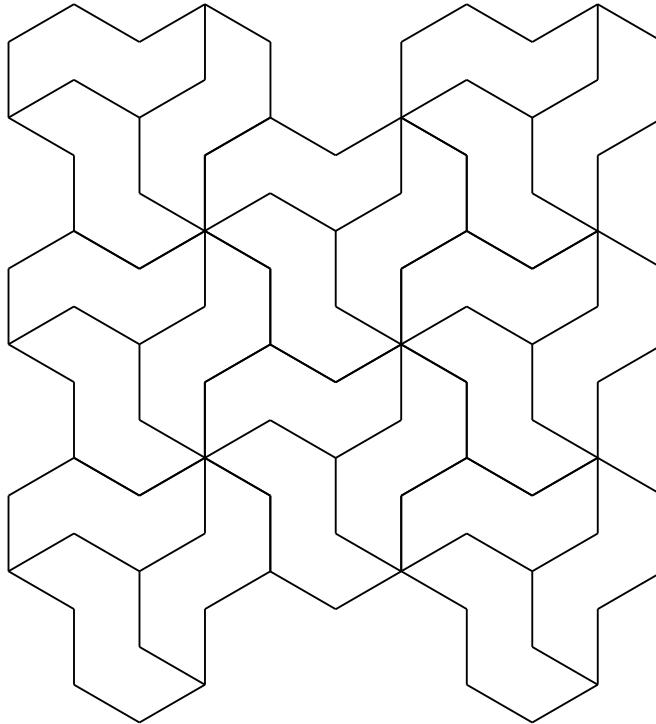


1 Symmetrie en transformatiegroepen

Het thema van deze cursus is het begrip *symmetrie*. Wat betekent het dat een object symmetrie bezit? Laten we deze vraag bestuderen aan de hand van een voorbeeld met een grote mate van symmetrie. In figuur ziet

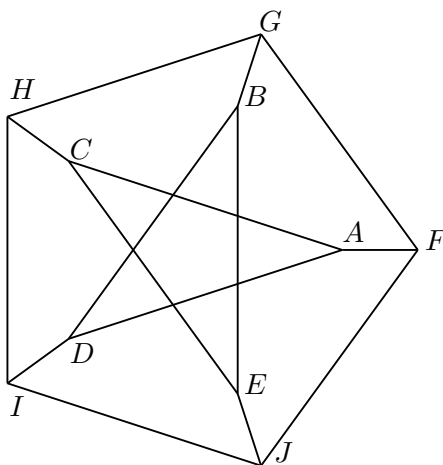


Figuur 1: Een stukje uit een regelmatige vlakverdeling.

men aangegeven hoe men het vlak zou kunnen opvullen met een bepaald model ‘tegels’: copieën van een vaste figuur. Het feit dat de tegels star zijn en een vast model hebben betekent dat de plaatsing van elk tweetal tegels verbonden is door een afbeelding $f: \mathbf{R}^2 \rightarrow \mathbf{R}^2$ die afstanden bewaart.

Dat de vlakverdeling regelmatig is betekent dat er afbeeldingen f van dit type zijn die het *hele* patroon in zichzelf overvoeren: het beeld onder f van een goed geplaatste tegel is weer een goede plek voor een tegel. Een afbeelding zoals hier die de relevante structuur bewaart noemen we een *symmetrie*. Hoe meer dergelijke afbeeldingen er zijn, hoe regelmatiger we de situatie vinden. Het is daarom zinvol om een studie te maken van de verzameling G van *alle* afbeeldingen die de structuur bewaren.

