $x \in p^n\mathbb{Z}_p$. Omgekeerd geldt dat $|xp^n|_p = |x|_p \frac{1}{p^n} \leq \frac{1}{p^n}$ omdat $x \in \mathbb{Z}_p$. Dus

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Z}_p || x|_p \leq \frac{1}{p^n}\} = \{x \in \mathbb{Z}_p | v_p(x) \geq n\}\,.$$

Stelling 4.1.28. *De natuurlijke inbedding $\mathbb{Z} \subset \mathbb{Z}_p$ induceert een ringisomorfisme tussen $\mathbb{Z}/p\mathbb{Z}$ en $\mathbb{Z}_p/p\mathbb{Z}_p$.*

Bewijs. Noem de inbedding φ en het geïnduceerde ringhomomorfisme $\overline{\varphi}$. Dan is $\overline{\varphi}(\overline{x}) = \overline{\varphi(x)}$. Stel $I = (p^n) \subset \mathbb{Z}_p$. Dan is $I = \{a \in \mathbb{Z}_p | v_p(a) \geq n\}$. Noodzakelijk is $\overline{\varphi}(\overline{a}) = 0 \iff v_p(a) \geq n \iff a \in p^n\mathbb{Z} \iff \overline{a} = 0$. Dus φ is injectief. Kies nu $\overline{b} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$. Wegens voorgaand lemma vinden we voor elke $n \in \mathbb{N}$ een $A_n \in \mathbb{Z}$ waarvoor $v_p(b - A_n) \geq n$, m.a.w. $b - A_n \in (p^n)$, dus A_n is ook een representant van $\overline{b}$. Dus $\overline{A_n} \in \mathbb{Z}/p^n\mathbb{Z}$ wordt door $\overline{\varphi}$ op $\overline{b}$ afgebeeld. Dus $\overline{\varphi}$ is surjectief. □

Aangezien $p\mathbb{Z}_p$ een maximaal ideaal is in $\mathbb{Z}_p$, is $\mathbb{Z}_p/p\mathbb{Z}_p$ een veld. Nu is duidelijk dat $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Lemma 4.1.29. *Een element $u \in \mathbb{Q}_p$ is een eenheid in $\mathbb{Z}_p$ als en slechts als $|u|_p = 1$, of nog, u is een eenheid in $\mathbb{Z}_p$ als en slechts als $u \not\equiv 0 \mod p$.*

Bewijs. Bewijs als oefening. □

Lemma 4.1.30. *Elk element $a \in \mathbb{Q}_p \setminus \{0\}$ kan op een unieke wijze geschreven worden als $a = p^n u$, $n \in \mathbb{Z}$, u een eenheid in $\mathbb{Z}_p$.*

Bewijs. Stel $n := v_p(a)$, dan is $v_p(ap^{-n}) = 0$, dus $u := ap^{-n}$ is een eenheid in $\mathbb{Z}_p$. Stel omgekeerd dat $a = p^n u$, u een eenheid in $\mathbb{Z}_p$, dan is $p \nmid u$, dus $v_p(a) = n$, en $u = ap^{-n}$. De voorstelling is dus uniek bepaald. □

Lemma 4.1.31. *De ring $\mathbb{Z}_p$ is een hoofdideaaldomein. De enige idealen zijn de idealen (p^n), $n \geq 1$.*

Bewijs. Stel I is een ideaal in $\mathbb{Z}_p$. Definieer $n := \min\{v_p(a) | a \in I\}$. Kies $a \in I \setminus \{0\}$. Voor $u := ap^{-v_p(a)}$ geldt $v_p(u) = 0$, dus u is een eenheid in $\mathbb{Z}_p$. Door de definitie van n is $p^{v_p(a)-n}u \in \mathbb{Z}_p$ en dus $a = p^n p^{v_p(a)-n}u \in p^n\mathbb{Z}_p$. Dus $I \subset p^n\mathbb{Z}_p$.

Omgekeerd, door de definitie van n bestaat er een $a \in I$ met $v_p(a) = n$. Dus $a = p^n u$, met u een eenheid in $\mathbb{Z}_p$, dus $p^n = au^{-1} \in I$, met andere woorden, $p^n\mathbb{Z}_p \subset I$. □

We kiezen nu een element $a \in \mathbb{Z}_p$. Voor elke $n \in \mathbb{N}$ kunnen we dus het beeld van a modulo p^n beschouwen. Aangezien $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, definieert het element a dus een rij (a_n), $a_n \in \mathbb{Z}/p\mathbb{Z}$, en $a_{n+1} \equiv a_n \pmod{p^n}$. We zullen nu een alternatieve manier beschrijven om $\mathbb{Z}_p$ te definiëren.

We noemen een rij $(a_n)_{n\geq 1}$, $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ een coherente rij als $a_{n+1} \equiv a_n \pmod{p^n}$. De verzameling van alle coherente rijden is de *inverse limiet* van $\mathbb{Z}/p^n\mathbb{Z}$, genoteerd

$$\lim_{\leftarrow n} \mathbb{Z}/p\mathbb{Z}_p\,.$$

We definiëren de optelling, respectievelijk vermenigvuldiging, als componentsgewijze optelling, respectievelijk vermenigvuldiging. Het is duidelijk dat $\lim_{\leftarrow n} \mathbb{Z}/p\mathbb{Z}_p$ een ring is.

Stelling 4.1.32. *Beschouw de afbeelding $\Phi : \mathbb{Z}_p \to \lim_{\leftarrow n} \mathbb{Z}/p\mathbb{Z}_p$, $a \mapsto \Phi(a) = (a \pmod{p^n})_{n\geq 1}$. Dan is Φ een ringisomorfisme.*

Bewijs. Het is duidelijk dat Φ een ringhomomorfisme is. Veronderstel dat $a, b \in \mathbb{Z}_p$ en $a \equiv b \pmod{p^n}$. Dus $a - b \in (p^n)$, of nog, $v_p(a - b) \geq n$. Als $\Phi(a) = \Phi(b)$, dan is $a \equiv b \pmod{p^n}$, voor alle $n \in \mathbb{N}$, dus $v_p(a - b) \geq n$ voor alle n, dus $a = b$ in $\mathbb{Z}_p$. We besluiten dat Φ injectief is.

Kies nu een willekeurige coherente rij (a_n). Voor elke a_n kiezen we een representant $A_n \in \mathbb{Z}$. Voor elke $n, m \in \mathbb{N}$ geldt nu dat $v_p(A_n - A_m) \geq \min\{m, n\}$. Dus de rij (A_n) is een Cauchyrij, en convergeert naar een $a \in \mathbb{Z}_p$. Omdat $v_p(a - A_n) \geq n$, geldt $a - A_n \in (p^n)$, dus $a \equiv A_n \pmod{p^n}$, dus $\Phi(a) = (A_n)$, en Φ is surjectief. □

Eens $\mathbb{Z}_p$ als inverse limiet geconstrueerd is, kan men $\mathbb{Q}_p$ definiëren als breukenveld. Deze definitie heeft als nadeel dat men achteraf de p-adische absolute waarde moet definiëren.

Het veld $\mathbb{Q}_p$ heeft topologische eigenschappen die nodig zijn om analyse te doen. Een aantal van deze eigenschappen is totaal verschillend van de eigenschappen van $\mathbb{R}$. Zo kan men aantonen dat $\mathbb{Q}_p$ niet geordend kan worden. Het veld der reële getallen is eenvoudig algebraïsch uit te breiden tot $\mathbb{C}$, een veld dat algebraïsch gesloten is. Voor $\mathbb{Q}_p$ ligt dit anders, er zijn een oneindig aantal velduitbreidingen nodig om $\mathbb{Q}_p$ algebraïsch af te sluiten. Het resulterende veld is daarenboven niet meer topologisch compleet. Een topologische completering levert dan het veld $\mathbb{C}_p$, wat op zijn beurt algebraïsch afgesloten blijkt. Bij elke uitbreiding blijft de p-adische absolute waarde en bijhorende valuatie blijft overeind. Het waardengebied van v_p op $\mathbb{C}_p$ is $\mathbb{Q}$.

Toepassingen

Getaltheorie

Het gebruik van p-adische getallen levert soms opmerkelijke bewijzen op van resultaten uit de getaltheorie die zeer moeilijk of onmogelijk op een *elementaire* manier te bewijzen zijn. Beschouw de volgende stelling.

Stelling 4.1.33. *Voor elk natuurlijk getal $M > 0$ bestaat er een $n \in \mathbb{N}$ zodanig dat*

$$2^M \mid 2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \ldots + \frac{2^n}{n}\,.$$

Een bewijs kan via p-adische analyse gevonden worden. Beschouw de volgende reeks

$$\sum_{i=1}^{\infty} (-1)^{(i+1)} \frac{X^i}{i}\,.$$

Men kan aantonen dat deze reeks convergeert voor alle $X \in \{x \in \mathbb{Q}_p || x|_p < 1\}$. We noteren de reekssom als $\log(1+X)$. We definiëren dan de *p-adische logaritme* van $x \in B = \{x \in \mathbb{Z}_p : |x-1|_p < 1\} = 1 + p\mathbb{Z}_p$ als

$$\log_p(x) := \log(1 + (x-1))\,.$$

Stelling 4.1.34. *Voor alle $a, b \in 1 + p\mathbb{Z}_p$ geldt*

$$\log_p(ab) = \log_p(a) + \log_p(b)\,.$$

Stel nu $p = 2$, dan is $-1 = 1 - p \in B$. Dus $2\log_2(1) = \log_2(-1) = 0$. Maar

$$\log_2(-1) = \log(1-2) = -\left(2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \dots\right) = 0\,.$$

De laatste gelijkheid is een limiet in $\mathbb{Q}_2$, equivalent met

$$\left|2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \dots\right|_2 = 0$$

of, voor elke $M \in \mathbb{N}$, bestaat er een $n \in \mathbb{N}$ zodat $2^M \mid 2 + \frac{2^2}{2} + \frac{2^3}{3} + \frac{2^4}{4} + \dots + \frac{2^n}{n}$.

Computeralgebra

De volgende stelling is zuiver algebraïsch en geeft het verband tussen de algebra van polynomen over $\mathbb{Z}_p$ en de eindige ringen $\mathbb{Z}/p^n\mathbb{Z}$.

Stelling 4.1.35 (Lemma van Hensel)**.** *Veronderstel dat $f(X) \in \mathbb{Z}_p[X]$, en veronderstel dat er polynomen $g_1(X), h_1(X) \in \mathbb{Z}_p[X]$ bestaan zodat $g_1(X)$ monisch is en $g_1(X)$ en $h_1(X)$ zijn relatief priem modulo p, en*

$$f(X) \equiv g_1(X)h_1(X) \pmod{p}$$

dan bestaan er polynomen $g(X), h(X) \in \mathbb{Z}_p[X]$ zodat $g_1(X) \equiv g(X) \pmod{p}$ en $h_1(X) \equiv h(X) \pmod{p}$ zodat

$$f(X) = g(X)h(X)\,.$$

Deze stelling is van fundamenteel belang in het vakgebied *computeralgebra*. We hebben gezien dat $\mathbb{Z}$ een UFD is, en dat ook $\mathbb{Z}[X]$ een UFD is. Twee polynomen $f(X)$ en $g(X)$ hebben dus een grootste gemene deler. Wanneer we $f(X)$ en $g(X)$ als polynomem over het breukenveld $\mathbb{Q}$ beschouwen, dan kunnen we een grootste gemene deler berekenen op een efficieënte wijze. Nadien kunnen we de gemeenschappelijke noemer van alle coëfficiënten bepalen en het resultaat in $\mathbb{Q}[X]$ daarmee vermenigvuldigen. Dit levert, op een eventuele factor uit $\mathbb{Z}$ na, een grootste gemene deler van f en g in $\mathbb{Z}[X]$. Men kan echter aantonen dat dit naieve algoritme niet efficiënt is.

We kunnen ook een priemgetal p kiezen, en f en g beschouwen als polynomen over het eindig veld $\mathbb{Z}/p\mathbb{Z}$. Via het uitgebreid algoritme van Euclides kunnen we nu opnieuw een grootste gemene deler bepalen. Deze is een gemeenschappelijke factor van f en g. Via het lemma van Hensel, dat ook in de praktijk geïmplementeerd kan worden, kan deze

factor als het ware gelift worden naar een factor over $\mathbb{Z}_p$. Omdat echter $f, g \in \mathbb{Z}[X]$, zal de gelifte factor ook behoren to $\mathbb{Z}[X]$. Men kan aantonen dat dit algoritme even efficiënt is als het uitgebried algoritme van Euclides en veel efficiënter dan het naieve algoritme.

Een tweede toepassing van ringtheorie vinden we in de ontwikkeling van snelle algoritmen voor de vermenigvuldiging van grote gehele getallen. Het is duidelijk dat een geheel getal voorgesteld kan worden als een polynoom over $\mathbb{Z}$ in $X = 2^{64}$. Van de gekende Fouriertransformatie bestaat ook een discrete variant. Net als de gekende Fouriertransformatie, zal de discrete Fouriertransformatie een convolutieproduct van polynomen omzetten in een puntsgewijze product, i.e. het polynoom dat men bekomt door de coëfficiënten van elke term te vermenigvuldigen. Nadien kan men het convolutieproduct vinden door de inverse discrete Fouriertransormatie uit te voeren. Merk op dat het convolutieproduct van twee polynomen over $\mathbb{Z}$ niets anders is dan het gewoon product modulo een polynoom van de vorm $x^n + 1$. Kiezen we n groot genoeg, dan is het convolutieproduct dus het gewoon product. Een belangrijke voorwaarde om de discrete Fouriertransformatie te kunnen uitvoeren in een polynomenring $R[X]$ is het bestaan van een zogenaamde primitieve $2n$-de eenheidswortel in R (waarbij n de graad van het polynoom is). Dit is problematisch in $\mathbb{Z}$. Men kan echter eenvoudig de algebraïsche uitbreiding $R := \mathbb{Z}[X]/(X^n + 1)$ beschouwen, en ten opzichte van deze ring de discrete Fouriertransformatie uitvoeren. Vanuit computationieel standpunt, is het rekenen in R echter niet zo eenvoudig, en dus niet zo efficiënt als in $\mathbb{Z}$. Enkele slimme observaties liggen echter aan de basis van het algoritme van Schönhage en Strassen, dat precies op onrechtstreekse wijze de berekeningen in R kan uitvoeren, en aldus op een snelle wijze polynomen over $\mathbb{Z}$ met elkaar kan vermenigvuldigen, waardoor ook grote gehele getallen met op efficiënte wijze met elkaar vermenigvuldigd kunnen worden. De essentie is hier dat precies de beschikbaarheid van de *abstracte* theorie van de ringuitbreidingen aan de basis ligt van efficiëntie algoritmen die dagelijks gebruikt worden.

Kwadratische vormen

Een laatste toepassing illustreert het zogenaamde local-global principe. We beginnen met een eerder verrassende toepassing van getaltheorie en kwadratische vormen in de incidentiemeetkunde.

Beschouw over $\mathbb{Q}_p$ de kwadratische vergelijking

$$aX^2 + bY^2 = Z^2 \,.$$

Het *Hilbertsymbool* $(a, b)_p$ is als volgt gedefinieerd: $(a, b)_p = 1$ als en slechts als bovenstaande vergelijking een niet triviale oplossing heeft, anders is $(a, b)_p = -1$. We kunnen bovenstaande vergelijking ook over $\mathbb{R}$ beschouwen, dan definiëren we het bijhorende

Hilbertsymbool met dezelfde betekenis en noteren het als $(a,b)_\infty$. Met de notatie (a,b) bedoelen we $(a,b)_v$, $v = p$ een priemgetal of $v = \infty$. Enkele eigenschappen kan men vrijwel onmiddellijk afleiden uit de definitie.

Lemma 4.1.36. *(i)* $(a,b) = (b,a)$

(ii) $(a,-a) = (a,1-a) = 1$

(iii) $(aa',b) = (a,b)(a',b)$ *en* $(a,bb') = (a,b)(a,b')$

Een aantal meer geavanceerde eigenschappen kan men bewijzen voor het Hilbertsymbool. De volgende stelling is een voorbeeld van het local-global principe. Informatie over een kwadratische vorm over $\mathbb{Q}$, kan verkregen worden door te kijken naar dezelfde vorm over $\mathbb{R}$ en $\mathbb{Q}_p$, voor alle priemgetallen p. Het volstaat daarbij doorgaans om maar enkele priemgetallen te gebruiken.

Stelling 4.1.37. *Voor* $a,b \in \mathbb{Q} \setminus \{0\}$ *geldt dat* $(a,b)_v = 1$ *voor bijna alle* v *en*

$$\prod_{v \in P} (a,b)_v = 1\,.$$

Het Hilbertsymbool wordt op een vernuftige wijze gebruikt in het bewijs van de zogenaamde stelling van Bruck-Ryser.

Stelling 4.1.38 (Bruck-Ryser)**.** *Als* $n \equiv 1,2 \pmod 4$*, en* n *is niet te schrijven als de som van twee kwadraten, dan bestaat er geen axiomatisch projectief vlak van orde* n*.*

De oorspronkelijke formulering van de stelling is iets ingewikkelder. Het originele bewijs maakt gebruik van invarianten van de incidentiematrix van een hypothetisch projectief vlak. Eén van die invarianten is gedefinieerd door middel van het Hilbertsymbool, en de bovenstaande voorwaarden zijn rechtstreeks af te leiden uit enkele (geavanceerde) eigenschappen van het Hilbertsymbool. De stelling van Bruck-Ryser sluit het bestaan van een projectief vlak van orde 6 uit, hetgeen gekend was door Euler. Het eerstvolgende geval dat uitgesloten wordt is $n = 14$. Het geval $n = 10$ wordt niet uitgesloten, maar werd uitgesloten door een totaal ander bewijs, geleverd door Lam. Het kleinste open geval is $n = 12$.

Ondertussen is er een alternatief bewijs gekend voor de stelling van Bruck-Ryser, gebaserd op de vierkwadratenstelling van Lagrange. Kwadratische vormen spelen echter ook onrechtstreeks een rol in het oorspronkelijke bewijs. Dit brengt ons bij een geavanceerder voorbeeld van het local-global principe, de zogenaamde stelling van Hasse-Minkowski.

Een bekende stelling over kwadratische vormen over $\mathbb{Q}$ is de volgende.

Stelling 4.1.39 (Hasse–Minkowski)**.** *Veronderstel dat* $F(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ *een homogeen polynoom van graad* 2 *is. De vergelijking*

$$F(X_1, X_2, \ldots, X_n) = 0$$

heeft niet-triviale oplossingen over $\mathbb{Q}$ *als en slechts als ze niet-triviale oplossingen heeft in* $\mathbb{Q}_p$*, voor elk priemgetal, en* $\mathbb{R}$*.*

De studie van kwadratische vormen over $\mathbb{Q}$ is heel ingewikkeld, terwijl het bestuderen van oplossingen van bovenstaande vergelijking over de reële getallen en over $\mathbb{Q}_p$ veel eenvoudiger is.

4.2 De stelling van Cayley-Hamilton

Veronderstel dat K een veld is, en V een n-dimensionale vectorruimte over K. We beschouwen een lineaire afbeelding $\varphi \in \mathrm{End}_K(V)$. Ten opzichte van een gekozen basis, wordt φ beschreven door een $n \times n$ matrix M. We definiëren de karakteristieke veelterm van φ als volgt:

$$P_\varphi(t) = \det(tI_n - M)\,.$$

Als N een inverteerbare $n \times n$ matrix is, dan rekent met eenvoudig na dat $\det(tI_n - N^{-1}MN) = \det(tI_n - M)$. Het karakteristiek polynoom is dus bepaald door φ en onafhankelijk van de keuze van een basis in V. De stelling van Cayley-Hamilton zegt precies dat elke matrix M die φ voorstelt ten opzichte van een gekozen basis, *voldoet aan de karakteristieke vergelijking van* φ, i.e. $P_\varphi(M) = 0$. Er bestaan enkele bewijzen van deze stelling die in meer of mindere mate afhankelijk zijn van het feit dat K een veld is. Nochtans geldt de stelling van Cayley-Hamilton ook voor R-lineaire afbeeldingen tussen vrije modulen over een commutatieve ring R.

Veronderstel dus dat R een commutatieve ring is, en E een vrij R-moduul van rang n, $\varphi \in \mathrm{End}_R(V)$. We hebben gezien dat vele beschouwingen over basisveranderingen en matrixvoorstellingen onveranderd blijven voor R-lineaire afbeeldingen tussen vrije R-modulen. We herhalen de belangrijkste eigenschap met betrekking tot determinanten. Voor een $n \times n$ matrix A over R geldt

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij})\,,$$

met A_{ij} de $(n-1) \times (n-1)$-matrix die we verkrijgen uit A door de i-de rij en de j-de kolom te schrappen. Verder kan men de zogenaamde regel van Cramer afleiden uit

$$A \,\mathrm{adj}(A) = \mathrm{adj}(A) A = \det(A) I\,,$$

met $\mathrm{adj}(A) = (b_{ij})$, en $b_{ij} = (-1)^{i+j} \det(A_{ji})$.

We zullen nu het R-moduul E interpreteren als een moduul over $R[t]$, de veeltermring in 1 veranderlijke over de ring R. Zoals we gezien hebben, is $\mathrm{End}_R(E)$ zelf een ring, en men kan eenvoudig nagaan dat $\theta : R[t] \to \mathrm{End}_R(E)$: $\theta(f(t)) \mapsto f(\varphi)$ een ringhomomorfisme is. De vermenigvuldiging van elementen uit E met ringelementen $f(t) \in R[t]$ definieert men als $f(t)v := f(\varphi)(v)$. Men gaat eenvoudig na dat met deze vermenigvuldiging, E een $R[t]$-moduul is. Omdat R ingebed wordt in $R[t]$ door θ, blijft E ook over $R[t]$ een vrij moduul van rang n. We kunnen dus werken met een basis van E.

Stelling 4.2.1 (Cayley-Hamilton)**.** *Voor een willekeurige afbeelding $\varphi \in \mathrm{End}_R(E)$ en een matrix A die φ voorstelt ten opzichte van een gekozen basis geldt $P_\varphi(A) = 0$.*

Bewijs. Kies een basis $B = \{v_1, \ldots, v_n\}$ voor het moduul E, en noem $A = (a_{ij})$ de matrix die φ voorstelt ten opzichte van B. Door de definite van E als $R[t]$-moduul geldt

$$tv_j = \sum_{i=1}^{n} a_{ij} v_i \,.$$

Definieer de matrix $B := tI_n - A$. De matrix B is een matrix over de ring $R[t]$, dus geldt $\mathrm{adj}(B)B = \det(B)I_n$. Merk op dat $\det(B) = P_\varphi(t)$. Nu geldt echter, met $B = (b_{ij})$,

$$\sum_{i=1}^{n} b_{ij} v_i = tv_j - \sum_{i=1}^{n} a_{ij} v_i = 0 \,. \tag{4.1}$$

Anderzijds geldt $B\mathrm{adj}(B) = \det(tI_n - A)I_n = P_\varphi(t)I_n$. Heel precies uitgedrukt, met $B = (b_{ij})$ en $\mathrm{adj}(B) = (c_{ij})$ geldt dus

$$\sum_{j=1}^{n} b_{ij} c_{jk} = P_\varphi(t)\delta_{ik} \,.$$

Combineren we dit met (4.1), en gebruiken we dat R een commutatieve ring is, dan vinden we

$$\sum_{j=1}^{n} c_{jk} \left(\sum_{i=1}^{n} b_{ij} v_i \right) = \left(\sum_{i=1}^{n} \sum_{j=1}^{n} b_{ij} c_{jk} \right) v_i = P_\varphi(t) v_k = 0 \,.$$

Dus voor de matrices $\mathrm{adj}(B)$ en B geldt $\mathrm{adj}(B)\, B = (c_{ij})$ met $c_{ij} = P_\varphi(t)\delta_{ij}$. Dus in E als $k[t]$-moduul geldt voor elk basiselement $P_\varphi(t)v_k = 0$, dus geldt $P_\varphi(t)x = 0$ voor elk moduulement $x \in E$. We besluiten dat $P_\varphi(A) = 0$ in de ring $R[A]$, of, met andere woorden, de matrix A voldoet aan zijn karakteristieke vergelijking. □

4.3 Exacte rijen en projectieve modulen

Veronderstel dat M, N, P en Q R-modulen zijn, en dat f, g, k, l R-moduul homomorfismen zijn:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle k} & & \downarrow{\scriptstyle l} \\ P & \xrightarrow{g} & Q \end{array}$$

Als $l \circ f = g \circ k$, dan zeggen we dat het *diagram commutatief* is. Beschouw nu een rij R-moduul homomorfismen

$$\cdots \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \xrightarrow{f_{i+2}} \cdots$$

De rij mag van eindige of oneindige lengte zijn. Als $f_{i+1} \circ f_i = 0$, voor elke i, dan noemen we de rij een *complex*. De rij is *exact* in M_i als $\mathrm{Im}\,(f_{i-1}) = \mathrm{Ker}\,(f_i)$. Als de rij overal exact is, dan spreken we gewoon van een *exacte rij*.

Voorbeelden 4.3.1.

1) De rij

$$0 \longrightarrow M \xrightarrow{f} N$$

is exact als en alleen als f injectief is. Immers, f is injectief als en slechts als $\mathrm{Ker}\,(f) = \{0\}$.

2) De rij

$$M \xrightarrow{f} N \longrightarrow 0$$

is exact als en alleen als f surjectief is. Immers, f is surjectief als en slechts als $\mathrm{Im}\,(f) = N$.

3) Een rij

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0 \tag{4.2}$$

is exact als en slechts als f injectief is, g surjectief en $\mathrm{Im}(f) = \mathrm{Ker}(g)$. Zo'n exacte rij heet een *korte exacte rij*. De volgende twee voorbeelden zijn hiervan specifieke gevallen.

4) Zij M en N twee R-modulen. Beschouw de rij

$$0 \longrightarrow M \xrightarrow{i_1} M \times N \xrightarrow{\pi_2} N \longrightarrow 0 \tag{4.3}$$

waarbij $i_1 : M \to M \times N$ de canonieke injectie is, gegeven door $i_1(m) = (m, 0)$, en $\pi_2 : M \times N \to N$ de canonieke projectie $\pi_2(m, n) = n$. De afbeeldingen $0 \to M$ en $N \to 0$ zijn de enige mogelijke, namelijk de canonieke injectie van het nulmoduul in M, en de afbeelding van N naar 0 die alles op 0 afbeeldt. De rij (4.3) is exact.

5) Neem $n \in \mathbb{Z}$. De rij

$$0 \longrightarrow n\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \tag{4.4}$$

is exact.

Stelling 4.3.2. *Zij k een veld en zij*

$$0 \longrightarrow V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} V_3 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-1}} V_n \longrightarrow 0$$

een exacte rij van eindigdimensionale vectorruimten over k. Dan is

$$\dim(V_1) - \dim(V_2) + \dim(V_3) - \cdots + (-1)^{n+1}\dim(V_n) = 0 \tag{4.5}$$

Bewijs. Uit de dimensieformule volgt

$$\begin{aligned}
\dim(V_1) &= \dim(\mathrm{Im}(f_1)),\\
\dim(V_2) &= \dim(\mathrm{Ker}(f_2)) + \dim(\mathrm{Im}(f_2)),\\
\dim(V_3) &= \dim(\mathrm{Ker}(f_3)) + \dim(\mathrm{Im}(f_3)),\\
&\vdots\\
\dim(V_{n-1}) &= \dim(\mathrm{Ker}(f_{n-1})) + \dim(\mathrm{Im}(f_{n-1})),\\
\dim(V_n) &= \dim(\ker(f_n)).
\end{aligned}$$

De stelling volgt als we deze formules alternerend optellen, en rekening houden met de eigenschap dat $\mathrm{Im}(f_{i-1}) = \mathrm{Ker}(f_i)$. □

Merk op dat een willekeurig epimorfisme $g: N \to N''$ altijd kan aangevuld worden tot een exacte rij (neem $N' = \mathrm{Ker}(g)$), en een willekeurig monomorfisme $f: N \to N''$ kan steeds worden aangevuld tot een exacte rij (neem $N'' = \mathrm{Coker}(f)$). We zeggen dat een korte exacte rij

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0 \tag{4.6}$$

een *gesplitste exacte rij* is, als ze op isomorfisme na van de vorm (4.3) is. D.w.z. als er een commutatief diagram bestaat van de vorm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N' & \xrightarrow{f} & N & \xrightarrow{g} & N'' & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle id_{N'}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle id_{N''}} & & \\
0 & \longrightarrow & N' & \longrightarrow & N' \times N'' & \longrightarrow & N'' & \longrightarrow & 0
\end{array} \tag{4.7}$$

waarbij $\phi: N \to N' \times N''$ een isomorfisme is. Hiervan kunnen we verschillende karakterisaties geven.

Stelling 4.3.3. *Onderstel dat (4.2) een exacte rij is. De volgende eigenschappen zijn equivalent:*

1) (4.2) is een gesplitste exacte rij;

2) g heeft een rechtsinverse (moduul homomorfisme) $k: N'' \to N$:

$$g \circ k = id_{N''};$$

3) f heeft een linksinverse (moduul homomorfisme) $l: N \to N'$:

$$l \circ f = id_{N'}.$$

Bewijs. 1) $\Rightarrow$ 2) en 1) $\Rightarrow$ 3) zijn triviaal.

2) $\Rightarrow$ 3) Zij $n \in N$. Dan is $n - k(g(n)) \in \mathrm{Ker}\,(g)$. Immers

$$g(n - k(g(n))) = g(n) - g(k(g(n)) = g(n) - g(n) = 0.$$

Omdat f injectief is bestaat er dus een unieke $n' \in N'$ zodat

$$f(n') = n - k(g(n)) \tag{4.8}$$

en we definiëren $l: N \to N'$ door $l(n) = n'$.

We beweren dat l lineair is. Inderdaad zij $n, m \in N$. Stel $l(n) = n'$ en $l(m) = m'$, zodat

$$f(n') = n - k(g(n)) \quad \text{en} \quad f(m') = m - k(g(m)).$$

Hieruit volgt onmiddellijk dat

$$f(rn' + sm') = rn + sm - k(g(rn + sm))$$

en $l(rn + sm) = rn' + sm' = rl(n) + sl(m)$.

We moeten nog bewijzen dat $l \circ f = id_{N'}$. Neem $x \in N'$, en schrijf $n = f(x)$. Dan is

$$n - k(g(n)) = n - k(g(f(x)) = n = f(x)$$

en dus is $x = l(n) = l(f(x))$. Hiermee is 2) $\Rightarrow$ 3) bewezen.

We merken voor later gebruik op dat $l \circ k = 0$. Inderdaad zij $n'' \in N''$ en stel $n = k(n'')$. Dan

$$n - k(g(n)) = k(n'') - k(g(k(n''))) = 0 = f(0)$$

en dus is $l(k(n'')) = l(n) = 0$. Uit (4.8) volgt ook nog dat

$$n = k(g(n)) + f(l(n)) \tag{4.9}$$

3) $\Rightarrow$ 2) Dit laten we als oefening aan de lezer. Het bewijs is analoog aan dat van 2) $\Rightarrow$ 3).

2) $\Rightarrow$ 1). We hebben reeds bewezen dat 3) volgt uit 2). Definieer $\phi : \ N \to N' \times N''$ door

$$\phi(n) = (l(n), g(n))$$

Het is duidelijk dat het diagram (4.7) commutatief is. Bovendien is ϕ een isomorfisme: de inverse afbeelding wordt gegeven door

$$\phi^{-1}(n', n'') = f(n') + k(n'')$$

Inderdaad,

$$\begin{aligned} \phi(\phi^{-1}(n', n'')) &= \phi(f(n') + k(n'')) \\ &= (l(f(n')) + l(k(n'')), g(f(n')) + g(k(n''))) \\ &= (n', n'') \end{aligned}$$

(merk op dat wij gebruik maakten van $l \circ k = 0$) en

$$\begin{aligned} \phi^{-1}(\phi(n)) &= \phi^{-1}(l(n), g(n)) \\ &= f(l(n)) + k(g(n)) = n \end{aligned}$$

waarbij we gebruik maakten van (4.9). □

In het bewijs van de vorige stelling hebben wij eigenlijk ook het volgende bewezen

Stelling 4.3.4. *Onderstel dat (4.2) een exacte rij is. De volgende eigenschappen zijn equivalent:*

1) (4.2) is een gesplitste exacte rij;

2) $\mathrm{Im}\,(f) = \mathrm{Ker}\,(g)$ *is een direct sommand van* N*, d.w.z., er bestaat een deelmoduul* D *van* N *zodat* $N = \mathrm{Im}\,(f) \oplus D$*.*

Uit Stelling 4.3.3 volgt dat de exacte rij (4.4) niet gesplitst is.

Definitie 4.3.5. We noemen een R-moduul M projectief als en alleen als volgende eigenschap geldt: als $g:\ N \to N''$ een epimorfisme is, en $\psi:\ M \to N''$ een homomorfisme is, dan bestaat er een homomorfisme $\phi:\ M \to N$ zodat $g \circ \phi = \psi$.

We kunnen de definitie op een aanschouwelijke manier als volgt herformuleren: elk diagram van de vorm

$$\begin{array}{ccccc} N & \xrightarrow{g} & N'' & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \psi} & & \\ & & M & & \end{array}$$

waarvan de bovenste rij exact is, kan aangevuld worden tot een commutatief diagram

$$\begin{array}{ccccc} N & \xrightarrow{g} & N'' & \longrightarrow & 0 \\ & \nwarrow^{\phi} & \uparrow{\scriptstyle \psi} & & \\ & & M & & \end{array}$$

Alvorens een voorbeeld te geven, veralgemenen we het begrip *vrij moduul*. Zij I een willekeurige index verzameling, en

$$R^I = \{(x_i)_{i\in I} \mid \#\{i \in I \mid x_i \neq 0\} \text{ eindig}\}$$

De componentsgewijze optelling en scalaire vermenigvuldiging maken van R^I een R-moduul, en we noemen R^I een vrij R-moduul. Als I eindig is, dan vinden we de definitie van een eindig voortgebracht vrij R-moduul terug. Voor elke $j \in I$ definiëren we $e_j \in R^I$ door

$$(e_j)_i = \delta_{ij}.$$

Elke $x = (x_i)_{i\in I} \in R^I$ kunnen we dan op een unieke manier schrijven als

$$x = \sum_{i\in I}{}' x_i e_i.$$

Het accent in de som herinnert ons eraan dat slechts een eindig aantal termen in de som verschillend van nul zijn. We kunnen dit nog herschrijven als volgt. Voor elke $j \in I$ definiëren we $\pi_j:\ R^I \to R$ door

$$\pi_j(x) = x_j.$$

Dan is

$$x = \sum_{j\in I}{}' \pi_j(x) e_j \tag{4.10}$$

Lemma 4.3.6. *Een vrij moduul is projectief.*

Bewijs. Zij $M = R^I$ een vrij R-moduul. Onderstel dat $g: N \to N''$ een epimorfisme is, en $\psi: M = R^I \to N''$ een homomorfisme. Voor elke $i \in I$ kiezen we $n_i \in N$ zodanig dat

$$g(n_i) = \psi(e_i)$$

en we definiëren $\phi: R^I \to N$ door

$$\phi(x) = \sum_{j\in I}{}' \pi_j(x) n_j.$$

Merk op dat dit goed gedefinieerd is. Bovendien is het duidelijk dat ϕ lineair is, en

$$\begin{aligned} g(\phi(x)) &= g\left(\sum_{j\in I}{}' \pi_j(x) n_j\right) \\ &= \sum_{j\in I}{}' \pi_j(x) g(n_j) \\ &= \sum_{j\in I}{}' \pi_j(x) \psi(e_j) \\ &= \psi\left(\sum_{j\in I}{}' \pi_j(x) e_j\right) = \psi(x) \end{aligned}$$

Dus is $g \circ \phi = \psi$, zoals gewenst. □

Voor een gegeven R-moduul M, en een R-lineaire afbeelding $f: L' \to L$ definiëren we

$$f_*: \mathrm{Hom}_R(M, L') \to \mathrm{Hom}_R(M, L)$$

door $f_*(\alpha) = f \circ \alpha$.

Stelling 4.3.7. *Voor een R-moduul M zijn de volgende eigenschappen equivalent.*

1) M is projectief.

2) voor elke exacte rij

$$0 \longrightarrow L' \xrightarrow{f} L \xrightarrow{g} L'' \longrightarrow 0 \tag{4.11}$$

is ook de rij

$$0 \longrightarrow \mathrm{Hom}_R(M, L') \xrightarrow{f_*} \mathrm{Hom}_R(M, L) \xrightarrow{g_*} \mathrm{Hom}_R(M, L'') \longrightarrow 0 \tag{4.12}$$

exact.

3) Elke korte exacte rij

$$0 \longrightarrow L \xrightarrow{f} N \xrightarrow{g} M \longrightarrow 0 \tag{4.13}$$

is gesplitst.

4) M is de directe summand van een vrij R-moduul. Dit wil zeggen dat er een vrij R-moduul R^I bestaat en een R-moduul N zodat $R^I \cong M \times N$.

Bewijs. 1) $\Longrightarrow$ 2). Onderstel dat (4.11) exact is. We moeten bewijzen dat ook (4.12) exact is. Hiervoor moeten wij vier eigenschappen van deze rij bewijzen.

Vooreerst tonen wij aan dat f_* injectief is. Onderstel dat

$$f_*(\alpha) = f \circ \alpha = 0.$$

Dus voor elke $m \in M$ geldt dat $f(\alpha(m)) = 0$. Omdat f injectief is, volgt er dat $\alpha(m) = 0$. Bijgevolg $\alpha = 0$.

Vervolgens tonen wij aan dat $g_* \circ f_* = 0$. Inderdaad, voor elke $\alpha \in \mathrm{Hom}_R(M, L')$ geldt dat

$$g_*(f_*(\alpha)) = g \circ f \circ \alpha = 0 \circ \alpha = 0.$$

Ten derde tonen wij aan dat $\mathrm{Im}\,(f_*) = \mathrm{Ker}\,(g_*)$. Een inclusie volgt uit het vorige. Voor de omgekeerde inclusie, stel $\beta \in \mathrm{Ker}\,(g_*)$. Dus, voor elke $m \in M$ geldt dat $g(\beta(m)) = 0$, zodat $\beta(m) \in \mathrm{Ker}\,(g) = \mathrm{Im}\,(f)$. Aangezien f injectief is, bestaat er dus een unieke $l' \in L'$ zodat $f(l') = \beta(m)$. Definieer

$$\alpha : \ M \to L'$$

door $\alpha(m) = l'$. Nu geldt $\beta(m) = f(l') = f(\alpha(m))$, en dus $\beta = f \circ \alpha$. We moeten enkel nog aantonen dat α lineair is (want dan $\beta \in \mathrm{Im}\,(f_*)$). Zij daarom $m_1, m_2 \in M$. Stel

$$\alpha(m_1) = l'_1 \ \text{ en } \ \alpha(m_2) = l'_2.$$

Dan,

$$f(l_1') = \beta(m_1) \quad \text{en} \quad f(l_2') = \beta(m_2)$$

en, voor elke $r, s \in R$:

$$f(rl_1' + sl_2') = rf(l_1') + sf(l_2') = r\beta(m_1) + s\beta(m_2) = \beta(rm_1 + sm_2).$$

Bijgevolg

$$\alpha(rm_1 + sm_2) = rl_1' + sl_2' = r\alpha(m_1) + s\alpha(m_2).$$

Uiteindelijk tonen wij aan dat g_* surjectief is. Zij daarom

$$\gamma \in \mathrm{Hom}_R(M, L'').$$

Vanwege de projectiviteit van M bestaat er een $\beta \in \mathrm{Hom}_R(M, L)$ zodat het volgende diagram commutatief is:

$$\begin{array}{ccccc} L & \xrightarrow{g} & L'' & \longrightarrow & 0 \\ & \nwarrow^{\beta} & \uparrow{\scriptstyle \gamma} & & \\ & & M & & \end{array}$$

We zien dat $\gamma = g \circ \beta = g_*(\beta)$, zoals gewenst.

2) $\Longrightarrow$ 1). Neem een diagram

$$\begin{array}{ccccc} N & \xrightarrow{g} & N'' & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \gamma} & & \\ & & M & & \end{array}$$

waarvan de bovenste rij exact is. We kunnen de bovenste rij aanvullen tot een korte exacte rij

$$0 \longrightarrow \mathrm{Ker}\,(g) = N' \longrightarrow N \xrightarrow{g} N'' \longrightarrow 0$$

en we hebben dus ook een korte exacte rij van de vorm (4.12). Omdat g_* surjectief is, bestaat er een $\alpha \in \mathrm{Hom}_R(M, N)$ zodat $\gamma = g_*(\alpha) = g \circ \alpha$. Deze α vervolledigt het commutatieve diagram.

1) $\Longrightarrow$ 3). We vervolledigen het diagram

$$\begin{array}{ccccc} N & \xrightarrow{g} & M & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle id_M} & & \\ & & M & & \end{array} \qquad \text{tot} \qquad \begin{array}{ccccc} N & \xrightarrow{g} & M & \longrightarrow & 0 \\ & \nwarrow^{k} & \uparrow{\scriptstyle id_M} & & \\ & & M & & \end{array}$$

Hieruit volgt onmiddellijk dat $g \circ k = I_M$, zodat g een rechtsinverse heeft. Uit Stelling 4.3.3 volgt dat de exacte rij (4.13) gesplitst is.

3) $\Longrightarrow$ 4). Zij $\{x_i \mid i \in I\}$ een stel voorbrengers voor M, en definieer $g: R^I \to M$ door

$$g(\sum_{i\in I}{}' r_i e_i) = \sum_{i\in I}{}' r_i x_i.$$

Het is duidelijk dat g lineair en surjectief is. Stel $N = \mathrm{Ker}\,(g)$, dan hebben wij de volgende korte exacte rij

$$0 \longrightarrow N \longrightarrow R^I \xrightarrow{g} M \longrightarrow 0$$

Deze is bij onderstelling gesplitst, en dus is $R^I \cong M \times N$.