Wat wel of niet tot G behoort is natuurlijk afhankelijk welke structuur relevant gevonden wordt. We illustreren dat met een tweede voorbeeld, nu geen tegelpatroon maar een netwerk van verbindingen. Als we op de lengtes



Figuur 2: Een netwerk van verbindingen.

van de lijnstukken letten dan heeft deze figuur 10 symmetrieën (inclusief de identieke afbeelding): 5 draaiingen en 5 spiegelingen. Letten we nu echter niet op de lengtes maar alleen op het al dan niet verbonden zijn van een tweetal punten. Het gaat dan over een verzameling van 10 elementen A, \dots, J tesamen met een collectie paren $\{A, C\}, \dots, \{I, J\}$. In dit geval telt dit object maar liefst 120 symmetrieën. Zo bijvoorbeeld de afbeelding f gegeven door

$$\begin{aligned} f(A) &= A, & f(B) &= H, & f(C) &= D, & f(D) &= C, & f(E) &= I, \\ f(F) &= F, & f(G) &= G, & f(H) &= B, & f(I) &= E, & f(J) &= J \end{aligned}$$

We vatten de voorgaande beschouwing nu samen. Er is gegeven een verzameling X (in het eerste voorbeeld het vlak \mathbf{R}^2 , in het tweede geval de verzameling A, \dots, J). Verder is gegeven een zekere extra structuur op X , bijvoorbeeld in de vorm van een collectie deelverzamelingen van X . De mate van symmetrie van dit geheel wordt beschreven door een zekere collectie G van afbeeldingen van X naar zichzelf, namelijk al de afbeeldingen die de voorhanden structuur precies in zich zelf overvoeren. We constateren nu dat G de volgende eigenschappen heeft

- De identieke afbeelding 1_X van X ligt in G .
- Als $f \in G$ dan is f een bijectie, en $f^{-1} \in G$
- Als $f \in G$ en $g \in G$ dan $f \circ g \in G$.

Definitie 1.1. Zij gegeven een verzameling X . Een collectie afbeeldingen van X naar zichzelf die aan bovenstaande drie eisen voldoet noemen we een *groep van transformaties* van X .

Voorbeeld 1.2. Zij X een verzameling die niet leeg is, en zij G de verzameling van *alle* bijecties $\sigma: X \rightarrow X$. Dan is duidelijk aan bovenstaande eisen voldaan. We noemen deze G de *symmetrische groep* of *permutatie-groep* van X en noteren hem als $\text{Sym}(X)$. In het geval $X = \{1, 2, \dots, n\}$ met $n \in \mathbf{N}$ schrijven we S_n voor $\text{Sym}(X)$. Een notatie voor een element $\sigma \in S_n$ is

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Het aantal elementen van S_n is dus $n \cdot (n-1) \dots 2 \cdot 1 = n!$. Zo geldt bijvoorbeeld in S_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Voorbeeld 1.3. Zij $\mathbf{F} = \mathbf{Q}, \mathbf{R}$ of \mathbf{C} en zij X een eindig-dimensionale vectorruimte over \mathbf{F} . Afbeeldingen $A: X \rightarrow X$ die de structuur van vectorruimte over \mathbf{F} respecteren kennen we als *lineaire* afbeeldingen, en een lineaire afbeelding heeft een inverse precies als zijn determinant niet nul is. In Aanhangsel 12 geven we een samenvatting van de theorie van matrices en determinanten. De collectie G bestaande uit deze lineaire bijecties noemen we de *algemene lineaire groep* van X en we noteren deze als $\text{GL}(X)$. Als $X = \mathbf{F}^n$ dan noteren we ook wel $\text{GL}(n, \mathbf{F})$ of $\text{GL}_n(\mathbf{F})$.

Voorbeeld 1.4. Als in bovenstaande situatie de determinant van A zelfs precies 1 is dan betekent dat meetkundig dat A ook nog volume behoudt (omdat deze cursus niet over volumens en integratie gaat kunnen we deze opmerking hier niet verder toelichten). De collectie G bestaande uit deze lineaire afbeeldingen $X \rightarrow X$ met determinant 1 noemen we de *speciale lineaire groep* van X en we noteren deze als $\text{SL}(X)$. Als $X = \mathbf{F}^n$ dan noteren we ook wel $\text{SL}(n, \mathbf{F})$ of $\text{SL}_n(\mathbf{F})$.