4) $\Longrightarrow$ 1). Bekijk het commutatief diagram

$$\begin{array}{ccccc} N & \xrightarrow{g} & N'' & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \beta} & & \\ & & M & & \end{array}$$

Onderstel dat $M \times N \cong R^I$, en beschouw de canonieke injectie $i_1: M \to R^I$ en surjectie $p_1: R^I \to M$. We hebben dus volgend diagram

$$\begin{array}{ccccc} N & \xrightarrow{g} & N'' & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \beta} & & \\ & & M & & \\ & & {\scriptstyle i_1}\downarrow\uparrow{\scriptstyle p_1} & & \\ & & R^I & & \end{array}$$

Uit Lemma 4.3.6 weten we dat R^I projectief is. Er bestaat dus een lineaire afbeelding $\phi: R^I \to N$ zodat

$$g \circ \phi = \beta \circ p_1$$

Stel $\alpha = \phi \circ i_1: M \to N$. Dan is

$$g \circ \alpha = g \circ \phi \circ i_1 = \beta \circ p_1 \circ i_1 = \beta$$

□

Voor een R-moduul M schrijven we $\mathrm{Hom}_R(M, R) = M^*$. Voor $f \in M^*$ en $m \in M$ schrijven we ook

$$\langle f, m \rangle = f(m)$$

Stelling 4.3.8. *Een R-moduul M is projectief als en slechts als*

$$\{m_i \mid i \in I\} \subseteq M \text{ en } \{f_i \mid i \in I\} \subseteq M^*$$

bestaan zodat

a) $\{i \in I \mid \langle f_i, m\rangle \neq 0\}$ *is eindig, voor elke* $m \in M$*;*

b) voor elke $m \in M$ *geldt*

$$m = \sum_{i \in I} \langle f_i, m\rangle m_i. \tag{4.14}$$

We noemen $\{m_i, f_i \mid i \in I\}$ *een duale basis voor* M*. Als* M *eindig voortgebracht is, dan kunnen we* I *eindig nemen, en dan is ook* M^* *projectief indien* R *ook commutatief is. Bovendien is dan* $\{f_i, m_i \mid i \in I\}$ *een duale basis voor* M^**, en*

$$f = \sum_{i \in I} \langle f, m_i\rangle f_i \tag{4.15}$$

voor elke $f \in M^*$*.*

Bewijs. Onderstel eerst dat M projectief is. We weten dat M een directe summand van een vrij R-moduul R^I is. Zij dus N een R-moduul zodat

$$R^I \cong M \times N.$$

Uit (4.10) weten we dat

$$x = \sum_{j \in I}{}' \pi_j(x) e_j \tag{4.16}$$

wat in feite zegt dat $\{e_j, \pi_j \mid j \in I\}$ een duale basis is voor R^I. Zoals voorheen zijn $i_1 : M \to R^I$ en $p_1 : R^I \to M$ de canonieke injectie en surjectie. Voor elke $i \in I$, stel

$$m_i = p_1(e_i) \text{ en } f_i = \pi_i \circ i_1.$$

Voor elke $m \in M$ geldt dat

$$\{i \in I \mid f_i(m) \neq 0\} = \{i \in I \mid \pi_i(i_1(m)) \neq 0\}$$

eindig is. Immers, $i_1(m) \in R^I$ heeft slechts een eindig aantal van nul verschillende

componenten. Bovendien,

$$\begin{aligned}\sum_{i\in I}{}'\langle f_i, m\rangle m_i &= \sum_{i\in I}{}'\pi_i(i_1(m))\; p_1(e_i)\\ &= p_1\left(\sum_{i\in I}{}'\langle \pi_i, i_1(m)\rangle e_i\right) \qquad (p_1 \text{ is } R\text{-lineair})\\ &= p_1(i_1(m))\\ &= m\end{aligned}$$

Omgekeerd, onderstel dat $\{m_i, f_i \mid i \in I\}$ een duale basis is voor M. Definieer $i_1 :\ M \to R^I$ en $p_1 :\ R^I \to M$ door

$$i_1(m) = \sum_{i\in I}{}'\langle f_i, m\rangle e_i \ \text{ en } \ p_1(x) = \sum_{i\in I}{}'\langle \pi_i, x\rangle m_i.$$

Duidelijk zijn deze functies R-lineair. Bovendien, voor elke $m \in M$ geldt dat

$$\begin{aligned}p_1(i_1(m)) &= p_1\left(\sum_{i\in I}{}'\langle f_i, m\rangle e_i\right)\\ &= \sum_{i\in I}{}'\langle f_i, m\rangle\langle p_1, e_i\rangle\\ &= \sum_{i\in I}{}'\sum_{j\in I}{}'\langle f_i, m\rangle\langle \pi_j, e_i\rangle m_j\\ &= \sum_{i\in I}{}'\sum_{j\in I}{}'\langle f_i, m\rangle\delta_{ij} m_j\\ &= \sum_{i\in I}{}'\langle f_i, m\rangle m_i = m\end{aligned}$$

Dus is

$$0 \longrightarrow \mathrm{Ker}p_1 \longrightarrow R^I \xrightarrow{p_1} M \longrightarrow 0$$

een gesplitste exacte rij en $R^I \cong M \times \mathrm{Ker}p_1$. Als M eindig voortgebracht is, dan kunnen we $I = \{1, \ldots, n\}$ nemen. Indien bovendien R commutatief is, dan voor elke $f \in M^*$

en elke $m \in M$ geldt:

$$\begin{aligned}\left\langle \sum_{i=1}^{n} \langle f, m_i \rangle f_i, m \right\rangle &= \sum_{i=1}^{n} \langle f, m_i \rangle \langle f_i, m \rangle \\ &= \left\langle f, \sum_{i=1}^{n} \langle f_i, m \rangle m_i \right\rangle \\ &= \langle f, m \rangle\end{aligned}$$

zodat

$$\sum_{i=1}^{n} \langle f, m_i \rangle f_i = f$$

□

Voorbeeld 4.3.9. Stel

$$R = \mathbb{Z}[i\sqrt{5}] = \{r + si\sqrt{5} \mid r, s \in \mathbb{Z}\} \cong \mathbb{Z}[X]/(X^2 + 5)$$

a) R is geen UFD. Om dit in te zien merken we eerst op dat 1 en -1 de enige inverteerbare elementen van R zijn. We beschouwen de afbeeldingen

$$N : \ \mathbb{C} \to \mathbb{R}^+ : \ x + iy \mapsto x^2 + y^2$$

N is multiplicatief: $N(zz') = N(z)N(z')$, en beperkt zich tot een afbeelding $N : \ R \to \mathbb{N}$. In R geldt dat

$$6 = 2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

We beweren dat $2, 3, 1 + i\sqrt{5}$ en $1 - i\sqrt{5}$ allen irreducibel zijn. Als dit het geval is, dan hebben we twee verschillende ontbindingen van 6 in irreducibele elementen, zodat R geen UFD is.

Als $2 = ab$, met a en b niet inverteerbaar, dan is $N(2) = N(a)N(b) = 4$. De enige elementen van R die door N op 1 worden afgebeeld zijn 1 en -1, de inverteerbare elementen van R. Het is dus onmogelijk dat $N(a) = 1$ of $N(b) = 1$, en dus is $N(a) = N(b) = 2$. Stel $a = u + vi\sqrt{5}$. Dan is $N(a) = u^2 + 5v^2 = 2$, maar deze vergelijking heeft geen oplossingen in $\mathbb{Z}$. De andere elementen behandelt men op een analoge manier.

b) Bekijk nu het ideaal

$$I = (2, 1 + i\sqrt{5}) = \{2r + s + si\sqrt{5} \mid r, s \in \mathbb{Z}\}$$

We beweren nu dat I, bekeken als R-moduul, projectief is. Om dit aan te tonen volstaat het om te bewijzen dat de surjectieve lineaire afbeelding

$$g : \ R^2 \to I$$

gedefinieerd door

$$g\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 2 \;\; ; \;\; g\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1 + i\sqrt{5}$$

een rechtsinverse lineaire afbeelding $k: \; I \to R^2$ heeft. Zulk een k wordt gegeven door de formule

$$k(x) = \frac{x}{2}\begin{pmatrix} 1 - 3i\sqrt{5} \\ 5 + i\sqrt{5} \end{pmatrix}$$

Immers, k is welgedefinieerd aangezien

$$k(2) = \begin{pmatrix} 1 - 3i\sqrt{5} \\ 5 + i\sqrt{5} \end{pmatrix}, \; k(1 + i\sqrt{5}) = \begin{pmatrix} 8 - 2i\sqrt{5} \\ 3i\sqrt{5} \end{pmatrix} \in R^2$$

en het is eenvoudig na te gaan dat $g(k(x)) = x$, voor elke $x \in I$.

c) Gebruik makend van het bewijs van Stelling 4.3.7 en Stelling 4.3.8 vinden we nu ook een duale basis voor I:

$$\{m_i, f_i \mid i = 1, 2\}$$

gegeven door

$$\begin{array}{cc} m_1 = 2 & m_2 = 1 + i\sqrt{5} \\ f_1(x) = (1 - 3i\sqrt{5})x/2 & f_2(x) = (5 + i\sqrt{5})x/2 \end{array}$$

Ga zelf na dat

$$f_1(m)m_1 + f_2(m)m_2 = m$$

voor elke $m = 2r + s + si\sqrt{5} \in I$.

d) I is geen vrij R-moduul, zodat we een voorbeeld hebben van een projectief moduul dat niet vrij is. Om dit te kunnen aantonen hebben we eerst een andere eigenschap nodig die ook op zichzelf belangrijk is.

Onderstel dat R een commutatieve ring is, en neem twee verschillende natuurlijke getallen n en m. Is het mogelijk om een isomorfisme $f: \; R^n \to R^m$ te vinden? Als R een veld is, dan is het antwoord negatief: dit is de stelling die zegt dat alle basissen van een eindigdimensionale vectorruimte eenzelfde aantal elementen bevatten. Alvorens we dezelfde eigenschap kunnen bewijzen voor een eindig voortgebracht vrij moduul, hebben we eerst een lemma nodig.

Lemma 4.3.10. *Zij R een commutatieve ring. Als $R^n \cong K \times R^n$, dan is $K = 0$.*

Bewijs. Omdat $R^n \cong K \times R^n$ en R^n vrij is, en dus projectief, hebben we een gesplitste exacte rij

$$0 \longrightarrow K \xrightarrow{f} R^n \xrightarrow{g} R^n \longrightarrow 0$$

Zij k de rechtsinverse van g, dit wil zeggen dat $g \circ k = id_{R^n}$. Beschouw nu de matrices $A, B \in \mathrm{M}_{nn}(R)$ van k en g tenopzichte van de standaardbasis van R^n. Dan is $BA = I_n$, en $\det(B)\det(A) = 1$, zodat $\det(A)$ inverteerbaar is in R. Dit betekent dat A een inverteerbare matrix is (zie (3.9)) en dat g een isomorfisme is. Bijgevolg is g injectief, en dus is $K = 0$. □

Stelling 4.3.11. *Als $f : R^n \to R^m$ een epimorfisme is, dan is $n \geq m$. Als f een isomorfisme is dan $n = m$.*

Bewijs. Stel $K = \mathrm{Ker}\,(f)$. De exacte rij

$$0 \longrightarrow K \longrightarrow R^n \xrightarrow{f} R^m \longrightarrow 0$$

splitst (omdat R^n projectief is) , zodat $R^n \cong K \times R^m$. Als $m > n$, dan vinden we

$$R^n \cong K \times R^{m-n} \times R^n$$

en uit Lemma 4.3.10 volgt dat $K \times R^{m-n} = 0$. Dit kan alleen als $K = 0$ en $m = n$, een contradictie.

Als nu f een isomorfisme is, dan is ook f^{-1} een isomorfisme. Bijgevolg verkrijgen wij het eerste gedeelte dat $n = m$. □

Als M een eindig voortgebracht vrij R-moduul is, isomorf met R^n, dan zeggen we dat M vrij is van *rang* n. Door Stelling 4.3.11 is de rang van een eindig voortgebracht vrij moduul over een commutatieve ring welgedefinieerd.

We keren nu terug naar Voorbeeld 4.3.9, en tonen aan dat I niet vrij is. Onderstel dat I vrij is. Omdat we een epimorfisme $g : R^2 \to I$ hebben, is de rang van I ten hoogste 2, door Stelling 4.3.11.

Als de rang van I gelijk is aan 1, dan is I een hoofdideaal. Verifieer zelf dat dit onmogelijk is.

Als $I \cong R^2$, dan is, alweer door Stelling 4.3.11, g een isomorfisme. Er volgt dat $\{m_1, m_2\}$ een basis van I is, en dit impliceert tevens dat $f_i(m_j) = \delta_{ij}$. Het is eenvoudig in te zien dat dit niet het geval is.

Hoofdstuk 5

Oefeningen

5.1 Vectorruimten

5.1.1. Gegeven twee niet-ledige verzamelingen S en T. (i) Gebruik Lemma 1.6.4 om aan te tonen dat er een isomorfisme

$$\tilde{f} : F(S) \otimes F(T) \to F(S \times T)$$

bestaat.
(ii) Je kan ook dit isomorfisme onmiddellijk opschrijven aan de hand van Stelling 1.6.3.

5.1.2. Gegeven drie vectorruimten V_1, V_2 en V_3 over hetzelfde veld K. (i). Schrijf een basis op voor $F = (V_1 \otimes V_2) \otimes V_3$ en $G = V_1 \otimes (V_2 \otimes V_3)$.
(ii) Zijn F en G isomorf? Zo ja, beschrijf een isomorfisme.
(iii). Toon aan dat er een uniek isomorfisme $\tilde{f}$ bestaat zodat

$$\tilde{f}((x \otimes y) \otimes z) = x \otimes (y \otimes z)\,,$$

voor alle $x \in V_1$, $y \in V_2$, $z \in V_3$.

5.2 Herhalingsoefeningen groepentheorie

5.2.1. Toon aan dat $\{\mathbb{R} \to \mathbb{R} : x \mapsto ax + b \mid a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}\}$ een groep voor de samenstelling van functies.

5.2.2. Bepaal alle deelgroepen van $(\mathbf{Z}, +)$. Hoeveel nevenklassen in $(\mathbf{Z}, +)$ heeft zo een deelgroep?

5.2.3. Zij f_1 en f_2 twee homomorfismen van de groep $(G, \cdot)$ in de groep $(H, *)$ en zij $K = \{x \in G \mid f_1(x) = f_2(x)\}$. Is K een deelgroep van G? Als zo, is K dan een normale deelgroep?

5.2.4. Bewijs de volgende eigenschap. Als φ een isomorfisme (d.w.z. een bijectief homomorfisme) van groepen is, dan is φ^{-1} er ook één.

5.2.5. Bewijs dat $(\mathbb{R}, +)$ en $(\mathbb{R}^+ \setminus \{0\}, .)$ isomorfe groepen zijn.

5.2.6. Bewijs dat $(\mathbb{R}_0, \cdot)$ en $(\mathbf{Z_2}, +) \times (\mathbb{R}_{\mathbf{0}}^+, \cdot)$ isomorfe groepen zijn.

5.2.7. Bewijs dat $(\mathbf{C_0}, \cdot)$ en $(S, \cdot) \times (\mathbb{R}_0^+; \cdot)$ isomorfe groepen zijn, waar S is gedefinieerd door $S = \{z \in \mathbf{C} \mid |\mathbf{z}| = \mathbf{1}\}$.

5.2.8. Ga na dat

$$det : GL_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$$

een homomorfisme is en bepaal zijn kern.

5.2.9. (Cayley) Zij G een groep. Voor elke g in G, definieer

$$\begin{aligned} r_g : G \to G &: x \mapsto xg \\ l_g : G \to G &: x \mapsto gx \end{aligned}$$

Zij $R = \{r_g \mid g \in G\}$ en $L = \{l_g \mid g \in G\}$. Bewijs dat R en L isomorfe deelgroepen van $\mathrm{Sym}(G)$ zijn.

5.2.10. Zij G een groep. Voor $g \in G$ definieer

$$\lambda_g : G \to G : x \mapsto gxg^{-1}$$

Bewijs dat λ_g een automorfisme van G is (men noemt dit het inwendig automorfisme (van G) bepaald door g).

5.2.11. Bepaal de conjugatieklassen van $Sym(E)$ als
a) $|E| = 3$.
b) $|E| = 4$.
c) $|E| = 5$.

5.2.12. Zij $(Q_8, \cdot) = (\{1, -1, i, -i, j, -j, k, -k\}, \cdot)$. Bepaal $Inn(Q_8, \cdot)$, $Z(Q_8, \cdot)$ en alle conjugatieklassen van $(Q_8, \cdot)$.

5.2.13. Hebben twee geconjugeerde elementen in een groep G noodzakelijkerwijs dezelfde orde? Is de invers waar?

5.2.14. Een deelgroep N van een groep G heet een normale deelgroep als $\lambda_g(N) = N$ voor elke $g \in G$. Bewijs dat N een normale deelgroep is van G als en slechts als $\lambda_g(N) \subset N$, $\forall g \in G$.

5.2.15. Zij G een groep en $\mathrm{Inn}(G) = \{\lambda_g \mid g \in G\}$. Bewijs dat $\mathrm{Inn}(G)$ een normale deelgroep is van $\mathrm{Aut}(G)$.

5.2.16. Zij $\varphi : G \to G'$ een homomorfisme van groepen. Bewijs dat de kern van φ een normale deelgroep is van G.

5.2.17. Zij H een deelgroep van G. Bewijs dat

$$\frac{G}{H} = \{gH \mid g \in G\}$$

een partitie is van G.

5.2.18. Zij N een normale deelgroep van G. Bewijs dat $\frac{G}{N}$ een groep is voor de welgedefinieerde (ga na!) bewerking $(g_1N)(g_2N) = g_1g_2N$.

5.2.19. Bewijs:

$$(\frac{\mathbf{Z}}{6\mathbf{Z}}, +) \ \cong \ (\frac{\mathbf{Z}}{7\mathbf{Z}} \setminus \{0\}, .)$$

5.2.20. Zij $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid det(A) = 1\}$. Bepaal $\frac{GL_2(\mathbb{R})}{SL_2(\mathbb{R})}$.

5.2.21. Zij $H = \{(4z, 6z) \mid z \in \mathbf{Z}\}$ een deelgroep van $(\mathbf{Z^2}, +)$. Gebruik het groephomomorfisme $f : (\mathbf{Z^2}, +) \to (\mathbf{Z}, +) \times (\mathbf{Z_2}, +) : (\mathbf{a}, \mathbf{b}) \mapsto (\mathbf{3a - 2b}, \mathbf{b_2})$ (b_2 staat voor de rest na deling van b door 2) en de eerste Isomorfismestelling om $(\frac{\mathbf{Z^2}}{H}, +)$ te bepalen.

5.2.22. Zij N een normale deelgroep van G. Bewijs de volgende stelling. Voor elk groepshomomorfisme $\phi : G \to L$ met $\phi(N) = 1$ bestaat er precies één homomorfisme $\phi' : \frac{G}{N} \to L$ zodanig dat $\phi = \phi' \circ p$, waarbij $p : G \to \frac{G}{N}$ de canonische projectie is.

5.2.23. (Isomorfismestelling) Zij $\phi : G \to L$ een epimorfisme (surjectief homomorfisme) met kern N. Toon aan dat er een uniek isomorfisme $\phi' : \frac{G}{N} \to L$ bestaat zodanig dat $\phi = \phi' \circ p$.

5.2.24. Bepaal $\frac{\mathbb{R}}{\mathbf{Z}}$. (Hint: $\mathbb{R} \to \mathbf{C} : x \mapsto e^{i2\pi x}$)

5.3 Representaties

Zij G een *eindige* groep en K een veld. Laat K^* de niet nulle elementen van K voorstellen.

1. Zij $\rho : G \to \mathrm{GL}_n(K)$ een representatie. Toon aan dat $G \to K^* : g \longmapsto \det(\rho(g))$ een representatie van graad 1 is.
2. Zij G' de commutatordeelgroep van G, i.e. de deelgroep voortgebracht door alle commutatoren $ghg^{-1}h^{-1}$ met $g, h \in G$.
   (a) Toon aan dat G' normaal is.
   (b) Geef een 1-1 verband tussen

- de representaties van G van graad 1
- de representaties van G/G' van graad 1.

3. Zij $\eta = e^{2\pi i/n}$. Beschouw de matrices $A = \begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}$ en $B = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. Toon dat
$$a \longmapsto A \, , b \longmapsto B$$
kan worden uitgebreid tot een trouwe complexe representatie van $D_{2n} = \langle a, b \,|\, a^n = 1 = b^2, ba = a^{-1}b \rangle$.

4. Beschouw de matrices $A = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$, $B_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $B_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Toon dat (voor $i = 1, 2$)
$$a \longmapsto A \, , b \longmapsto B_i$$
kan worden uitgebreid tot een trouwe reële representatie van $D_{2n} = \langle a, b \,|\, a^n = 1 = b^2, ba = a^{-1}b \rangle$.

5. Toon aan dat $S_n \to \mathbb{R}^* : \sigma \to \text{sgn}(\sigma)$ een reële representatie van graad 1 definieert van S_n.

6. Beschouw de canonische actie van S_3 op $X = \{1, 2, 3\}$, i.e. $1 : S_3 \to S_3 = \text{Sym}(X) : \sigma \longmapsto \sigma$. Zij $\rho : S_3 \to \text{GL}(V)$ de geassocieerde reële permutatierepresentatie op $V = \oplus_{i=1}^3 \mathbb{R}e_i$.
   (a) Is de representatie trouw?
   (b) Wat is het karakter $\chi((12))$?
   (c) Geef een 1-dimensionale S_3-invariante deelruimte V_1 en een 2-dimensionale S_3-invariante deelruimte V_2.
   (d) Is de geïnduceerde representatie $\rho_2 : S_3 \to \text{GL}(V_2)$ irreducibel?
   (e) Is de complexe representatie $\rho_{2,\mathbb{C}} : S_3 \to \text{GL}_2(\mathbb{C})$ met dezelfde matrixvoorstelling als ρ_2 irreducibel?
   (f) Schrijf het karakter van de complexe representatie $\rho_{\mathbb{C}} : G \to \text{GL}_3(\mathbb{C})$ als een som van irreducibele complexe karakters.

7. Zij G de deelgroep van S_5 voortgebracht door (123) en (45) en beschouw haar canonische actie op $X = \{1, 2, 3, 4, 5\}$. Zij $\rho_{\mathbb{R}} : G \to \text{GL}(V_{\mathbb{R}})$ de geassocieerde reële permutatierepresentatie op $V_{\mathbb{R}} = \oplus_{i=1}^5 \mathbb{R}e_i$ en zij $\rho_{\mathbb{C}} : G \to \text{GL}(V_{\mathbb{C}})$ de geassocieerde complexe permutatierepresentatie op $V_{\mathbb{C}} = \oplus_{i=1}^5 \mathbb{C}e_i$.

(a) Zijn de representaties trouw?

(b) Wat is het karakter $\chi((123))$?

(c) Volgens de stelling van Maschke zijn beide representaties volledig reducibel. Schrijf $\rho_{\mathbb{R}}$ en $\rho_{\mathbb{C}}$ elk als directe som van irreducibele representaties.

(d) Geef de complexe karaktertabel van G.

(e) Schrijf het karakter $\chi_{\mathbb{C}}$ van $\rho_{\mathbb{C}}$ als een som van irreducibele karakters.

8. Beschouw de matrix $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(a) Toon aan dat

$$\rho_{\mathbb{R}} : \mathbb{Z}_{20} \to \mathrm{GL}_2(\mathbb{R}) : [n] \longmapsto A^n$$

een representatie is. Is ze trouw? Is ze irreducibel? Zo ja, bewijs. Zo neen, geef een ontbinding in irreducibele deelrepresentaties.

(b) Zelfde vraag voor $\rho_{\mathbb{C}} : \mathbb{Z}_{20} \to \mathrm{GL}_2(\mathbb{C}) : [n] \longmapsto A^n$.

9. Bepaal de complexe karaktertabel van volgende groepen:

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2$

(b) $\mathbb{Z}_2 \times \mathbb{Z}_3$

(c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

10. (a) Bepaal de complexe karaktertabel van D_8.

(b) Bepaal de karakters van de representaties uit oefening 3 en 4 voor $n = 4$. Zijn het irreducibele complexe karakters?

11. (a) A_4 is isomorf met de groep van ruimte symmetrieën van een reguliere tetraeder (zie vorig jaar). Dit definieert een natuurlijke representatie van A_4 van graad 3. Bepaal het karakter van deze representatie. Is dit een irreducibel complex karakter?
HINT: Kies een basis van $\mathbb{R}^3$ met de oorspong binnenin de tetraeder en zo dat de coördinaatassen door de middelpunten van drie ribben grenzend aan eenzelfde hoekpunt gaan.

(b) A_4 heeft een normale deelgroep $N = \{1, (12)(34), (13)(24), (14)(23)\}$. Het quotient A_4/N is een gekende groep. Via $A_4 \to A_4/N$ geeft elke representatie van A_4/N aanleiding tot een representatie van A_4. Bepaal de irreducibele complexe karakters van A_4/N. Geven ze aanleiding tot irreducibele complexe karakters van A_4?

(c) Bepaal de complexe karaktertabel van A_4.

12. (a) S_4 is isomorf met de groep van ruimte symmetrieën van een kubus (zie vorig jaar). Dit definieert een natuurlijke representatie van S_4 van graad 3. Bepaal het karakter van deze representatie. Is het een irreducibel complex karakter?

    (b) S_4 heeft een normale deelgroep $N = \{1, (12)(34), (13)(24), (14)(23)\}$. Het quotient S_4/N is een gekende groep. Via $S_4 \to S_4/N$ geeft elke representatie van S_4/N aanleiding tot een representatie van S_4. Bepaal de irreducibele complexe karakters van S_4/N. Geven ze aanleiding tot irreducibele complexe karakters van S_4?

    (c) Bepaal de complexe karaktertabel van S_4.

13. Zij V een K-vectorruimte en

$$\rho : G \to \mathrm{GL}(V) : g \longmapsto \rho_g$$

een representatie met karakter χ. Zij V' de duale vectorruimte van V, i.e. $V' = \mathrm{Hom}_K(V, K)$. Toon dat er een unieke representatie

$$\rho' : G \to \mathrm{GL}(V') : g \longmapsto \rho'_g$$

bestaat met

$$(\rho'_g(x'))(\rho_g(x)) = x'(x)$$

voor alle $g \in G$, $x \in V$ en $x' \in V'$. We noemen ρ' de *duale representatie* van ρ. Bepaal het karakter χ' van ρ'.

14. Zij χ een complex karakter van G met $\chi(g) = 0$ voor alle $g \neq 1$. Toon aan dat χ een geheel veelvoud is van het karakter van de reguliere representatie van G.

15. Zij ρ een irreducibele complexe representatie van G van graad n met karakter χ. Zij C het centrum van G. Toon volgende beweringen aan:

    (a) ρ_g is een homothetie voor elke $g \in C$.

    (b) $|\chi(g)| = n$ voor elke $g \in C$.

    (c) $n^2 \leq |G|/|C|$.

    (d) Als G abels is zijn alle irreducibele representaties van graad 1.

    (e) Als ρ trouw is, dan is C een cyclische groep.

16. (a) Toon aan dat de verzameling $\hat{G}$ van alle irreducibele karakters van een *abelse* groep G een groep vormt voor de puntsgewijze vermenigvuldiging

$$\chi_1\chi_2(g) = \chi_1(g)\chi_2(g).$$

Deze groep $\hat{G}$ wordt de *duale groep van* G genoemd.

(b) Zijn G en $\hat{G}$ isomorfe groepen?

17. Beschouw een actie $\alpha : G \times X \to X : (g, x) \longmapsto gx$ van G op een eindige verzameling X. Voor $x \in X$ noteren we $G_x = \{g \in G \mid gx = x\} \subset G$ (dit is de *stabilisator* van x), $G(x) = \{gx \mid g \in G\} \subset X$ (dit is de *baan* van x) en voor $g \in G$ noteren we $\mathsf{Fix}(g) = \{x \in X \mid g(x) = x\} \subset X$ (dit zijn de *fixpunten* van g). Zij c het aantal banen van de actie α. Beschouw de permutatierepresentatie ρ met karakter χ geassocieerd aan α.

(a) Toon dat $\chi(g) = |\mathsf{Fix}(g)|$.

(b) Toon dat het aantal keer dat de triviale representatie 1 voorkomt in (de ontbinding in irreducibele representaties van) de representatie ρ gelijk is aan c.

HINT: Beschouw $R \subset X \times G$ waarvoor $(x, g) \in R \iff g(x) = x$. Door op twee manieren het aantal elementen van R te tellen, en gebruik te maken van de orbiet-stabilisator stelling, vind je een uitdrukking voor c (dit is het zgn. Lemma van Burnside).

(c) Beschouw de actie β van G op het produkt $X \times X$ gegeven door $g(x, y) = (gx, gy)$. Wat is het karakter van de overeenkomstige permutatierepresentatie?

(d) Veronderstel dat $c = 1$ (de actie α heet dan *transitief*). Schrijf $\rho = 1 \oplus \theta$. We noemen α *dubbel transitief* als voor elke $x \neq y$ en $x' \neq y'$ in X een $g \in G$ bestaat met $gx = x'$ en $gy = y'$. Toon dat volgende eigenschappen equivalent zijn:

i. α is dubbel transitief.

ii. β heeft twee banen: de diagonaal en haar complement.

iii. $\langle \chi^2 \mid 1 \rangle = 2$.

iv. θ is irreducibel.

5.4 Ringen

5.4.1. Zij R een ring, $a, b, c \in$ en $a = bc$.

1. Als b en c inverteerbaar zijn, dan is ook a en inverteerbaar en $a^{-1} = \cdots$?

2. Onderstel dat a inverteerbaar is. Als R ofwel commutatief, of een lichaam of een matrix ring over een veld is, bewijs dat dan ook b en c inverteerbaar zijn.

3. Zij $V = \mathbf{C}^{\mathbf{N}}$ en $R = \mathrm{End}_{\mathbf{C}}(V)$. Zij $f : V \to V : (x_0, x_1, x_2, \cdots) \mapsto (0, x_0, x_1, x_2, \cdots)$ en $g : V \to V : (x_0, x_1, x_2, \cdots) \mapsto (x_1, x_2, \cdots)$. Zijn $f \circ g$, $g \circ f$, f en g inverteerbaar in R?

5.4.2. Zij $q = 2 + i + 2j \in \mathbf{H} = \mathbf{H}(\mathbb{R})$.

1. Bereken q^{-1}.

2. Ga na dat $f : \mathbf{H} \to \mathbf{H} : x \mapsto qxq^{-1}$ $\mathbb{R}$-lineair is. Bepaal de matrix van f ten opzichte van de basis $\{1, i, j, k\}$ van $\mathbf{H}$.

5.4.3. Stel $K = \{a + b\sqrt{3} \mid a, b \in rat\}$. Dus $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$.

1. Toon aan dat K een veld is, en dat $p(X) = X^2 - 3$ en $X^2 - 75$ factoriseerbaar zijn in $K[X]$.

2. Toon aan dat $f : K \to K : a + b\sqrt{3} \mapsto a - b\sqrt{3}$ een automorfisme is van K. Is f continu, als K als metrische deelruimte van $\mathbb{R}$ opgevat wordt? Heeft K nog andere automorfismen buiten 1_K en f?

5.4.4. Beschouw $R = M_2(\mathbb{R})$ (dus $R \cong \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$).

1. R is een reële vectorruimte, alsook een ring met éénheidselement $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$. Als $x \in R$, bewijs dan dat $1 \cdots I$ (de scalaire vermenigvuldiging) hetzelfde is als $I \cdot x$ (het produkt in R).

2. Indien $L \subseteq R$ een links ideaal is, dan is L ook een deelruimte (analoog rechts; a fortiori tweezijdig).

3. $L = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$ is een links ideaal van R. Heeft R nog veel andere linkse idealen?

4. Zij $f, g \in R$. Bewijs dat $\ker(f \circ g) \subseteq \ker(g)$.

5. Geef een voorbeeld van een rechts ideaal van R dat geen links ideaal is.

6. Bewijs dat $\{0\}$ en R de enige tweezijdige idealen zijn van R (d.w.z. R is een eenvoudige ring).

7. Zij K een veld en V een eindig dimensionale K-vectorruimte. Als $V \neq \{0\}$, bewijs dat $\mathrm{End}_K(V)$ een eenvoudige ring is.

5.4.5. Zij $R = M_2(\mathbb{Q})$.

1. Als $z \in R$, toon aan dat $\text{rang}(z) \leq 1$ als en slechts als $z = \begin{bmatrix} ac & ad \\ bc & bd \end{bmatrix}$ voor zekere $a, b, c, s \in rat$.
2. Zij $m = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in R$. Bepaal het rechter ideaal $mR = \{my \mid y \in R\}$ en het linker ideaal $Rm = \{xm \mid x \in R\}$.
3. Bepaal $S = \{xmy \mid x, y \in R\}$. Is S een ideaal?
4. Is $\{x_1my_1 + x_2my_y \mid x_1, x_2, y_1, y_2\}$ een ideaal.

5.4.6. In een ring R heet e idempotent als $e^2 = e$. Bijvoorbeeld 0 en 1 zijn idempotenten.

1. Als e idempotent is, dan is ook $1 - e$ idempotent?
2. Als e idempotent is, is $1 - 2e$ idempotent?
3. Vind al de idempotenten in $\mathbb{Z}_{12}$.
4. Vind al de idempotenten in $M_2(\mathbb{R})$ en beschrijf ze meetkundig (Im, ker en eigenwaarden).
5. Zijn je bevindingen in (3) en (4) verenigbaar met (1)?
6. Als e een idempotent is, is dan Re een ring? Is eRe een ring? Is eRe een ideaal?

5.4.7. 1. Zij I een rechterideaal in een ring R. Bewijs dat $\text{ra}(I) = \{r \in R \mid Ir = \{0\}\}$ een tweezijdig ideaal is in R.

2. Bereken $\text{ra}(R_1)$ waar R_1 de eerste rij is $M_n(R)$ en R een ring is.

5.4.8. Zij $R[X]$ een polynomenring over een ring R.

1. Om een homomorfisme $f : R[X] \to R$ te bepalen met $f(r) = r$ voor elke $r \in R$ is het nodig en voldoende om $f(X)$ te geven.
2. Om een homomorfisme $f : \mathbb{R}[X] \to R$ (R een ring) te bepalen is het nodig en voldoende $f(X)$ te bepalen.
3. Bewijs dat een ring homomorfisme $f : \mathbb{R}[X] \to M_2(\mathbb{R})$ nooit injectief en nooit surjectief kan zijn. Toon ook aan dat $\dim(\text{Im}(f))$ ofwel 1- of 2-dimensionaal is (Hint: gebruik de stelling van Cayley-Hamilton).

4. In elk van de volgende gevallen, vind $\ker(f)$, $\mathrm{Im}(f)$ en controleer dat $\mathbb{R}[X]/\ker(f) \cong \mathrm{Im}(f)$:

   (a) $f(X) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$,

   (b) $f(X) = \begin{bmatrix} 3 & 0 \\ 0 & 5 \end{bmatrix}$,

   (c) $f(X) = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$,

   (d) $f(X) = \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}$

5.4.9. Is

$$I = \{a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \mid a_k \in \mathbb{Z} \text{ en } 2^{k+1} | a_k, \text{ voor elke } k\}$$

een ideaal in $\mathbb{Z}[X]$?

5.4.10. Beschrijf de kernen van de volgende ringhomomorfismen.

$$f_1 : \mathbb{R}[X,Y] \to \mathbb{R} : P(X,Y) \mapsto P(0,0)$$

$$f_2 : \mathbb{R}[X] \to \mathbb{C} : P(X) \mapsto P(2+i)$$

5.4.11. Beschouw de matrixring $R = \mathrm{M}_2(\mathbb{Q})$. Welk van de volgende deelverzamelingen van R zijn linker, rechter of tweezijdige idealen?

$$\begin{aligned}
I_1 &= \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \mid a,b,c \in \mathbb{Q} \right\} \\
I_2 &= \left\{ \begin{pmatrix} a & b \\ c & 1 \end{pmatrix} \mid a,b,c \in \mathbb{Q} \right\} \\
I_3 &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a,b \in \mathbb{Q} \right\} \\
I_4 &= \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q} \right\} \\
I_5 &= \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a,b \in \mathbb{Q} \right\} \\
I_6 &= \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a,b \in \mathbb{Q} \right\}
\end{aligned}$$

5.4.12. $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ is de kleinste deelring van $\mathbb{C}$ die $\sqrt{2}$ en $\sqrt{3}$ bevat. Toon aan dat

$$\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$$

5.4.13. Neem een rij (a_n) in een commutatieve ring R. Een uitdrukking van de vorm

$$\sum_{n=0}^{\infty} a_n X^n = a_0 + a_1 X + a_2 X^2 + \cdots$$

noemen we een formele machtreeks met coëfficiënten in R, Som en produkt van formele machtreeksen wordt alsvolgt gedefinieerd:

$$(\sum_{n=0}^{\infty} a_n X^n) + (\sum_{n=0}^{\infty} b_n X^n) = \sum_{n=0}^{\infty} (a_n + b_n) X^n$$

$$(\sum_{n=0}^{\infty} a_n X^n)(\sum_{n=0}^{\infty} b_n X^n) = a_0 b_0 + (a_1 b_0 + a_0 b_1) X + \cdots = \sum_{n=0}^{\infty} \sum_{i=0}^{n} a_i b_{n-i} X^n$$

Toon aan dat de verzameling $R[[X]]$ der formele machtreeksen een commutatieve ring vormen. Bewijs dat de formele machtreeks $\sum_{n=0}^{\infty} a_n X^n$ inverteerbaar is als en slechts als a_0 inverteerbaar is in R. Als $R = k$ een veld is, bewijs dan dat $k[[X]]$ een locale ring is.

5.4.14. Onderstel dat R een ring is van karakteristiek p (dit wil zeggen dat $\sum_{i=1}^{p} 1 = 0$ in R). Bewijs dat de afbeelding

$$f: \ R \to R: \ x \mapsto x^p$$

een ringhomomorfisme is. f wordt ook het Frobeniushomomorfisme genoemd.

5.4.15. Een element $e \in R$ wordt een idempotent genoemd als $e^2 = e$. Onderstel dat R commutatief is, en dat e een idempotent element van R is, en stel $f = 1 - e$. Toon aan dat f ook een idempotent is en dat $ef = 0$. Bewijs dat

$$R \cong Re \times Rf$$

Onderstel nu dat R een Noetherse commutatieve ring is. Bewijs dat er een eindig stel idempotenten $e_1, e_2, \ldots, e_n$ in R bestaan zodat

$$e_1 + e_2 + \ldots + e_n = 1$$

$$e_i e_j = 0 \ \text{ als } \ i \neq j$$

$$R \cong Re_1 \times Re_2 \times \cdots \times Re_n$$

en elke Re_i heeft op 0 en e_i na geen idempotenten.

5.4.16. Beschrijf de ringen

$$\mathbb{Z}[X]/(X^2 - 3, 2X + 4)$$
$$\mathbb{Z}[i]/(2 + i)$$
$$\mathbb{Z}[X]/(X^2 + 3, 3)$$
$$\mathbb{Z}[X]/(X^2 + 3, 5)$$

5.4.17. Onderstel dat I en J idealen zijn in een commutatieve ring R zodanig dat $I + J = R$ en $IJ = 0$. Toon aan dat

$$R \cong R/I \times R/J$$

en beschrijf de idempotenten die aanleiding geven tot dit isomorfisme.

5.4.18. Toon aan dat een commutatief domein met een eindig aantal elementen steeds een veld is.

5.4.19. Onderstel dat R een domein is. Toon aan dat $R[X]$ ook een domein is.

5.4.20. Bepaal de maximale idealen van de volgende ringen

$$\begin{array}{l} \mathbb{R} \times \mathbb{R} \\ \mathbb{R}[X]/(X^2) \\ \mathbb{R}[X]/(X^2 - 3X + 2) \\ \mathbb{R}[X]/(X^2 + X + 1) \end{array}$$

5.4.21. Voor welke natuurlijke getallen n is $X^4 + 3X^3 + X^2 + 6X + 10$ deelbaar door $x^2 + x + 1$ in $\mathbb{Z}/n\mathbb{Z}$?

5.4.22. R is een commutatieve ring. Als $a \in R$ inverteerbaar, en $x \in R$ nilpotent, toon dan aan dat $a + x$ inverteerbaar is.

5.4.23. R is commutatief, en

$$P(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$$

Bewijs:
1) P is inverteerbaar $\Longleftrightarrow$ a_0 is inverteerbaar in R, en voor elke $i > 0$ is a_i nilpotent.
2) P is nilpotent $\Longleftrightarrow$ voor elke $i \geq 0$ is a_i nilpotent.

5.4.24. R is commutatief. We noemen

$$\text{rad}(R) = \{x \in R \mid x^n = 0 \text{ voor een zekere } n \geq 1\}$$

het nilradikaal van R. Bewijs:
1) $\text{rad}(R)$ is een ideaal.
2) $R/\text{rad}(R)$ heeft 0 als enige nilpotent element.
3) $\text{rad}(R) = \cap\{P \mid P \text{ is een priemideaal van } R\}$.

5.4.25. Bereken het nilradikaal van $\mathbb{Z}/n\mathbb{Z}$.

5.4.26. In een commutatieve ring zijn de volgende drie eigenschappen equivalent. Bewijs!
1) R heeft juist 1 priemideaal;
2) $x \in R \implies x$ is inverteerbaar of x is nilpotent;
3) $R/\text{rad}(R)$ is een veld.

5.4.27. Onderstel dat S een multiplicatief gesloten deel van R is, en $g: R \to T$ een ringhomomorfisme. Onderstel verder dat $g(s)$ inverteerbaar is in T, voor elke $s \in S$. Toon aan dat er juist 1 ringhomomorfisme $h: S^{-1}R \to T$ bestaat zodat $g = h \circ f$, waarbij $f: R \to S^{-1}R$ het kanonieke homomorfisme.