Voorbeeld 1.5. Zij X een eindig-dimensionale vectorruimte over \mathbf{R} . Zij $A \in \text{GL}(X)$ en $v \in X$ en zij $f: X \rightarrow X$ de afbeelding gegeven door

$$f(x) = A(x) + v$$

Dan is f continu en bijectief en hij voert lijnen in lijnen over. Men kan bewijzen dat omgekeerd elke continue bijectieve afbeelding die lijnen in lijnen overvoert van bovenstaande vorm is, en dus een samenstelling van een lineaire transformatie A en een afbeelding van de vorm $X \mapsto x + v$, de zogenaamde *verschuiving* of *translatie* over v . De verzameling van al zulke afbeeldingen vormt een groep van transformaties van X genaamd de *affiene groep* van X , en we noteren deze als $\text{Aff}(X)$. Als $X = \mathbf{F}^n$ dan noteren we ook wel $\text{Aff}(n, \mathbf{F})$ of $\text{Aff}_n(\mathbf{F})$.

Voorbeeld 1.6. Zij nu X een eindig-dimensionale vectorruimte over \mathbf{R} voorzien van een scalair product B . In het Aanhangsel 12.5 geven we een samenvatting van de theorie van scalaire producten. De afbeeldingen $f: X \rightarrow X$ die niet alleen de vectorruimte-structuur op X bewaren maar ook het scalaire product B zijn precies de *orthogonale transformaties* van (X, B) . Daarom noemen we de verzameling van al deze afbeeldingen de *orthogonale groep* van (X, B) en noteren we deze met $O(X, B)$. Als $X = \mathbf{R}^n$ en B het standaard scalair product is dan schrijven we meestal $O(n)$.

Voorbeeld 1.7. In de voorgaande situatie kunnen we ook de aandacht beperken tot lineaire transformaties die zowel orthogonaal zijn als van determinant 1. De resulterende groep van transformaties noemen we de *speciale orthogonale groep* van (X, B) en we noteren daarvoor $SO(X, B)$. Er geldt dus $SO(X, B) = O(X, B) \cap SL(X)$. Als $X = \mathbf{R}^n$ en B het standaard scalair product is dan schrijven we meestal $SO(n)$.

Voorbeeld 1.8. Zij nu X een eindig-dimensionale vectorruimte over \mathbf{C} voorzien van een Hermiets inproduct H . In het Aanhangsel 12.6 geven we een samenvatting van de theorie van dergelijke koppels (X, H) . De afbeeldingen $f: X \rightarrow X$ die niet alleen de vectorruimte-structuur op X bewaren maar ook het inproduct H zijn precies de *unitaire transformaties* van (X, H) ; Daarom noemen we de verzameling van al deze afbeeldingen de *unitaire groep* van (X, H) en noteren we deze met $U(X, H)$. Als $X = \mathbf{C}^n$ en H het standaard inproduct is dan schrijven we meestal $U(n)$.

In de voorgaande situatie kunnen we ook de aandacht beperken tot lineaire transformaties die zowel unitair zijn als van determinant 1. De resulterende groep van transformaties noemen we de *speciale unitaire groep* van (X, H) en we noteren daarvoor $SU(X, H)$. Er geldt dus $SU(X, H) = U(X, H) \cap SL(X)$. Als $X = \mathbf{C}^n$ en H het standaard inproduct is dan schrijven we meestal $SU(n)$.

Voorbeeld 1.9. Zij nu X een eindig-dimensionale vectorruimte over \mathbf{R} voorzien van een scalair product B . Zij $A \in O(X, B)$ en $v \in X$ en zij $f: X \rightarrow X$ de afbeelding gegeven door

$$f(x) = A(x) + v$$

Dan geldt $\|f(x) - f(y)\| = \|x - y\|$ voor alle $x, y \in X$, wat betekent dat f afstanden bewaart. Men kan bewijzen dat elke afbeelding die afstanden bewaart van bovenstaande vorm is, en dus een samenstelling is van een orthogonale lineaire transformatie en een translatie. De verzameling van al zulke afbeeldingen vormt een groep van transformaties van X , genaamd de bewegingsgroep $E(X, B)$.