5.4.28. Stel $R = \mathbb{Z}[i] = \mathbb{Z}+i\mathbb{Z} \subset \mathbb{C}$, en definieer $N: R \to \mathbb{N}$ door $N(m+in) = m^2+n^2$. Toon aan dat R een Euclidisch domein is. Ga tewerk als volgt.
a) Het breukenveld van R is $\mathbb{Q}[i]$.
b) Het volstaat aan te tonen dat voor elke $a, b \in R$ met $b \neq 0$ er een $c \in R$ bestaat zo dat

$$N(a - bc) < N(b)$$

of (gebruik makend van het feit dat N multiplicatief is)

$$N(\frac{a}{b} - c) < 1$$

c) Stel $a/b = x + iy$, met $x, y \in \mathbb{Q}$. Neem $u, v \in \mathbb{Z}$ zodat $|u - x| < 1/2$ en $|v - y| < 1/2$. Neem nu $c = u + iv$.

5.4.29. Zij R een commutatieve ring, en I een ideaal van R. Beschrijf de endomorfismenring $\mathrm{End}_R(R/I)$.

5.4.30. Geef een voorbeeld van een ring waarvan het centrum een veld is maar de ring is niet enkelvoudig.

5.4.31. Zij R een ring. Bewijs dat de tweezijdige idealen in $M_{nn}(R)$ al de verzamelingen zijn van de vorm $M_{nn}(I)$ met I een tweezijdig ideaal in R.

Zij I een ideaal in R. Bewijs dat

1. $M_{nn}(R)/M_{nn}(I) \cong M_{nn}(R/I)$,
2. $M_{nn}(I)$ is een priem (respectievelijk maximaal) ideaal in $M_{nn}(R)$ als en slechts als I een priem (respectievelijk maximaal) ideaal is in R.

5.4.32. Bewijs dat de bovendriehoeksmatrices in $M_2(\mathbf{Z})$ geen priem ring vormen. Geef een maximaal ideaal in deze ring.

5.4.33. Zij R een ring en e_1, e_2 idempotenten in R. Is $e_1 + e_2$ terug een idempotent? Indien zo, geef een bewijs, anders geef een tegenvoorbeeld.

5.4.34. Zij R een domein, $r \in R$ en $P = R[X](X - r)$. Bewijs dat P een priem ideaal is van $R[X]$. Beschrijf $R[X]/P$ (op isomorfisme na). Als, bovendien, R een veld is, bewijs dat P een maximaal ideaal is.

5.4.35. Zij f een irreducibele polynoom in $F[X]$, F a veld. Bewijs dat $(f) = F[X]f$ een maximaal ideaal is in $F[X]$.

5.4.36. Zij $M_1, \ldots, M_n$ verschillende maximale idealen van een ring R. Als $M_1 \cap \cdots \cap M_n = \{0\}$, bewijs dat

1. $M_1, \ldots, M_n$ de enige priem idealen zijn van R;
2. $R \cong \prod_{i=1}^{n} R/M_i$.

5.4.37. Beschouw de volgende deelverzamelingen van de ring $\mathbf{R}[X]$:

$$\begin{aligned} I &= \{f \in \mathbf{R}[X] \mid f(0) = 0\} \\ J &= \{f \in \mathbf{R}[X] \mid f(3) = f'(3) = 0\} \\ K &= \{f \in \mathbf{R}[X] \mid f(n) = 0, \text{ voor alle } n \in \mathbf{N}\} \end{aligned}$$

1. Zijn I, J, K hoofidealen van $\mathbf{R}[X]$?
2. Zijn I, J, K maximale idealen of priemidealen van $\mathbf{R}[X]$?
3. Welk paar van I, J, K is comaximaal?
4. Vond $u, v \in \mathbf{R}[X]$ zodat $ux + v(x^2 - 6x + 9) = 1$.

5.4.38. Zij $R = \mathbf{Z}_6$ en $S = \{1, 2, 4\} \subseteq R$. Dan is S een multiplicatief gesloten deel van R. Bepaal de ring $S^{-1}R$. Is het natuurlijk homomorfisme $f : R \to S^{-1}R$ injectief?

5.4.39. Zijn de volgende elementen van $\mathbf{Q}[[X]]$ inverteerbaar? Zo ja, kan je hun inverse bepalen?

1. $1 - X$,
2. $\sum_{n=0}^{\infty} (-3)^{n+1} X^n$,
3. $X - X^3$,
4. $1 - X^2$,
5. $\sum_{n=0}^{\infty} (n+1) X^n$,
6. $\sum_{n=0}^{\infty} n!\, X^n$,
7. 5,
8. $\sum_{n=2}^{\infty} n^3 X^n$,

9. $\sum_{n=0}^{\infty} \frac{X^n}{n!}$.

5.4.40. Zij $R = \{a + b\sqrt{10} \mid a, b \in \mathbf{Z}\}$. Dan is R een deelring van $\mathbf{R}$ (geen deelring van $\mathbf{Q}$). Is R een veld? Bevat R nuldelers? Is R noethers? (Vind een epimorfisme $\mathbf{Z}[X] \to R$.)

Welke factorisatie is "essentieel verschillend" van $6 = 2 \cdot 3$?

1. $6 = (-2) \cdot (-3)$,
2. $6 = 3 \cdot 2$,
3. $6 = (-6 + \sqrt{40})(9 + \sqrt{90})$,
4. $6 = (4 + \sqrt{10})(4 - \sqrt{10})$.

5.4.41. Beschouw de noetherse ring $A = \mathbf{C}[X, Y]$.

1. Als $\varphi : A \to \mathbf{C} : f \mapsto f(0, 0)$ dan is $M = \ker \varphi$ een maximaal ideaal van A. Is $M = (X, Y) = (X + 2Y, X + 3Y)$ een hoofdideaal?
2. Is er een ideaal dat niet kan voortgebracht worden door minder dan drie elementen?
3. $P = (X)$ is een priemideaal, en $\{0\} \subset P \subset M$ is een strikt stijgende keten van drie priemidealen. Bestaat er een langere strikt stijgende keten van priemidealen?

5.4.42. Zij $R[G]$ be the groepring of de ring R over de groep G. Definieer:

$$\omega : R[G] \to R : \sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g.$$

1. Bewijs dat ω een ringhomomorfisme is.
2. Bewijs dat het ideaal Ker (ω) een vrij links R-moduul is met basis $\{1 - g \mid g \in G\}$.
3. Bewijs dat $R[G]/ker(\omega) \cong R$.

Het ideaal Ker (f) noemt men het augmentatie ideaal van de groepring $R[G]$.

5.5 Modulen

5.5.1. Zij R een commutatieve ring. Een R-moduul P wordt *enkelvoudig* of *simpel* genoemd als $P \neq 0$, en als P geen enkel echt deelmoduul heeft.
a) Toon aan dat elk enkelvoudig R-moduul P isomorf is met R/M, waarbij M een maximaal ideaal van R is.
b) Als $\varphi : \ P \to Q$ een homomorfisme van enkelvoudige R-modulen is, dan is ofwel $\varphi = 0$, ofwel is φ een isomorfisme.

5.5.2. Zij R een commutatieve ring, en P een R-moduul. De *annihilator* van P is de verzameling

$$I = \{r \in R \mid rP = 0\}$$

a) Bewijs dat I een ideaal van R is.
b) Bepaal de annihilatoren van de $\mathbb{Z}$-modulen $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\times$ en $\mathbb{Z}$.

5.5.3. Zij R een commutatieve ring, en $W \subset V \subset U$ R-modulen.
a) Beschrijf de natuurlijke homomorfismen die er zijn tussen de quotiëntmodulen U/W, U/V en V/W.
b) Bewijs dat $U/V \cong (U/W)/(V/W)$.

5.5.4. Zij R een commutatieve ring, en V en W deelmodulen van een R-moduul U.
a) Bewijs dat $V + W$ en $V \cap W$ deelmodulen zijn van U.
b) Bewijs dat $(V + W)/W \cong V/(V \cap W)$.

5.5.5. Zij I een ideaal in een commutatieve ring R. Bewijs dat I een vrij R-moduul is als en alleen als I een hoofdideaal is dat voortgebracht is door een element dat geen nuldeler is.

5.5.6. Zoek een basis voor de volgende deelmodulen van $\mathbb{Z}^3$:
a) Het moduul voortgebracht door $(1, 0, -1),\ (2, 3, -1),\ (0, 3, 1)$ en $(3, 1, 5)$.
b) Het moduul dat bestaat uit de (x, y, z) die oplossingen zijn van het stelsel

$$\begin{aligned} x + 2y + 3z &= 0 \\ x + 4y + 9z &= 0 \end{aligned}$$

5.5.7. Onderstel dat R een commutatieve ring is, en e en f twee idempotenten verschillend van 0 en 1, zodat $e + f = 1$ en $ef = 0$. Zoals we reeds zagen is R isomorf met het product $Re \times Rf$. We maken van Re een R-moduul via de scalaire vermenigvuldiging

$$r(se) = rse$$

Toon aan dat Re een projectief R-moduul is, maar geen vrij R-moduul. Bepaal een duale basis voor Re.

5.5.8. Zij R een Euclidisch domein. Maak gebruik van Stelling 2.2.4 om aan te tonen dat elk eindig voortgebracht R-moduul vrij is.

5.5.9. Bewijs dat de volgende $\mathbf{Z}$-modulen niet Noethers zijn:

1. $\mathbf{Q}$.
2. $\mathbf{Z}$-moduul $\mathbf{Q}/\mathbf{Z}$.
3. $\mathbb{R}/\mathbf{Z}$.

5.5.10. 1. Zij $(A, +)$ een commutatieve groep. Bewijs dat

$$Hom_{\mathbf{Z}}(\mathbf{Z}_n, G) \cong \{g \in G \mid ng = 0\}.$$

(isomorf als $\mathbf{Z}$-modulen)

2. Bewijs dat $Hom_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_2) \not\subseteq Hom_{\mathbf{Z}}(\mathbf{Q}, \mathbf{Z}_2)$.

5.5.11. Zij R een ring en zij M_1, M_2, M, N_1, N_2, N R-modulen. Bewijs dat

1. $Hom_R(M_1 \oplus M_2, N) \cong Hom_R(M_1, N) \oplus Hom_R(M_2, N)$;
2. $Hom_R(M, N_1 \oplus N_2) \cong Hom_R(M, N_1) \oplus Hom_R(M, N_2)$.

Alle isomorfismen zijn als $\mathbf{Z}$-modulen, behalve als R een commutatieve ring is, dan zijn alle isomorfismen R-moduul ismorfismen.

5.5.12. Als een moduul M maximale deelmodulen $N_1, \ldots, N_n$ heeft zodat $N_1 \cap \cdots \cap N_n = \{0\}$, met n minimaal, bewijs dat $M \cong \prod_{i=1}^{n} M/N_i$.

Bibliografie

[1] M. Artin, *Algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[2] T. S. Blyth, *Module theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, second ed., 1990. An approach to linear algebra.

[3] P. J. Cameron, *Introduction to algebra*, Oxford Science Publications, Oxford University Press, Oxford, 1998.

[4] P. M. Cohn, *Algebra, Vol. 1*, John Wiley & Sons, London-New York-Sydney, 1974.

[5] I. M. Isaacs, *Algebra*, Brooks/Cole Publishing Co., Pacific Grove, CA, 1994. A graduate course.

[6] S. Lang, *Algebra*, vol. 211 of Graduate Texts in Mathematics, Springer-Verlag, New York, third ed., 2002.

[7] L. Rowen, *Algebra*, A K Peters, Ltd., Wellesley, MA, 1994. Groups, rings, and fields.

[8] L. H. Rowen, *Ring theory*, Academic Press, Inc., Boston, MA, student ed., 1991.

[9] I. Stewart and D. Tall, *Algebraic number theory*, Chapman and Hall, London; A Halsted Press Book, John Wiley & Sons, New York, 1979. Chapman and Hall Mathematics Series.

Index

Some historical data

From Wikipedia

Frobenius

Article by: J J O'Connor and E F Robertson
http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Frobenius.html

Georg Frobenius's father was Christian Ferdinand Frobenius, a Protestant parson, and his mother was Christine Elizabeth Friedrich. Georg was born in Charlottenburg which was a district of Berlin which was not incorporated into the city until 1920. He entered the Joachimsthal Gymnasium in 1860 when he was nearly eleven years old and graduated from the school in 1867. In this same year he went to the University of Göttingen where he began his university studies but he only studied there for one semester before returning to Berlin.

Back at the University of Berlin he attended lectures by Kronecker, Kummer and Weierstrass. He continued to study there for his doctorate, attending the seminars of Kummer and Weierstrass, and he received his doctorate (awarded with distinction) in 1870 supervised by Weierstrass. In 1874, after having taught at secondary school level first at the Joachimsthal Gymnasium then at the Sophienrealschule, he was appointed to the University of Berlin as an extraordinary professor of mathematics.

For the description of Frobenius's career so far, the attentive reader may have noticed that no mention has been made of him receiving his habilitation before being appointed to a teaching position. This is not an omission, rather it is surprising given the strictness of the German system that this was allowed. We should say that it must ultimately have been made possible due to strong support from Weierstrass who was extremely influential and considered Frobenius one of his most gifted students.

Frobenius was only in Berlin for a year before he went to Zürich to take up an

appointment as an ordinary professor at the Eidgenössische Polytechnikum. For seventeen years, between 1875 and 1892, Frobenius worked in Zürich. He married there and brought up a family and did much important work in widely differing areas of mathematics. We shall discuss some of the topics which he worked on below, but for the moment we shall continue to describe how Frobenius's career developed.

In the last days of December 1891 Kronecker died and, therefore, his chair in Berlin became vacant. Weierstrass, strongly believing that Frobenius was the right person to keep Berlin in the forefront of mathematics, used his considerable influence to have Frobenius appointed. However, for reasons which we shall discuss in a moment, Frobenius turned out to be something of a mixed blessing for mathematics at the University of Berlin.

The positive side of his appointment was undoubtedly his remarkable contributions to the representation theory of groups, in particular his development of character theory, and his position as one of the leading mathematicians of his day. The negative side came about largely through his personality:-

... occasionally choleric, quarrelsome, and given to invectives.

Biermann, looks more closely at his character (no pun intended!), and how it affected the success of mathematical education at the university. He describes the strained relationships which developed between Frobenius and his colleagues at Berlin. He had such high standards that in the end these did not serve Berlin well. He:-

... suspected at every opportunity a tendency of the Ministry to lower the standards at the University of Berlin, in the words of Frobenius, to the rank of a technical school ... Even so, Fuchs and Schwarz yielded to him, and later Schottky, who was indebted to him alone for his call to Berlin. Frobenius was the leading figure, on whom the fortunes of mathematics at Berlin university rested for 25 years. Of course, it did not escape him, that the number of doctorates, habilitations, and docents slowly but surely fell off, although the number of students increased considerably. That he could not prevent this, that he could not reach his goal of maintaining unchanged the times of Weierstrass, Kummer and Kronecker also in their external appearances, but to witness helplessly these developments, was doubly intolerable for him, with his choleric disposition.

We should not be too hard on Frobenius for, as Haubrich explains, Frobenius's attitude was one which was typical of all professors of mathematics at Berlin at this time:-

They all felt deeply obliged to carry on the Prussian neo-humanistic tradition of university research and teaching as they themselves had experienced it as students. This is especially true of Frobenius. He considered himself to be a scholar whose duty it was to contribute to the knowledge of pure mathematics. Applied mathematics, in his opinion, belonged to the technical colleges.

The view of mathematics at the University of Göttingen was, however, very different. This was a time when there was competition between mathematians in the University of Berlin and in the University of Göttingen, but it was a competition that Göttingen won, for there mathematics flourished under Klein, much to Frobenius's annoyance. Biermann writes that:-

The aversion of Frobenius to Klein and S Lie knew no limits ...

Frobenius hated the style of mathematics which Göttingen represented. It was a new approach which represented a marked change from the traditional style of German universities. Frobenius, as we said above, had extremely traditional views. In a letter to Hurwitz, who was a product of the Göttingen system, he wrote on 3 February 1896:-

If you were emerging from a school, in which one amuses oneself more with rosy images than hard ideas, and if, to my joy, you are also gradually becoming emancipated from that, then old loves don't rust. Please take this joke facetiously.

One should put the other side of the picture, however, for i Siegel, who knew Frobenius for two years from 1915 when he became a student until Frobenius's death, relates his impression of Frobenius as having a warm personality and expresses his appreciation of his fast-paced varied and deep lectures. Others would describe his lectures as solid but not stimulating.

To gain an impression of the quality of Frobenius's work before the time of his appointment to Berlin in 1892 we can do no better than to examine the recommendations of Weierstrass and Fuchs when Frobenius was elected to the Prussian Academy of Sciences in 1892. Fairly extensive quotes from this document, and another similar document from Fuchs and Helmholtz, are given but we quote a short extract to show the power, variety and high quality of Frobenius's work in his Zürich years. Weierstrass and Fuchs list 15 topics on which Frobenius had made major contributions:-

1. On the development of analytic functions in series.

2. On the algebraic solution of equations, whose coefficients are rational functions of one variable.
3. The theory of linear differential equations.
4. On Pfaff's problem.
5. Linear forms with integer coefficients.
6. On linear substitutions and bilinear forms...
7. On adjoint linear differential operators...
8. The theory of elliptic and Jacobi functions...
9. On the relations among the 28 double tangents to a plane of degree 4.
10. On Sylow's theorem.
11. On double cosets arising from two finite groups.
12. On Jacobi's covariants...
13. On Jacobi functions in three variables.
14. The theory of biquadratic forms.
15. On the theory of surfaces with a differential parameter.

In his work in group theory, Frobenius combined results from the theory of algebraic equations, geometry, and number theory, which led him to the study of abstract groups. He published Über Gruppen von vertauschbaren Elementen in 1879 (jointly with Stickelberger, a colleague at Zürich) which looks at permutable elements in groups. This paper also gives a proof of the structure theorem for finitely generated abelian groups. In 1884 he published his next paper on finite groups in which he proved Sylow's theorems for abstract groups (Sylow had proved his theorem as a result about permutation groups in his original paper). The proof which Frobenius gives is the one, based on conjugacy classes, still used today in most undergraduate courses. In his next paper in 1887 Frobenius continued his investigation of conjugacy classes in groups which would prove important in his later work on characters. In the introduction to this paper he explains how he became interested in abstract groups, and this was through a study of one of Kronecker's papers. It was in the year 1896, however, when Frobenius was professor at Berlin that his really important work on groups began to appear. In that year he published five papers on group theory and one of them Über die Gruppencharactere on group characters is of fundamental importance. He wrote in this paper:-

I shall develop the concept [of character for arbitrary finite groups] here in the belief that through its introduction, group theory will be substantially enriched.

This paper on group characters was presented to the Berlin Academy on July 16 1896 and it contains work which Frobenius had undertaken in the preceding few months. In a series of letters to Dedekind, the first on 12 April 1896, his ideas on group characters quickly developed. Ideas from a paper by Dedekind in 1885 made an important contribution and Frobenius was able to construct a complete set of representations by complex numbers. It is worth noting, however, that although we think today of Frobenius's paper on group characters as a fundamental work on representations of groups, Frobenius in fact introduced group characters in this work without any reference to representations. In was not until the following year that representations of groups began to enter the picture, and again it was a concept due to Frobenius. Hence 1897 is the year in which the representation theory of groups was born.

Over the years 1897-1899 Frobenius published two papers on group representations, one on induced characters, and one on tensor product of characters. In 1898 he introduced the notion of induced representations and the Frobenius Reciprocity Theorem. It was a burst of activity which set up the foundations of the whole of the machinery of representation theory.

In a letter to Dedekind on 26 April 1896 Frobenius gave the irreducible characters for the alternating groups A4, A5, the symmetric groups S4, S5 and the group PSL(2,7) of order 168. He completely determined the characters of symmetric groups in 1900 and of characters of alternating groups in 1901, publishing definitive papers on each. He continued his applications of character theory in papers of 1900 and 1901 which studied the structure of Frobenius groups.

Only in 1897 did Frobenius learn of Molien's work which he described in a letter to Dedekind as "very beautiful but difficult". He reformulated Molien's work in terms of matrices and then showed that his characters are the traces of the irreducible representations. This work was published in 1897. Frobenius's character theory was used with great effect by Burnside and was beautifully written up in Burnside's 1911 edition of his Theory of Groups of Finite Order.

Frobenius had a number of doctoral students who made important contributions to mathematics. These included Edmund Landau who was awarded his doctorate in 1899, Issai Schur who was awarded his doctorate in 1901, and Robert Remak who was awarded his doctorate in 1910. Frobenius collaborated with Schur in representation theory of groups and character theory of groups. It is certainly to Frobenius's credit that he so quickly spotted the genius of his student Schur. Frobenius's representation theory for finite groups was later to find important applications in quantum mechanics

and theoretical physics which may not have entirely pleased the man who had such "pure"views about mathematics.

Among the topics which Frobenius studied towards the end of his career were positive and non-negative matrices. He introduced the concept of irreducibility for matrices and the papers which he wrote containing this theory around 1910 remain today the fundamental results in the discipline. The fact so many of Frobenius's papers read like present day text-books on the topics which he studied is a clear indication of the importance that his work, in many different areas, has had in shaping the mathematics which is studied today. Having said that, it is also true that he made fundamental contributions to fields which had already come into existence and he did not introduce any totally new mathematical areas as some of the greatest mathematicians have done.

Haubrich gives the following overview of Frobenius's work:-

The most striking aspect of his mathematical practice is his extraordinary skill at calculations. In fact, Frobenius tried to solve mathematical problems to a large extent by means of a calculative, algebraic approach. Even his analytical work was guided by algebraic and linear algebraic methods. For Frobenius, conceptual argumentation played a somewhat secondary role. Although he argued in a comparatively abstract setting, abstraction was not an end in itself. Its advantages to him seemed to lie primarily in the fact that it can lead to much greater clearness and precision.

Brauer

Article by: J J O'Connor and E F Robertson
http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Brauer.html

Richard Brauer's father was Max Brauer who was a well-off businessman in the wholesale leather trade. Max Brauer's wife was Lilly Caroline and Richard was the youngest of their three children. He had an older brother Alfred Brauer, who also became a famous mathematician and has a biography in this archive. Alfred Brauer was seven years older than Richard and of an age between the two brothers was Richard's sister Alice.

Richard entered the Kaiser-Friedrich-Schule in Charlottenburg in 1907. Charlottenburg was a district of Berlin which was not incorporated into the city until 1920. Richard studied at this school until 1918 and it was during his school years that he developed his love of mathematics and science. However, this was not due to the teaching at the school, but it came about through the influence of his brother Alfred. Richard writes

about his school teachers who he describes as not being very competent. There was one exception however, and it was fortunate that this good teacher was a mathematician who had a doctorate awarded for research done under Frobenius's supervision.

Of course Richard's last four years at school were the years of World War I, but, unlike his brother, he was young enough to avoid being drafted into the army. When he graduated from the Kaiser-Friedrich-Schule in September 1918 the war was still in progress, and Brauer was drafted to undertake civilian war service in Berlin. Only two months later, in November 1918, the war ended, Brauer was released from war service and he resumed his education. Despite the love for mathematics which he had gained from his brother, Brauer decided to follow his boyhood dreams of becoming an inventor. He entered the Technische Hochschule of Charlottenburg in February 1919 where he studied for a term before, having realised that his talents were in theory rather than practice, he transferred to the University of Berlin.

At the University of Berlin Brauer was taught by a number of really outstanding mathematicians including Bieberbach, Carathéodory, Einstein, Knopp, von Mises, Planck, Schmidt, Schur and Szego. Brauer describes some of the lectures he attended; talking of Schmidt's lectures he writes:-

It is not easy to describe their fascination. When Schmidt stood in front of a blackboard, he never used notes, and was hardly ever well prepared. He gave the impression of developing the theory right there and then.

It was the custom that German students at this time spent periods in several different universities during their degree course. Brauer was no exception to this, although he made only one visit during his studies, that being for a term to the University of Freiburg. Back in Berlin he attended seminars by Bieberbach, Schmidt and Schur. He was increasingly attracted towards the algebra which Schur was presenting in his seminar (which was attended in the same year by Alfred Brauer). Schur, unlike Schmidt, -

... was very well prepared for his classes, and he lectured very fast. If one did not pay the utmost attention to his words, one was quickly lost. There was hardly any time to take notes in class; one had to write them up at home. ... He conducted weekly problem hours, and almost every time he proposed a difficult problem. Some of the problems had already been used by his teacher Frobenius, and others originated with Schur. Occasionally he mentioned a problem he could not solve himself.

In fact it was one of these open problems which Richard working with his brother Alfred solved in 1921 and this was eventually to be included in Brauer's first publication.

Schur suggested the problem that Brauer worked on for his doctorate and the degree was awarded (with distinction) in March 1926. His dissertation took an algebraic approach to calculating the characters of the irreducible representations of the real orthogonal group. Before the award of his doctorate, however, Brauer had married Ilse Karger in September 1925. They had been a fellow students in one of Schur's courses on number theory. Before his marriage Brauer was appointed as Knopp's assistant at the University of Königsberg and he took up this post in the autumn of 1925.

Shortly after Brauer arrived in Königsberg, Knopp left to take up an appointment at Tübingen. The mathematics department at Königsberg was small, with two professors Szego and Reidemeister, and with Rogosinski and Kaluza holding junior positions like Brauer. It was in Königsberg that Brauer's two sons, George Ulrich Brauer and Fred Günter Brauer were born. Brauer taught at Königsberg until 1933 and during this period he produced results of fundamental importance. Green writes:-

This was the time when Brauer made his fundamental contribution to the algebraic theory of simple algebras. ... Brauer developed ... a theory of central division algebras over a given perfect field, and showed that the isomorphism classes of these algebras can be used to form a commutative group whose properties gave great insight into the structure of simple algebras. This group became known (to the author's embarrassment) as the "Brauer group"...

Political events forced Brauer's family to move. He wrote:-

I lost my position in Königsberg in the spring of 1933 after Hitler became Reichskanzler of Germany.

Brauer was from a Jewish family so was dismissed from his post under the Nazi legislation which removed all Jewish university teachers from their posts. This was a desperate time for Brauer who realised that he had to find a post outside Germany. Fortunately action was taken in several countries to find posts abroad for German academics forced from their positions and a one year appointment was arranged for Brauer in Lexington, Kentucky for the academic year 1933-34. In November 1933 Brauer arrived to take up his appointment at the University of Kentucky, his wife and two sons following three months later. We should record that Alfred Brauer left Germany in 1939, but Brauer's sister Alice stayed behind and was murdered in a concentration camp by the Nazis.

Following his year in Lexington, Brauer was appointed as Weyl's assistant at the Institute for Advanced Study in Princeton. He wrote about this appointment with Weyl:-

I had hoped since the days of my PhD thesis to get in contact with him some day; this dream was now fulfilled.

Collaboration between Brauer and Weyl on several projects followed, in particular a famous joint paper on spinors published in 1935 in the American Journal of Mathematics. This work was to provide a background for the work of Paul Dirac in his exposition of the theory of the spinning electron within the framework of quantum mechanics.

A permanent post followed the two temporary posts when Brauer accepted an assistant professorship at the University of Toronto in Canada in the autumn of 1935. It was largely as a result of Emmy Noether's recommendation, which she made while visiting Toronto, which led to his appointment. This was a time when Brauer developed some of his most impressive theories, carrying the work of Frobenius into a whole new setting, in particular the work on group characters Frobenius published in 1896. Brauer carried Frobenius's theory of ordinary characters (where the characteristic of the field does not divide the order of the group) to the case of modular characters (where the characteristic does divide the group order). He also studied applications to number theory.

C J Nesbitt was Brauer's first doctoral student in Toronto and he described their relationship as doctoral student and supervisor:-

Curiously, as thesis advisor, he did not suggest much preparatory reading or literature search. Instead we spent many hours exploring examples of the representation theory ideas that were evolving in his mind.

It was in joint work with Nesbitt, published in 1937, that Brauer introduced the theory of blocks. This he used to obtain results on finite groups, particularly finite simple groups, and the theory of blocks would play a big part in much of Brauer's later work.

Alperin also spoke of Brauer's thirteen years in Toronto:-

The years he spent at Toronto were his most productive years. He achieved five or six great results during that time, any one of which would have established a person as a first-rank mathematician for the rest of their life. ... those years had their high points, but also contained fallow periods, when there was the day-to-day grind of raising a family in modest circumstances.

Brauer spent 1941 at the University of Wisconsin having been awarded a Guggenheim Memorial Fellowship. He was the Colloquium lecturer at the American Mathematical

Society Summer Meeting in Madison, Wisconsin in 1948. Later that year he moved from Toronto back to the United States, accepting a post at the University of Michigan in Ann Arbor. In 1949 Brauer was awarded the Cole Prize from the American Mathematical Society for his paper On Artin's L-series with general group characters which he published in the Annals of Mathematics in 1947. In 1951 Harvard University offered him a chair and, in 1952, he took up the position in Harvard which he was to hold until he retired in 1971. In the year of his retirement he was honoured with the award of the National Medal for Scientific Merit.

We have mentioned a number of topics which Brauer worked on in the course of this biography. However we have not yet mentioned the work which in many ways was his most famous and this he began around the time he took up the chair at Harvard. He began to formulate a method to classify all finite simple groups and his first step on this road was a group-theoretical characterisation of the simple groups PSL(2,q) in 1951 (although for a complicated number of reasons this did not appear in print until 1958). This work was done jointly with his doctoral student K A Fowler, and in 1955 they published a major paper which was to set mathematicians on the road to the classification. The paper was On groups of even order and it provided the key to the major breakthrough by Walter Feit and John Thompson when they proved that every finite simple group has even order.

Brauer was to spend the rest of his life working on the problem of classifying the finite simple groups. He died before the classification was complete but his work provided the framework of the classification which was completed only a few years later. (See the biography of Gorenstein for further details on the programme to classify finite simple groups.) Most important was Brauer's vital step in setting the direction for the whole classification programme in the paper On groups of even order where it is shown that there are only finitely many finite simple groups containing an involution whose centraliser is a given finite group. Brauer had announced these results and his programme for classifying finite simple groups at the International Congress of Mathematicians in Amsterdam in 1954.

Green points out that when Brauer went to Harvard he was 51 years old, yet almost half his total of 147 publications were published after this date. He certainly did not sit quietly working away in Harvard. He spent extended periods visiting friends and colleagues in universities around the world, for example Frankfurt and Göttingen in Germany, Nagoya in Japan, and Newcastle and Warwick in England.

Despite his remarkable contributions to research, Brauer found time to act as an editor for a number of journals. He was an editor of the Transactions of the Canadian Mathematical Congress from 1943 to 1949, the American Journal of Mathematics from 1944 to 1950, the Canadian Journal of Mathematics from 1949 to 1959, the Duke

Mathematical Journal from 1951 to 1956 and again from 1963 to 1969, the Annals of Mathematics from 1953 to 1960, the Proceedings of the Canadian Mathematical Congress from 1954 to 1957, and the Journal of Algebra from 1964 to 1970. A quick glance will show that in 1955 he held editorships of four learned journals.

We have mentioned above a number of honours which Brauer received. We should also mention the learned societies which honoured him with membership: the Royal Society of Canada (1945), the American Academy of Arts and Sciences (1954), the National Academy of Sciences (1955), the London Mathematical Society (1963), the Akademie der Wissenschaften Göttingen (1964), and the American Philosophical Society (1974). He was also elected President of the Canadian Mathematical Congress (1957-58) and the American Mathematical Society (1959-60).

Green describes Brauer's character (no pun intended):-

All who knew him best were impressed by his capacity for wise and independent judgement, his stable temperament and his patience and determination in overcoming obstacles. He was the most unpretentious and modest of men, and remarkably free of self-importance. ...

Brauer's interest in people was natural and unforced, and he treated students and colleagues alike with the same warm friendliness. In mathematical conversations, which he enjoyed, he was usually the listener. If his advice was sought, he took this as a serious responsibility, and would work hard to reach a wise and objective decision.

Richard Brauer occupied an honoured position in the mathematical community, in which the respect due to a great mathematician was only one part. He was honoured as much by those who knew him for his deep humanity, understanding and humility; these were the attributes of a great man.

Maschke

(Article by: J J O'Connor and E F Robertson)
http://www-groups.dcs.st-and.ac.uk/∼ history/Mathematicians

Heinrich Maschke's father was an important medical man. Heinrich attended the Gymnasium in Breslau where he showed great ability. He entered the University of Heidelberg in 1872, studying there under Königsberger.

Military service was required at that time so Maschke spent a year in the army before he continued his studies at the University of Berlin. At Berlin he was taught by some

outstanding mathematical teachers including Weierstrass, Kummer and Kronecker. He took the examinations to become a secondary school teacher in 1878 but he was aiming higher than this for he wanted to become a university teacher. In common with the standard practice of the time he moved around different German universities, next going to Göttingen from where he received his doctorate in 1880. Realising that it would be almost impossible to obtain a university position, Maschke decided to take up secondary school teaching.

His first teaching post was in the Luisenstädtische Gymnasium in Berlin. However he found both the long hours teaching and the elementary nature of the mathematics he was having to teach made him feel that he was in the wrong profession. This said, he was by all accounts a very good school teacher. He was given a sabbatical year and returned to Göttingen for the year 1886-87, working there with Klein. He had become a close friend of Bolza's while the two studied together at Berlin, and they were now together again at Göttingen both working with Klein. Maschke found working with Klein in his home in the evenings very rewarding and was fascinated with Klein's ideas on using group theory to solve algebraic equations. Due to Klein's encouragement, Maschke published his first paper in 1887, namely Über die quaternäre endliche, lineare Substitutionsgruppe der Borchardt'schen Moduln. Hermite, Kronecker and Brioschi had, in 1858, discovered how to solve the quintic equation by means of elliptic functions. In 1888 Maschke proved that a particular sixth-degree equation could be solved by using hyperelliptic functions and Brioschi showed that any sixth-degree algebraic equation could be reduced to Maschke's equation and therefore solved in the same way.

Maschke had returned to the Gymnasium in Berlin before he wrote the paper we just mentioned but, as is evident, he was not teaching in a secondary school yet concentrating on research. However, he wrote to Klein on 8 December 1888:-

... everyone here works in isolation and can hardly be moved to talk about his research.

By 1889 he had made a definite decision to give up school teaching. In this year Bolza, who was by now in the United States, was working at Johns Hopkins University where he had been given a temporary short-term appointment, and he had already accepted an appointment at Clark University in Worcester, Massachusetts. Maschke decided that the best course of action for him was to follow Bolza to the United States but Bolza warned him that it was not easy to get academic positions there. Maschke thought he had better have qualifications to enter some other profession otherwise he might emigrate to the United States and end up there as a school teacher - the profession he had now decided to give up. Keeping his teaching post, he began part-time study of electrotechnics at the Polytechnicum in Charlottenburg in 1889-90. In 1890 he resigned his teaching post and took up full-time technical training in Darmstadt.

In 1891 Maschke emigrated to the United States and worked for a year with the Western Electrical Instrument Company, Newark, New Jersey. In 1892 the University of Chicago opened and the head of the mathematics department, Eliakim Moore, began building up a strong unit. Bolza joined the University of Chicago in 1892 and then he persuaded Moore to appoint Maschke to Chicago. The three were highly influential in building up a strong mathematics research school in Chicago. R C Archibald writes:-

These three men supplemented one another remarkably. Moore was a fiery enthusiast, brilliant, and keenly interested in the popular mathematical research movements of the day; Bolza, a product of the meticulous German school of analysis led by Weierstrass, was an able, and widely read research scholar; Maschke was more deliberate than the other two, sagacious, brilliant in research, and a most delightful lecturer in geometry. During the period 1892-1908 the University of Chicago was unsurpassed in America as an institution for the study of higher mathematics.

Between 1892 and 1910 the mathematics department was outstandingly successful with thirty-nine students graduating with doctorates (but only five of them were students of Maschke). Maschke was promoted to associate professor in 1896 and then to full professor in 1907.

Under Klein's inspiration while at Göttingen, Maschke had worked in group theory, in particular working on finite groups of linear transformations. He is best known today for Maschke's theorem, which he published in 1899, which states that if the order of the finite group G is not divisible by the characteristic of the field K, then the (finite-dimensional) K-representations of G are completely reducible. A closer look at events surrounding this provide an interesting insight into the interplay between various mathematicians. Maschke proved a special case of his theorem in the paper Über den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen published in 1898. The general result appeared in the following year in Beweiss des Satzes, dass diejenigen endlichen linearen Substitutionesgruppen, in welchen einige durchgehends verschwindende Coefficienten auftenen intransitiv sind. In his proof Maschke used a theorem by Moore which he had announced to the Mathematics Club at the University of Chicago on 10 July 1896. He had subsequently written it up in a paper which he submitted to Klein for publication in Mathematische Annalen. Klein reported to Moore that Alfred Loewy had stated the result without proof in an article he published in 1896. Moore's paper appeared in Mathematische Annalen two years later and the Loewy-Moore theorem provided Maschke with a critical step in the proof of his own theorem.

Maschke's second area of work was on differential geometry in particular the theory of quadratic differential quantics. In this area, which he started to work in after 1900, he led the symbolic treatment of the subject.

At Chicago, together with Moore, Maschke was responsible for the rapid rise to eminence of the University in mathematics research. David Eugene Smith says:-

He devoted the remainder of his life to the training of mathematicians and to assisting in building up and maintaining a strong department in that university. He was a teacher of great ability and his courses were made more valuable by his all-round culture, by his originality of thought, and by his personal interest in the large numbers of young mathematicians who attended his lectures.

Among the papers he published while at Chicago are: On systems of six points lying in three ways in involution (1896), Note on the unilateral surface of Möbius (1900), A new method of determining the differential parameters and invariants of quadratic differential quantics (1900), On superosculating quadric surfaces (1902), A symbolic treatment of the theory of invariants of quadratic differential quantics of n variables (1903), Differential parameters of the first order (1906); The Kronecker-Gaussian curvature of hyperspace (1906) and A geometrical problem connected with the continuation of a power-series (1906). Six of these papers were published in the Transactions of the American Mathematical Society and Maschke played a large role in getting the American Mathematical Society established, being a founder member of the Chicago Section of the Society in 1897. Maschke served on the Council of the American Mathematical Society from 1902 to 1905 and was vice president of the Society in 1907.

Eliakim Moore recognised the influence of Klein, through Bolza and Maschke, on his leading American research university and wrote to him in 1904 saying:-

Certainly in the domain of mathematics German scholars in general and yourself in particular have played, by way of example and counsel and direct and indirect inspiration, quite a leading role in the development of creative mathematicians in this country ...

At the end of February 1908 Maschke entered hospital to undergo emergency surgery. He died following complications.

Schur

Article by: J J O'Connor and E F Robertson
http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Schur.html

Although Issai Schur was born in Mogilyov on the Dnieper, he spoke German without a trace of an accent, and nobody even guessed that it was not his first language. He went to Latvia at the age of 13 and there he attended the Gymnasium in Libau, now called Liepaja.

In 1894 Schur entered the University of Berlin to read mathematics and physics. Frobenius was one of his teachers and he was to greatly influence Schur and later to direct his doctoral studies. Frobenius and Burnside had been the two main founders of the theory of representations of groups as groups of matrices. This theory proved a very powerful tool in the study of groups and Schur was to learn the foundations of this subject from Frobenius. Schur then made major steps forward, both in work of his own and work done in collaboration with Frobenius.

In 1901 Schur obtained his doctorate with a thesis which examined rational representations of the general linear group over the complex field. Functions which Schur introduced in his thesis are today called S-functions, where the S stands for Schur. Interest in the results of Schur's thesis continues today; for example J A Green published an account of these results in a modern setting in 1980.

In 1903 Schur became a lecturer at Berlin University and then, from 1911 until 1916, he held a professorship in mathematics at the University of Bonn. He returned to Berlin in 1916 and there he built his famous school and spent most of the rest of his life there. He was promoted to full professor in Berlin in 1919, three years after he returned there, and he held this chair until he was dismissed by the Nazis in 1935.

Schur is mainly known for his fundamental work on the representation theory of groups but he also worked in number theory, analysis and other topics described below. Between 1904 and 1907 he worked on projective representations of groups and group characters. One of the most fundamental results which he discovered at this time is today called Schur's Lemma.

In a series of papers he introduced the concept now known as the 'Schur multiplier'. This is an extremely important abstract concept which arose from the concrete problems that Schur was studying. Much later, in 1949, Eilenberg and Mac Lane defined cohomology groups. They were unaware at that time that the second cohomology group with coefficients in the nonzero complex numbers is the Schur multiplier, and therefore that Schur had made some of the first steps forty years earlier.

Around 1914 Schur's interest in representations of groups was put to one side while he worked on other topics but, around 1925, developments in theoretical physics showed that group representations were of fundamental importance in that subject. Schur returned to work on representation theory with renewed vigour and he was able to complete the programme of research begun in his doctoral dissertation and give a complete de-

scription of the rational representations of the general linear group.

Schur was also interested in reducibility, location of roots and the construction of the Galois group of classes of polynomials such as Laguerre and Hermite polynomials. An indication of the other topics that Schur worked on is given:-

First there was pure group theory, in which Schur adopted the surprising approach of proving without the aid of characters, theorems that had previously been demonstrated only by that means. Second, he worked in the field of matrices. Third, he handled algebraic equations, sometimes proceeding to the evaluation of roots, and sometimes treating the so-called equation without affect, that is, with symmetric Galois groups. He was also the first to give examples of equations with alternating Galois groups. Fourth, he worked in number theory; Fifth, in divergent series; Sixth, in integral equations; and lastly in function theory.

The school which Schur built at Berlin was of major importance not only for the representation theory of groups but, as indicated above, for other areas of mathematics. The school partly worked through the Schur's lecturing:-

...there are [many] mathematicians who went to Schur's lectures and seminars in Berlin and were strongly influenced by him...

The school also worked with collaborations:-

A lively interchange with many colleagues led Schur to contribute important memoirs .... Some of these were published as collaborations with other authors, although publications with dual authorship were almost unheard of at that time.

This school was certainly the most coherent and influential group of mathematicians in Berlin, and among the most important in all of Germany. Schur's charismatic leadership inspired those around him to push forward with research on group representations. Schur's own impressive contributions were extended by his students in a number of different directions. They worked on topics such as soluble groups, combinatorics, and matrix theory.

Among the students who completed their doctorates under Schur were Richard Brauer, Alfred Brauer (Richard Brauer's brother), Robert Frucht, Bernhard Neumann, Richard Rado, and Helmut Wielandt. There were others who worked under Schur such as Kurt Hirsch, Walter Ledermann, Hanna Neumann and Menahem Max Schiffer.