Opmerking 1.10. Zij gegeven een groep van transformaties G van een verzameling X . Zij verder gegeven een verzameling Y en een bijectieve

afbeelding $\beta: X \rightarrow Y$. Dan krijgen we als volgt een groep van transformaties van Y :

$$H = \{\beta \circ f \circ \beta^{-1} ; f \in G\}$$

De afbeelding $\phi: G \rightarrow H$ gegeven door $\phi(f) = \beta \circ f \circ \beta^{-1}$ is bijectief en voldoet aan

- $\phi(1_X) = 1_Y$
- $\phi(f) \circ \phi(g) = \phi(f \circ g)$ voor alle $f, g \in G$.

We komen in Hoofdstuk 3 terug op dit stel eisen.

Opmerking 1.11. Zij gegeven een groep van transformaties G van een verzameling X , en een groep van transformaties H van een verzameling Y . Zoals bekend staat de notatie $X \times Y$ voor de verzameling van alle paren (x, y) waar $x \in X$ en $y \in Y$. Nu hoort bij elke $(g, h) \in G \times H$ een bijectieve afbeelding van $X \times Y \rightarrow X \times Y$, namelijk de afbeelding die aan (x, y) toevoegt $(g(x), h(y))$. Op deze manier is $G \times H$ op te vatten als groep van transformaties van de verzameling $X \times Y$.

2 Eindige voorbeelden in \mathbf{R}^3 .

In dit Hoofdstuk geven we een opsomming van de eindige groepen van orthogonale lineaire transformaties van \mathbf{R}^2 en van \mathbf{R}^3 .

We kijken eerst naar groepen van orthogonale transformaties van \mathbf{R}^2 . Gemakshalve identificeren we elke lineaire afbeelding $\mathbf{R}^2 \rightarrow \mathbf{R}^2$ met zijn 2×2 matrix.

Voorbeeld 2.1. Zij $n \in \mathbf{Z}$ positief. Voor $k \in \mathbf{Z}$ definiëren we $r_{n,k} \in \text{SO}(2)$ door

$$r_{n,k} = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix}$$

Uit de eigenschappen van \cos en \sin leid je gemakkelijk de volgende feiten af:

- $r_{n,0}$ is de identieke afbeelding,
- $r_{n,k} \circ r_{n,m} = r_{n,k+m}$
- $r_{n,-k}$ is de inverse van $r_{n,k}$.
- $r_{n,k} = r_{n,m}$ dan en slechts dan als $m - k$ een geheel veelvoud is van n .

Hieruit blijkt dat de *cyclische groep* $C_n = \{r_{n,k}; k \in \mathbf{Z}\}$ uit n elementen bestaat en een groep van transformaties is van \mathbf{R}^2 .

Voorbeeld 2.2. Zij $n \in \mathbf{Z}$ positief. Voor $k \in \mathbf{Z}$ definiëren we $t_{n,k} \in \text{O}(2)$ door

$$t_{n,k} = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ -\sin\left(\frac{2\pi k}{n}\right) & -\cos\left(\frac{2\pi k}{n}\right) \end{pmatrix}, \quad \text{met name} \quad t_{n,0} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Dan is $t_{n,k}$ te interpreteren als de spiegeling om de lijn voortgebracht door

$$\begin{pmatrix} \cos\left(\frac{\pi k}{n}\right) \\ -\sin\left(\frac{\pi k}{n}\right) \end{pmatrix}$$

Je rekt gemakkelijk na dat geldt:

$$t_{n,k} r_{n,m} = t_{n,k+m}$$

$$r_{n,k} t_{n,m} = t_{n,m-k}$$

$$t_{n,k} t_{n,m} = r_{n,m-k}$$

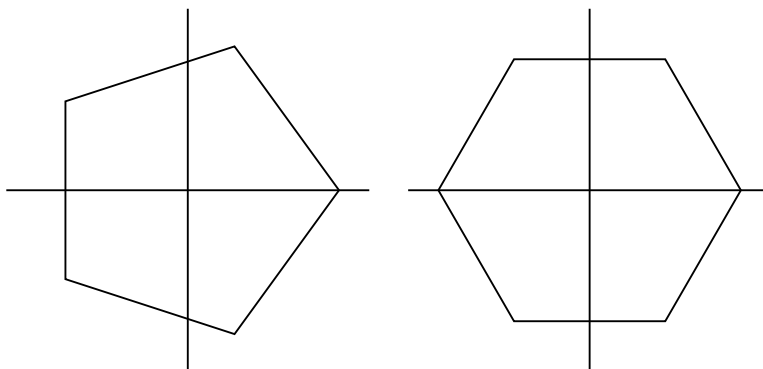
Verder is $t_{n,k} = t_{n,m}$ precies als $m - k$ een veelvoud is van n . Uit deze feiten volgt dat de *diëdergroep* $D_n = C_n \cup \{t_{n,k}; k \in \mathbf{Z}\}$ uit $2n$ elementen bestaat en een groep van transformaties is van \mathbf{R}^2 .

Opmerking 2.3. Uit de formules in Voorbeeld 2.1 blijkt dat alle elementen van C_n uit $r_{n,1}$ zijn te krijgen door herhaald samenstellen. Het is daarom nuttig deze matrix in het vervolg kortweg r_n te noemen. Evenzo zijn alle elementen van D te verkrijgen door bovendien $t_{n,0}$ te gebruiken. Het is daarom nuttig deze matrix in het vervolg kortweg t te noemen.

Zij $X_n \subset \mathbf{R}^2$ de verzameling van de punten

$$p_{n,j} = \begin{pmatrix} \cos \frac{2j\pi}{n} \\ \sin \frac{2j\pi}{n} \end{pmatrix} \in \mathbf{R}^2$$

voor $j = 1, 2, \dots, n$. Deze vormen de hoekpunten van een regelmatige n -hoek in \mathbf{R}^2 . Voor $n = 5$ en $n = 6$ is dit geschetst in Figuur 3.



Figuur 3: De regelmatige 5-hoek en 6-hoek

Propositie 2.4. *De transformatiegroep C_n bestaat precies uit de rotatiesymmetrieën van X_n .*

$$C_n = \{a \in \text{SO}(2) ; a(x) \in X_n \text{ voor alle } x \in X_n\}$$

De transformatiegroep D_n bestaat precies uit alle symmetrieën van X_n .

$$D_n = \{a \in \text{O}(2) ; a(x) \in X_n \text{ voor alle } x \in X_n\}$$

Bewijs. Als $a \in \text{SO}(2)$ en $a(X_n) = X_n$ dan is zeker $a(e_1) = a(p_{n,n}) \in X_n$, en dus is er een j zodat $a(e_1) = p_{n,j} = r_{n,j}(e_1)$. Volgens Lemma 12.15 ligt een $a \in \text{SO}(2)$ vast door zijn waarde op e_1 , dus $a = r_{n,j}$ voor diezelfde j . Als $b \in D_n$ en $b \notin C_n$ dan is $tb \in C_n$, zeg $tb = r_{n,j}$. Dan is $b = t^2b = tr_{n,j}$ voor diezelfde j . •

Opmerking 2.5. Van belang zijn de inclusie-relaties tussen deze transformatiegroepen:

- Voor elke n is $C_n \subset D_n$.
- Voor elke n en j is $C_n \subset C_{jn}$.
- Voor elke j en n is $D_n \subset D_{jn}$.

De eerste inclusie volgt direct uit de definitie van D_n ; de tweede en derde volgen uit de constatering dat $r_{jn,jk} = r_{n,k}$ en $t_{jn,nk} = t_{n,k}$.

We gaan nu de eindige groepen van orthogonale transformaties van \mathbf{R}^3 bestuderen. We zullen daarbij de symbolische namen geven zoals die gebruikt worden in o.a. de molecuulfysica, de zogenaamde Schoenfliess-notatie. We zullen daarbij in dit diktaat echter tekens uit het caligrafische font gebruiken, met name de symbolen $\mathcal{C}, \mathcal{D}, \mathcal{T}, \mathcal{O}, \mathcal{I}$. Dit om verwarring te voorkomen, omdat de symbolen C, D, T, O, I traditionele namen zijn voor zekere andere voorbeelden die ook in deze cursus voorkomen. Het moge duidelijk zijn dat U buiten deze cursus zelf uit omringende tekst zult moeten opmaken in welke betekenis een bepaald symbool gebruikt wordt.