Ledermann describes Schur as a teacher:-

Schur was a superb lecturer. His lectures were meticulously prepared... [and] were exceedingly popular. I remember attending his algebra course which was held in a lecture theatre filled with about 400 students. Sometimes, when I had to be content with a seat at the back of the lecture theatre, I used a pair of opera glasses to get at least a glimpse of the speaker.

In 1922 Schur was elected to the Prussian Academy, proposed by Planck, the secretary of the Academy. Planck's address which listed Schur's outstanding achievements had been written by Frobenius, at least five years earlier, as Frobenius died in 1917.

From 1933 events in Germany made Schur's life increasingly difficult. Hirsch spoke of the events of 1 April 1933 when posters carried the message 'Germans defend yourselves against jewish atrocity propaganda : buy only at German shops':-

That was the so-called 'Boycott Day', the day on which Jewish shops were boycotted and Jewish professors and lecturers were not allowed to enter the university. Everybody who was there had to make a little speech about the rejuvenation of Germany etc. And Bieberbach did this quite nicely and then he said 'A drop of remorse falls into my joy because my dear friend and colleague Schur is not allowed to be among us today'.

On 7 April 1933 the Nazis passed a law which, under clause three, ordered the retirement of civil servants who were not of Aryan descent, with exemptions for participants in World War I and pre-war officials. Schur had held an appointment before World War I which should have qualified him as a civil servant, but the facts were not allowed to get in the way, and he was 'retired'. Schiffer wrote :-

When Schur's lectures were cancelled there was an outcry among the students and professors, for Schur was respected and very well liked. The next day Erhard Schmidt started his lecture with a protest against this dismissal and even Bieberbach, who later made himself a shameful reputation as a Nazi, came out in Schur's defence. Schur went on quietly with his work on algebra at home.

Schur saw himself as a German, not a Jew, and could not comprehend the persecution and humiliation he suffered under the Nazis. In fact Schur's dismissal was revoked and he was able to carry out some of his duties for a while. By November 1933 when Walter Ledermann took his Staatsexamen he was examined by Schur together with Bieberbach who was wearing Nazi uniform.

There were invitations to Schur to go to the United States and to Britain but he declined them all, unable to understand how a German was not welcome in Germany.

For example Ledermann obtained a scholarship to go to St Andrews in Scotland in the spring of 1934 and he tried unsuccessfully to persuade Schur to join him in St Andrews.

Schur continued to suffer the humiliation that was heaped on him. Schiffer recalls an event relating to Schur's 60th birthday on 10 January 1935:-

Schur told me that the only person at the Mathematical Institute in Berlin who was kind to him was Grunsky, then a young lecturer. Long after the war, I talked to Grunsky about that remark and he literally started to cry: "You know what I did? I sent him a postcard to congratulate him on his sixtieth birthday. I admired him so much and was very respectful in that card. How lonely he must have been to remember such a small thing."

Later in 1935 Schur was dismissed from his chair in Berlin but he continued to work there suffering great hardship and difficulties. Alfred Brauer writes:-

When Landau died in February 1938, Schur was supposed to give an address at his funeral. For that reason he was in need of some mathematical details from the literature. He asked me to help him in this matter. Of course I was not allowed to use the library of the mathematical institute which I had built up over many years. Finally I got an exemption for a week and could use the library of the Prussian Staatsbibliothek for a fee. ... So I could answer at least some of Schur's questions.

Pressure was put on Schur to resign from the Prussian Academy to which he had been honoured to be elected in 1922. On 29 March 1938 Bieberbach wrote below Schur's signature on a document of the Prussian Academy:-

I find it surprising that Jews are still members of academic commissions.

Just over a week later, on 7 April 1938, Schur resigned from Commissions of the Academy. However, the pressure on him continued and later that year he resigned completely from the Academy.

Schur left Germany for Palestine in 1939, broken in mind and body, having the final humiliation of being forced to find a sponsor to pay the 'Reichs flight tax' to allow him to leave Germany. Without sufficient funds to live in Palestine he was forced to sell his beloved academic books to the Institute for Advanced Study in Princeton. He died two years later on his 66th birthday.

Dedekind

Article by: J J O'Connor and E F Robertson
http://www-groups.dcs.st-and.ac.uk/ history/Biographies/Dedekind.html

Richard Dedekind's father was a professor at the Collegium Carolinum in Brunswick. His mother was the daughter of a professor who also worked at the Collegium Carolinum. Richard was the youngest of four children and never married. He was to live with one of his sisters, who also remained unmarried, for most of his adult life.

He attended school in Brunswick from the age of seven and at this stage mathematics was not his main interest. The school, Martino-Catharineum, was a good one and Dedekind studied science, in particular physics and chemistry. However, physics became less than satisfactory to Dedekind with what he considered an imprecise logical structure and his attention turned towards mathematics.

The Collegium Carolinum was an educational institution between a high school and a university and he entered it in 1848 at the age of 16. There he was to receive a good understanding of basic mathematics studying differential and integral calculus, analytic geometry and the foundations of analysis. He entered the University of Göttingen in the spring of 1850 with a solid grounding in mathematics.

Göttingen was a rather disappointing place to study mathematics at this time, and it had not yet become the vigorous research centre that it turned into soon afterwards. Mathematics was directed by M A Stern and G Ulrich. Gauss also taught courses in mathematics, but mostly at an elementary level. The physics department was directed by Listing and Wilhelm Weber. The two departments combined to initiate a seminar which Dedekind joined from its beginning. There he learnt number theory which was the most advanced material he studied. His other courses covered material such as the differential and integral calculus, of which he already had a good understanding. The first course to really make Dedekind enthusiastic was, rather surprisingly, a course on experimental physics taught by Weber. More likely it was Weber who inspired Dedekind rather than the topic of the course.

In the autumn term of 1850, Dedekind attended his first course given by Gauss. It was a course on least squares and:-

... fifty years later Dedekind remembered the lectures as the most beautiful he had ever heard, writing that he had followed Gauss with constantly increasing interest and that he could not forget the experience.

Dedekind did his doctoral work in four semesters under Gauss's supervision and

submitted a thesis on the theory of Eulerian integrals. He received his doctorate from Göttingen in 1852 and he was to be the last pupil of Gauss. However he was not well trained in advanced mathematics and fully realised the deficiencies in his mathematical education.

At this time Berlin was the place where courses were given on the latest mathematical developments but Dedekind had not been able to learn such material at Göttingen. By this time Riemann was also at Gttingen and he too found that the mathematical education was aimed at students who were intending to become secondary school teachers, not those with the very top abilities who would go on to research careers. Dedekind therefore spent the two years following the award of his doctorate learning the latest mathematical developments and working for his habilitation.

In 1854 both Riemann and Dedekind were awarded their habilitation degrees within a few weeks of each other. Dedekind was then qualified as a university teacher and he began teaching at Göttingen giving courses on probability and geometry.

Gauss died in 1855 and Dirichlet was appointed to fill the vacant chair at Göttingen. This was an extremely important event for Dedekind who found working with Dirichlet extremely profitable. He attended courses by Dirichlet on the theory of numbers, on potential theory, on definite integrals, and on partial differential equations. Dedekind and Dirichlet soon became close friends and the relationship was in many ways the making of Dedekind, whose mathematical interests took a new lease of life with the discussions between the two. Bachmann, who was a student in Göttingen at this time :-

... recalled in later years that he only knew Dedekind by sight because Dedekind always arrived and left with Dirichlet and was completely eclipsed by him.

Dedekind wrote in a letter in July 1856:-

What is most useful to me is the almost daily association with Dirichlet, with whom I am for the first time beginning to learn properly; he is always completely amiable towards me, and he tells me without beating about the bush what gaps I need to fill and at the same time he gives me the instructions and the means to do it. I thank him already for infinitely many things, and no doubt there will be many more.

Dedekind certainly still continued to learn mathematics at this time as a student would by attending courses, such as those by Riemann on abelian functions and elliptic functions. Around this time Dedekind studied the work of Galois and he was the first

to lecture on Galois theory when he taught a course on the topic at Göttingen during this period.

While at Göttingen, Dedekind applied for J L Raabe's chair at the Polytechnikum in Zrich. Dirichlet supported his application writing that Dedekind was 'an exceptional pedagogue'. In the spring of 1858 the Swiss councillor who made appointments came to Göttingen and Dedekind was quickly chosen for the post. Dedekind was appointed to the Polytechnikum in Zrich and began teaching there in the autumn of 1858.

In fact it was while he was thinking how to teach differential and integral calculus, the first time that he had taught the topic, that the idea of a Dedekind cut came to him. He recounts that the idea came to him on 24 November 1858. His idea was that every real number r divides the rational numbers into two subsets, namely those greater than r and those less than r. Dedekind's brilliant idea was to represent the real numbers by such divisions of the rationals.

Dedekind and Riemann travelled together to Berlin in September 1859 on the occasion of Riemann's election to the Berlin Academy of Sciences. In Berlin, Dedekind met Weierstrass, Kummer, Borchardt and Kronecker.

The Collegium Carolinum in Brunswick had been upgraded to the Brunswick Polytechnikum by the 1860s, and Dedekind was appointed to the Polytechnikum in 1862. With this appointment he returned to his home town and even to his old educational establishment where his father had been one of the senior administrators for many years. Dedekind remained there for the rest of his life, retiring on 1 April 1894. He lived his life as a professor in Brunswick:-

... in close association with his brother and sister, ignoring all possibilities of change or attainment of a higher sphere of activity. The small, familiar world in which he lived completely satisfied his demands: in it his relatives completely replaced a wife and children of his own and there he found sufficient leisure and freedom for scientific work in basic mathematical research. He did not feel pressed to have a more marked effect in the outside world: such confirmation of himself was unnecessary.

After he retired, Dedekind continued to teach the occasional course and remained in good health in his long retirement. The only spell of bad health which Dedekind had experienced was 10 years after he was appointed to the Brunswick Polytechnikum when he had a serious illness, shortly after the death of his father. However he completely recovered and, as we mentioned, remained in good health.

Dedekind made a number of highly significant contributions to mathematics and his work would change the style of mathematics into what is familiar to us today. One

remarkable piece of work was his redefinition of irrational numbers in terms of Dedekind cuts which, as we mentioned above, first came to him as early as 1858. He published this in Stetigkeit und Irrationale Zahlen in 1872. In it he wrote:-

Now, in each case when there is a cut (A1, A2) which is not produced by any rational number, then we create a new, irrational number a, which we regard as completely defined by this cut; we will say that this number a corresponds to this cut, or that it produces this cut.

As well as his analysis of the nature of number, his work on mathematical induction, including the definition of finite and infinite sets, and his work in number theory, particularly in algebraic number fields, is of major importance.

Dedekind loved to take his holidays in Switzerland, the Austrian Tyrol or the Black Forest in southern Germany. On one such holiday in 1874 he met Cantor while staying in the beautiful city of Interlaken and the two discussed set theory. Dedekind was sympathetic to Cantor's set theory as is illustrated by this quote from Was sind und was sollen die Zahlen (1888) regarding determining whether a given element belongs to a given set :-

In what way the determination comes about, or whether we know a way to decide it, is a matter of no consequence in what follows. The general laws that are to be developed do not depend on this at all.

In this quote Dedekind is arguing against Kronecker's objections to the infinite and, therefore, is agreeing with Cantor's views.

Among Dedekind's other notable contributions to mathematics were his editions of the collected works of Peter Dirichlet, Carl Gauss, and Georg Riemann. Dedekind's study of Dirichlet's work did, in fact, lead to his own study of algebraic number fields, as well as to his introduction of ideals. Dedekind edited Dirichlet's lectures on number theory and published these as Vorlesungen über Zahlentheorie in 1863. It is noted that:-

Although the book is assuredly based on Dirichlet's lectures, and although Dedekind himself referred to the book throughout his life as Dirichlet's, the book itself was entirely written by Dedekind, for the most part after Dirichlet's death.

It was in the third and fourth editions of Vorlesungen ber Zahlentheorie, published in 1879 and 1894, that Dedekind wrote supplements in which he introduced the notion

of an ideal which is fundamental to ring theory. Dedekind formulated his theory in the ring of integers of an algebraic number field. The general term 'ring' does not appear, it was introduced later by Hilbert.

Dedekind, in a joint paper with Heinrich Weber published in 1882, applies his theory of ideals to the theory of Riemann surfaces. This gave powerful results such as a purely algebraic proof of the Riemann-Roch theorem.

Dedekind's work was quickly accepted, partly because of the clarity with which he presented his ideas and partly since Heinrich Weber lectured to Hilbert on these topics at the University of Königsberg. Dedekind's notion of ideal was taken up and extended by Hilbert and then later by Emmy Noether. This led to the unique factorisation of integers into powers of primes to be generalised to ideals in other rings.

In 1879 Dedekind published Über die Theorie der ganzen algebraischen Zahlen which was again to have a large influence on the foundations of mathematics. In the book Dedekind wrote :-

... presented a logical theory of number and of complete induction, presented his principal conception of the essence of arithmetic, and dealt with the role of the complete system of real numbers in geometry in the problem of the continuity of space. Among other things, he provides a definition independent of the concept of number for the infiniteness or finiteness of a set by using the concept of mapping and treating the recursive definition, which is so important to the theory of ordinal numbers.

Dedekind's brilliance consisted not only of the theorems and concepts that he studied but, because of his ability to formulate and express his ideas so clearly, he introduced a new style of mathematics that been a major influence on mathematicians ever since. As Edwards writes :-

Dedekind's legacy ... consisted not only of important theorems, examples, and concepts, but a whole style of mathematics that has been an inspiration to each succeeding generation.

Many honours were given to Dedekind for his outstanding work, although he always remained extraordinarily modest regarding his own abilities and achievements. He was elected to the Gttingen Academy (1862), the Berlin Academy (1880), the Academy of Rome, the Leopoldino-Carolina Naturae Curiosorum Academia, and the Acadmie des Sciences in Paris (1900). Honorary doctorates were awarded to him by the universities of Kristiania (Oslo), Zurich and Brunswick.

Noether

Article by: J J O'Connor and E F Robertson
http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Noether-Emmy.html

Emmy Noether's father Max Noether was a distinguished mathematician and a professor at Erlangen. Her mother was Ida Kaufmann, from a wealthy Cologne family. Both Emmy's parents were of Jewish origin and Emmy was the eldest of their four children, the three younger children being boys.

Emmy Noether attended the Höhere Töchter Schule in Erlangen from 1889 until 1897. She studied German, English, French, arithmetic and was given piano lessons. She loved dancing and looked forward to parties with children of her father's university colleagues. At this stage her aim was to become a language teacher and after further study of English and French she took the examinations of the State of Bavaria and, in 1900, became a certificated teacher of English and French in Bavarian girls schools.

However Noether never became a language teacher. Instead she decided to take the difficult route for a woman of that time and study mathematics at university. Women were allowed to study at German universities unofficially and each professor had to give permission for his course. Noether obtained permission to sit in on courses at the University of Erlangen during 1900 to 1902. Then, having taken and passed the matriculation examination in Nürnberg in 1903, she went to the University of Göttingen. During 1903-04 she attended lectures by Blumenthal, Hilbert, Klein and Minkowski.

In 1904 Noether was permitted to matriculate at Erlangen and in 1907 was granted a doctorate after working under Paul Gordan. Hilbert's basis theorem of 1888 had given an existence result for finiteness of invariants in n variables. Gordan, however, took a constructive approach and looked at constructive methods to arrive at the same results. Noether's doctoral thesis followed this constructive approach of Gordan and listed systems of 331 covariant forms.

Having completed her doctorate the normal progression to an academic post would have been the habilitation. However this route was not open to women so Noether remained at Erlangen, helping her father who, particularly because of his own disabilities, was grateful for his daughter's help. Noether also worked on her own research, in particular she was influenced by Fischer who had succeeded Gordan in 1911. This influence took Noether towards Hilbert's abstract approach to the subject and away from the constructive approach of Gordan.

Noether's reputation grew quickly as her publications appeared. In 1908 she was elected to the Circolo Matematico di Palermo, then in 1909 she was invited to become

a member of the Deutsche Mathematiker-Vereinigung and in the same year she was invited to address the annual meeting of the Society in Salzburg. In 1913 she lectured in Vienna.

In 1915 Hilbert and Klein invited Noether to return to Göttingen. They persuaded her to remain at Göttingen while they fought a battle to have her officially on the Faculty. In a long battle with the university authorities to allow Noether to obtain her habilitation there were many setbacks and it was not until 1919 that permission was granted. During this time Hilbert had allowed Noether to lecture by advertising her courses under his own name. For example a course given in the winter semester of 1916-17 appears in the catalogue as:-

Mathematical Physics Seminar: Professor Hilbert, with the assistance of Dr E Noether, Mondays from 4-6, no tuition.

Emmy Noether's first piece of work when she arrived in Göttingen in 1915 is a result in theoretical physics sometimes referred to as Noether's Theorem, which proves a relationship between symmetries in physics and conservation principles. This basic result in the general theory of relativity was praised by Einstein in a letter to Hilbert when he referred to Noether's

penetrating mathematical thinking.

It was her work in the theory of invariants which led to formulations for several concepts of Einstein's general theory of relativity.

At Göttingen, after 1919, Noether moved away from invariant theory to work on ideal theory, producing an abstract theory which helped develop ring theory into a major mathematical topic. Idealtheorie in Ringbereichen (1921) was of fundamental importance in the development of modern algebra. In this paper she gave the decomposition of ideals into intersections of primary ideals in any commutative ring with ascending chain condition. Lasker (the world chess champion) had already proved this result for polynomial rings.

In 1924 B L van der Waerden came to Göttingen and spent a year studying with Noether. After returning to Amsterdam van der Waerden wrote his book Moderne Algebra in two volumes. The major part of the second volume consists of Noether's work.

From 1927 on Noether collaborated with Helmut Hasse and Richard Brauer in work on non- commutative algebras.

In addition to teaching and research, Noether helped edit Mathematische Annalen. Much of her work appears in papers written by colleagues and students, rather than under her own name.

Further recognition of her outstanding mathematical contributions came with invitations to address the International Mathematical Congress at Bologna in 1928 and again at Zurich in 1932. In 1932 she also received, jointly with Artin, the Alfred Ackermann-Teubner Memorial Prize for the Advancement of Mathematical Knowledge.

In 1933 her mathematical achievements counted for nothing when the Nazis caused her dismissal from the University of Göttingen because she was Jewish. She accepted a visiting professorship at Bryn Mawr College in the USA and also lectured at the Institute for Advanced Study, Princeton in the USA.

Weyl in his Memorial Address said:-

Her significance for algebra cannot be read entirely from her own papers, she had great stimulating power and many of her suggestions took shape only in the works of her pupils and co-workers.

van der Waerden writes:-

For Emmy Noether, relationships among numbers, functions, and operations became transparent, amenable to generalisation, and productive only after they have been dissociated from any particular objects and have been reduced to general conceptual relationships.

Hermann Weyl

Article by: J J O'Connor and E F Robertson
http://www-groups.dcs.st-and.ac.uk/ history/Biographies/Weyl.html

Hermann Klaus Hugo Weyl (9 November 1885 8 December 1955) was a German mathematician.

Hermann Weyl was known as Peter to his close friends. His parents were Anna Dieck and Ludwig Weyl who was the director of a bank. As a boy Hermann had already showed that he had a great talents for mathematics and for science more generally. After taking his Abiturarbeit (high school graduation exam) he was ready for his university studies. In 1904 he entered the University of Munich, where he took courses on both

mathematics and physics, and then went on to study the same topics at the University of Göttingen. He was completely captivated by Hilbert. He later wrote:-

I resolved to study whatever this man had written. At the end of my first year I went home with the "Zahlberichtünder my arm, and during the summer vacation I worked my way through it - without any previous knowledge of elementary number theory or Galois theory. These were the happiest months of my life, whose shine, across years burdened with our common share of doubt and failure, still comforts my soul.

His doctorate was from Göttingen where his supervisor was Hilbert. After submitting his doctoral dissertation Singuläre Integralgleichungen mit besonder Berücksichtigung des Fourierschen Integraltheorems he was awarded the degree in 1908. This thesis investigated singular integral equations, looking in depth at Fourier integral theorems. It was at Göttingen that he held his first teaching post as a privatdozent, a post he held until 1913. His habilitation thesis Über gewöhnliche Differentialgleicklungen mit Singularitäten und die zugehörigen Entwicklungen willkürlicher Funktionen investigated the spectral theory of singular Sturm-Liouville problems. During this period at Göttingen, Weyl made a reputation for himself as an outstanding mathematician who was producing work which was having a major impact on the progress of mathematics. His habilitation thesis was one such piece of work but there was much more. He gave a lecture course on Riemann surfaces in session 1911-12 and out of this course came his first book Die Idee der Riemannschen Flche which was published in 1913. It united analysis, geometry and topology, making rigorous the geometric function theory developed by Riemann. The book introduced for the first time the notion of a:-

... two-dimensional differentiable manifold, a covering surface, and the duality between differentials and 1-cycles. ...Weyl's idea of a space also included the famous separation property later introduced and popularly credited to Felix Hausdorff (1914).

L Sario wrote in 1956 that Weyl's 1913 text:-

... has undoubtedly had a greater influence on the development of geometric function theory than any other publication since Riemann's dissertation.

It is rather remarkable that this 1913 text was reprinted in 1997. Weyl himself produced two later editions, the third (and final) of these editions appearing in 1955 covering the same topics as the original text but with a more modern treatment. It was the original 1913 edition, however, which was reprinted in 1997 showing perhaps

more fully than the later editions just how significant the original 1913 text was in the development of mathematics.

As a privatdozent at Göttingen, Weyl had been influenced by Edmund Husserl who held the chair of philosophy there from 1901 to 1916. Weyl married Helene Joseph, who had been a student of Husserl, in 1913; they had two sons. Helene, who came from a Jewish background, was a philosopher who was working as a translator of Spanish. Not only did Weyl and his wife share an interest in philosophy, but they shared a real talent for languages. Language for Weyl held a special importance. He not only wrote beautifully in German, but later he wrote stunning English prose despite the fact that, in his own words from a 1939 English text:-

... the gods have imposed upon my writing the yoke of a foreign language that was not sung at my cradle.

From 1913 to 1930 Weyl held the chair of mathematics at Zrich Technische Hochschule. In his first academic year in this new post he was a colleague of Einstein who was at this time working out the details of the theory of general relativity. It was an event which had a large influence on Weyl who quickly became fascinated by the mathematical principles lying behind the theory.

World War I broke out not long after Weyl took up the chair in Zürich. Being a German citizen he was conscripted into the German army in 1915 but the Swiss government made a special request that he be allowed to return to his chair in Zrich which was granted in 1916. In 1917 Weyl gave another course presenting an innovative approach to relativity through differential geometry. The lectures formed the basis of Weyl's second book Raum-Zeit-Materie which first appeared in 1918 with further editions, each showing how his ideas were developing, in 1919, 1920, and 1923. These later ideas included a gauge metric (the Weyl metric) which led to a gauge field theory. However Einstein, Pauli, Eddington, and others, did not fully accept Weyl's approach. Also over this period Weyl also made contributions on the uniform distribution of numbers modulo 1 which are fundamental in analytic number theory.

In 1921 Schrödinger was appointed to Zurich where he became a colleague, and soon closest friend, of Weyl. They shared many interests in mathematics, physics, and philosophy. Their personal lives also became entangled as Moore relates:-

Those familiar with the serious and portly figure of Weyl at Princeton would have hardly recognised the slim, handsome young man of the twenties, with his romantic black moustache. His wife, Helene Joseph, from a Jewish background, was a philosopher and literateuse. Her friends called her Hella, and a certain daring and

insouciance made her the unquestioned leader of the social set comprising the scientists and their wives. Anny [Schrödinger's wife] was almost an exact opposite of the stylish and intellectual Hella, but perhaps for that reason [Weyl] found her interesting and before long she was madly in love with him. ... The special circle in which they lived in Zurich had enjoyed the sexual revolution a generation before [the United States]. Extramarital affairs were not only condoned, they were expected, and they seemed to occasion little anxiety. Anny would find in Hermann Weyl a lover to whom she was devoted body and soul, while Weyl's wife Hella was infatuated with Paul Scherrer.

From 1923-38 Weyl evolved the concept of continuous groups using matrix representations. In particular his theory of representations of semisimple groups, developed during 1924-26, was very deep and considered by Weyl himself to be his greatest achievement. The ideas behind this theory had already been introduced by Hurwitz and Schur, but it was Weyl with his general character formula which took them forward. He was not the only mathematician developing this theory, however, for Cartan also produced work on this topic of outstanding importance.

From 1930 to 1933 Weyl held the chair of mathematics at Göttingen where he was appointed to fill the vacancy which arose on Hilbert's retirement. Given different political circumstances it is likely that he would have remained in Göttingen for the rest of his career. However:-

... the rise of the Nazis persuaded him in 1933 to accept a position at the newly formed Institute for Advanced Study in Princeton, where Einstein also went. Here Weyl found a very congenial working environment where he was able to guide and influence the younger generation of mathematicians, a task for which he was admirably suited.

One also has to understand that Weyl's wife was Jewish, and this must have played a major role in their decision to leave Germany in 1933. Weyl remained at the Institute for Advanced Study at Princeton until he retired in 1952. His wife Helene died in 1948, and two years later he married the sculptor Ellen Lohnstein Bär from Zürich.

Weyl certainly undertook work of major importance at Princeton, but his most productive period was without doubt the years he spent at Zrich. He attempted to incorporate electromagnetism into the geometric formalism of general relativity. He produced the first unified field theory for which the Maxwell electromagnetic field and the gravitational field appear as geometrical properties of space-time. With his application of group theory to quantum mechanics he set up the modern subject. It was his lecture course on group theory and quantum mechanics in Zrich in session 1927-28 which led to his third major text Gruppentheorie und Quantenmechanik published in 1928. John Wheeler writes:-

That book has, each time I read it, some great new message.

More recently attempts to incorporate electromagnetism into general relativity have been made by Wheeler. Wheeler's theory, like Weyl's, lacks the connection with quantum phenomena that is so important for interactions other than gravitation. Wheeler writes about meeting Weyl for the first time:-

Erect, bright-eyed, smiling Hermann Weyl I first saw in the flesh when 1937 brought me to Princeton. There I attended his lectures on the lie Cartan calculus of differential forms and their application to electromagnetism - eloquent, simple, full of insights.

We have seen above how Weyl's great works were first given as lecture courses. This was a deliberate design by Weyl:-

At another time Weyl arranged to give a course at Princeton University on the history of mathematics. He explained to me one day that it was for him an absolute necessity to review, by lecturing, his subject of concern in all its length and breadth. Only so, he remarked, could he see the great lacunae, the places where deeper understanding is needed, where work should focus.

Many other great books by Weyl appeared during his years at Princeton. These include Elementary Theory of Invariants (1935), The classical groups (1939), Algebraic Theory of Numbers (1940), Philosophy of Mathematics and Natural Science (1949), Symmetry (1952), and The Concept of a Riemannian Surface (1955). There is so much that could be said about all these works, but we restrict ourselves to looking at the contents of Symmetry for this perhaps tells us most about the full range of Weyl's interests. Coxeter reviewed the book and his review beautifully captures the spirit of the book:-

This is slightly modified version of the Louis Clark Vanuxem Lectures given at Princeton University in 1951 ... The first lecture begins by showing how the idea of bilateral symmetry has influenced painting and sculpture, especially in ancient times. This leads naturally to a discussion of "the philosophy of left and right", including such questions as the following. Is the occurrence in nature of one of the two enantiomorphous forms of an optically active substance characteristic of living matter? At what stage in the development of an embryo is the plane of symmetry determined? The second lecture contains a neat exposition of the theory of groups of transformations, with special emphasis on the group of similarities and its subgroups:

the groups of congruent transformations, of motions, of translations, of rotations, and finally the symmetry group of any given figure. ... the cyclic and dihedral groups are illustrated by snowflakes and flowers, by the animals called Medusae, and by the plans of symmetrical buildings. Similarly, the infinite cyclic group generated by a spiral similarity is illustrated by the Nautilus shell and by the arrangement of florets in a sunflower. The third lecture gives the essential steps in the enumeration of the seventeen space-groups of two-dimensional crystallography ... [In the fourth lecture he] shows how the special theory of relativity is essentially the study of the inherent symmetry of the four-dimensional space-time continuum, where the symmetry operations are the Lorentz transformations; and how the symmetry operations of an atom, according to quantum mechanics, include the permutations of its peripheral electrons. Turning from physics to mathematics, he gives an extraordinarily concise epitome of Galois theory, leading up to the statement of his guiding principle: "Whenever you have to do with a structure-endowed entity, try to determine its group of automorphisms".

In 1951 Weyl retired from the Institute for Advanced Study at Princeton. In fact he described the Symmetry book as his 'swan song'. After his retirement Weyl and his wife Ellen spent part of their time at Princeton and part at Zurich. He died unexpectedly while in Zurich. He was walking home after posting letters of thanks to those who had wished him well on his seventieth birthday when he collapsed and died.

We must say a little about another aspect of Weyl's work which we have not really mentioned, namely his work on mathematical philosophy and the foundations of mathematics. It is interesting to note what a large number of the references we quote deal with this aspect of his work and its importance is not only in the work itself but also in the extent to which Weyl's ideas on these topics underlies the rest of his mathematical and physical contributions. Weyl was much influenced by Husserl in his outlook and also shared many ideas with Brouwer. Both shared the view that the intuitive continuum is not accurately represented by Cantor's set-theoretic continuum. Wheeler writes:-

The continuum ..., Weyl taught us, is an illusion. It is an idealization. It is a dream.

Weyl summed up his attitude to mathematics, writing:-

My own mathematical works are always quite unsystematic, without mode or connection. Expression and shape are almost more to me than knowledge itself. But I believe that, leaving aside my own peculiar nature, there is in mathematics itself, in contrast to the experimental disciplines, a character which is nearer to that of free creative art.

His often quoted comment:-

My work always tried to unite the truth with the beautiful, but when I had to choose one or the other, I usually chose the beautiful ...

although half a joke, sums up his personality.

Bézout

Article by: J J O'Connor and E F Robertson, http://www-groups.dcs.st-and.ac.uk/∼ history/Mathematicians

Étienne Bézout's father was Pierre Bézout who was a magistrate in the town of Nemours. One might have expected Étienne to follow the same career, for his grandfather had also been a magistrate in Nemours. Étienne's mother was Hélène-Jeanne Filz.

As we have already indicated the family tradition almost demanded that Étienne follow in his father and grandfather's footsteps. However the remarkable mathematics of Leonard Euler proved stronger than his parents wishes, for once Bézout had read Euler's works he wished to devote himself to mathematics. In 1756 he published a memoir Dynamique. In the following year he published Quantités différentielles and in 1758 Rectification des courbes. These latter two papers were investigations of integration.

In 1758 Bézout was appointed an adjoint in mechanics of the Académie des Sciences and, in the same year, as royal censor. He was appointed examiner of the Gardes de la Marine in 1763, the post being offered to him by the Duke of Choiseul. One important task that he was given in this role was to compose a textbook specially designed for teaching mathematics to the students.

Bézout is famed for the texbooks which came out of this assignment. The first was Cours de mathématiques l'usage des Gardes du Pavillon et de la Marine, a four volume work which appeared in 1764-67.

In 1768 Camus, who was the examiner for the artillery, died. Bézout was appointed to succeed him becoming examiner of the Corps d'Artillerie. He began work on another mathematics textbook and as a result he produced Cours complet de mathématiques l'usage de la marine et de l'artillerie, a six volume work which appeared between 1770 and 1782. This was a very successful textbook and for many years it was the book which students hoping to enter the École Polytechnique studied. Grabiner writes:-

The experience of teaching non-mathematicians shaped the style of the works: Bézout treated geometry before algebra, observing that beginners were not yet familiar enough with mathematical reasoning to understand the force of algebraic demonstrations, although they did appreciate proofs in geometry. He eschewed the frightening terms äxiom", "theorem", "scholium", and tried to avoid arguments that were too close and detailed.

As might be expected given this approach aimong at the readership for whom Bézout intended his texts, his books came in for a certain amount of criticism for lacking rigour. However, despite this they were books which could be understood by those who needed to use mathematics and as a result were very popular and widely used. Their use spread beyond France for they were translated into English and used in North America. In particular Harvard University adopted them as calculus textbooks.

Returning to give more information about Bézout's career, we should note that he was promoted to associé in mechanics at the Académie des Sciences in 1768 and then further promoted to pensionnaire in 1770.

As we have indicated Bézout is famed for being a writer of textbooks but he is famed also for his work on algebra, in particular on equations. He was much occupied with his teaching duties after his 1763 appointments and he took these very seriously indeed. As a consequence he could devote relatively little time to research and he made a conscience decision to restrict the range of his work so that he could produce worthwhile results in a narrow order.

The way Bézout went about his research is interesting since still today it is a good approach for obtaining results. He attacked quite general problems, but since an attack was usually beyond what could be achieved with the mathematical knowledge then available, he attacked special cases of the general problems which he could solve. This approach often leads slowly to more and more understanding of the general case which may eventually become soluble. Bézout had a name for this approach to mathematics, namely the "method of simplifying assumptions".

His first paper on the theory of equations Sur plusieurs classes d'équations de tous les degrés qui admettent une solution algébrique examined how a single equation in a single unknown could be attacked by writing it as two equations in two unknowns. He wrote in this paper:-

It is known that a determinate equation can always be viewed as the result of two equations in two unknowns, when one of the unknowns is eliminated.

Of course on the face of it this does not help solve the equation but Bézout made the simplifying assumption that one of the two equations was of a particularly simple

form. For example he considered the case when one of the two equations had only two terms, the term of degree n and a constant term. Already this paper had introduced the topic to which Bézout would make his most important contributions, namely methods of elimination to produce from a set of simultaneous equations, a single resultant equation in one of the unknowns.

He also did important work on the use of determinants in solving equations. This appears in a paper Sur le degré des équations résultantes de l'évanouissement des inconnues which he published in 1764. As a result of the ideas in this paper for solving systems of simultaneous equations, Sylvester, in 1853, called the determinant of the matrix of coefficients of the equations the Bézoutiant.

These and further papers published by Bézout in the theory of equations were gathered together in Théorie générale des équations algébraiques which was published in 1779. This work includes a result known as Bézout's theorem:-

The degree of the final equation resulting from any number of complete equations in the same number of unknowns, and of any degrees, is equal to the product of the degrees of the equations.

By a complete equation Bézout meant one defined by a polynomial which contains terms of all possible products of the unknowns whose degree does not exceed that of the polynomial. One has to understand the problems that faced Bézout for he did not have our simple suffix notation to denote the unknowns by x1, x2, x3, ... nor could he even label his equations with a suffix notation. Despite this Bézout, who was prepared to enter long and difficult algebraic manipulations, proved his theorem with just a little hand waving over an inductive argument.

In this work Bézout also gave the first satisfactory proof of a result of Maclaurin on the intersection of two algebraic curves.

Grabiner tells us that:-

Bézout married early and happily; although he was reserved and somewhat sombre in society, those who knew him spoke of his great kindness and warm heart. By 1763 Bézout had become a father ...

After his death in 1783 a statue was erected in Nemours, the town of his birth, to commemorate his great achievements.

Zorn

Article by: J J O'Connor and E F Robertson
http://www-groups.dcs.st-and.ac.uk/∼ history/Mathematicians

Max Zorn was born in Krefeld in western Germany, about 20 km northwest of Dusseldorf. He attended Hamburg University where he studied under Artin. Hamburg was Artin's first academic appointment and Zorn became his second doctoral student. He received his Ph.D. from Hamburg in April 1930 for a thesis on alternative algebras. We shall explain below what an alternative algebra is and describe some of the mathematical contributions which Zorn made at this time. At this stage, however, we should comment that his achievements were considered outstanding by the University of Hamburg and he was awarded a university prize. He was appointed as an assistant at Halle but he did not have the opportunity to work there for long since, in 1933, he was forced to leave Germany because of the Nazi policies. He was not, however, Jewish.

Zorn emigrated to the United States and was appointed a Sterling Fellow at Yale University. He worked there from 1934 to 1936 and it was during this period that he proposed "Zorn's Lemma"for which he is best known. We describe below the form in which Zorn originally stated this result. Following his years at Yale, he moved to the University of California at Los Angeles where he remained until 1946. During this time Herstein was one of his doctoral students. He left the University of California to become professor at Indiana University, holding this position from 1946 until he retired in 1971.

Since Zorn is best known for "Zorn's Lemmaït is perhaps appropriate that we should begin a discussion of his mathematical achievements by considering this contribution. Of course Zorn did not call his result "Zorn's Lemma", rather it was given by him as a "maximum principleïn a short paper entitled A remark on method in transfinite algebra which he published in the Bulletin of the American Mathematical Society in 1935. Perhaps in passing we should note that the name "Zorn's Lemma"was due to John Tukey. Zorn's aim in this paper was to study field theory and in particular to improve on the method used for obtaining results in the subject. Methods used up to that time had depended heavily on the well-ordering principle which Zermelo had proposed in 1904, namely that every set can be well-ordered. What Zorn proposed in the 1935 paper was to develop field theory from the standard axioms of set theory, together with his maximum principle rather than Zermelo's well-ordering principle.

The form in which Zorn stated his maximum principle was as follows. The principle involved chains of sets. A chain is a collection of sets with the property that for any two sets in the chain, one of the two sets is a subset of the other. Zorn defined a collection of sets to be closed if the union of every chain is in the collection. His maximum principle

asserted that if a collection of sets is closed, then it must contain a maximal member, that is a set which is not a proper subset of some other in the collection. The paper then indicated how the maximum principle could be used to prove the standard field theory results.

Today we know that the Axiom of Choice, the well-ordering principle, and Zorn's Lemma (the name now given to Zorn's maximum principle by Tukey and now the standard name) are equivalent. Did Zorn know this when he wrote his 1935 paper? Well at the end of the 1935 paper he did say that these three are all equivalent and promised a proof in a future paper. Was Zorn's idea entirely new? Well similar maximum principles had been proposed earlier in different contexts by several mathematicians, for example Hausdorff, Kuratowski and Brouwer. Paul Campbell examines this question and:-

... investigates the claim that "Zorn's Lemma" is not named after its first discoverer, by carefully tracing the origins of several related maximal principles and of the name "Zorn's Lemma".

Zorn made other contributions to set theory, such as his 1944 paper Idempotency of infinite cardinals in which he proved that an infinite cardinal number is equal to its square. His proof uses his maximum principle rather than using ordinal numbers as had been done in previous proofs of the result.

In addition to his well known work in infinite set theory, Zorn worked on topology and algebra. As we mentioned above his doctoral thesis was on alternative algebras. These are algebras in which (xy)z - x(yz) is an alternating function in the sense that it is zero whenever any two of x, y, z are equal or, put another way, any two dimensional subalgebra is associative. Zorn went on to publish four papers on alternative algebras. He proved the uniqueness of the Cayley numbers (or octonians) in 1933 by showing that it was the only alternative, quadratic, real nonassociative algebra without zero divisors. He studied the structure of semisimple alternative rings in 1932, proving that such a ring is a direct sum of simple alternative algebras which he classified. In Alternative rings and related questions I: existence of the radical published in 1941 Zorn considered the theory of the radical of an alternative ring. He also published results on algebras which were fundamental in the study of algebraic number fields.

We have looked briefly at Zorn's contributions to algebra and to set theory. Let us now take a brief look at his contributions to analysis. In 1945 he published the paper Characterization of analytic functions in Banach space in the Annals of Mathematics. We quote from the introduction to that paper since it both states the type of problems that Zorn was examining very clearly, and also because it illustrates his clear style of writing mathematics:-

The concept of analyticity may be extended in various ways to functions from one complex Banach space to another. We may ask that the function be differentiable on one-dimensional (complex) subspaces; here one is led to the theory of the Gâteaux differential. Or we may prescribe a seemingly much more powerful condition, namely, that the function possesses a development into (abstract) power series about each point of the domain of definition. Here the Fréchet differential plays a decisive role.

The characterization theorem which we are going to derive will serve to show that the functions which fall under the first definition but not under the second are, from a certain point of view, to be considered as freaks, counter examples rather than examples. They are similar in character to, say, additive functions of a real variable which are not linear. For it turns out that only a very weak continuity property has to be added to the existence of the Gâteaux differential in order to ensure the existence of the power series development called for by the second definition.

After 1947 Zorn stopped publishing mathematical papers. This does not mean that he gave up mathematics. As Haile said at the Memorial Symposium held for Zorn at Indiana University in June 1993:-

... Max's published work, as significant and substantial as it is, is not what we will remember him by. It is rather Max's life-long dedication to mathematics and his apparently endless curiosity about mathematical ideas that we remember and from which we draw inspiration.

Ewing writes:-

In his retirement Max Zorn became an essential part of the department. He came to the office every day, seven days a week. He was at tea, at seminars, and at colloquia. His questions were often penetrating and sometimes enigmatic. Outside speakers were usually charmed by Max and his passion for mathematics.

Halmos also describes the colloquia:-

I don't remember any colloquium at which he didn't ask a question afterwards (and sometimes during) - a relevant question, a pertinent question, a sharp question. His questions showed that he understood the subject, understood the talk, and was ready to understand and remember the answers.

Returning to Ewing:-

In recent years Max became fascinated by the Riemann Hypothesis and possible proofs using techniques from functional analysis. He read and studied and talked about mathematics nearly every day of his life. From time to time he published a slim newsletter, the Piccayune Sentinel, devoted to cryptic remarks about mathematics and mathematicians. He was a gentle man with a sharp wit who, during nearly half a century, inspired and charmed his colleagues at Indiana University.

Perhaps the reference to the Piccayune Sentinel deserves comment. Zorn did spell this with two c's but it is named after the newspaper the New Orleans Picayune. Halmos gives more details:-

I don't know just when he started it; the first issue that I have a copy of is dated November 1950. It was a one-sheet affair that Max called the world's smallest newspaper and that he gave to a few friends (usually by putting copies into his colleagues' mailboxes, and rarely, for distant friends, by mailing them). ... The contents of the Piccayune Sentinel were of the same kind as Max himself and his postcards (and as unpredictable and as confusion-inducing) ...

Max Zorn married Alice Schlottau and they had one son Jens and one daughter Liz.