Voorbeeld 2.6. Zij $n \in \mathbf{N}^{>0}$. Voor $k \in \mathbf{Z}$ definiëren we $r_{n,k} \in \text{SO}(3)$ door

$$r_{n,k} = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) & 0 \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Dit is te interpreteren als een draaiing om de derde coördinaat-as: met de eerste twee coördinaten gebeurt hetzelfde als in Voorbeeld 2.1, en met de derde coördinaat gebeurt niets.

Het is duidelijk dat tussen transformaties $r_{n,k}$ en $t_{n,k}$ van \mathbf{R}^3 dezelfde relaties gelden als tussen de transformaties van \mathbf{R}^2 met overeenkomstige namen. We krijgen dus een groep van transformaties. Ook deze noemt men de cyclische groep, en hij heeft Schoenfliess symbool \mathcal{C}_n .

Voorbeeld 2.7. Zij $n \in \mathbf{N}^{>0}$. Voor $k \in \mathbf{Z}$ definiëren we $t_{n,k} \in \text{SO}(3)$ door

$$t_{n,k} = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) & 0 \\ -\sin\left(\frac{2\pi k}{n}\right) & -\cos\left(\frac{2\pi k}{n}\right) & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Dit is te interpreteren als een rotatie over een hoek π om de lijn voortgebracht door

$$\begin{pmatrix} \cos\left(\frac{\pi k}{n}\right) \\ -\sin\left(\frac{\pi k}{n}\right) \\ 0 \end{pmatrix}$$

Het is duidelijk dat tussen deze transformaties van \mathbf{R}^3 dezelfde relaties gelden als tussen de transformaties van \mathbf{R}^2 met overeenkomstige namen. We krijgen dus een groep van transformaties. Ook deze noemt men de diëdergroep, en hij heeft Schoenfliess symbool \mathcal{D}_n .

Behalve deze twee oneindige series van voorbeelden zijn er nog drie losse voorbeelden, die gerelateerd zijn aan regelmatige veelvlakken in \mathbf{R}^3 . We bespreken elk van deze groepen van transformaties uitgaande van een beschrijving van het betreffende veelvlak.

Voorbeeld 2.8. Bekijk de verzameling X_{tet} bestaande uit de volgende 4 punten in \mathbf{R}^3 :

$$\begin{aligned} A &= (+1, +1, +1), \\ B &= (+1, -1, -1), \\ C &= (-1, +1, -1), \\ D &= (-1, -1, +1) \end{aligned}$$

De afstand tussen twee van deze punten is steeds $2\sqrt{2}$. Elke drie van deze punten vormen de hoekpunten van een gelijkzijdige driehoek. Omdat er 4 van zulke drietallen zijn vormen die driehoeken samen een regelmatig viervlak of tetraëder.

We kunnen narekenen welke elementen van $SO(3)$ de verzameling X_{tet} in zichzelf overvoeren en komen dan uit op de volgende lijst.

$$\begin{aligned} &\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ &\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix} \end{aligned}$$

We kunnen dat samenvatten als de matrices van de vorm

$$\begin{pmatrix} \kappa & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \kappa\lambda \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & \kappa \\ \lambda & 0 & 0 \\ 0 & \kappa\lambda & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \kappa & 0 \\ 0 & 0 & \lambda \\ \kappa\lambda & 0 & 0 \end{pmatrix}$$

met $\kappa \lambda \in \{+1, -1\}$.

De zojuist beschreven groep van rotatie-symmetrieën van het tetraëder noemt men de tetraëdergroep en heeft Schoenflies-notatie \mathcal{T} .

Voorbeeld 2.9. Bekijk de deelverzameling X_{oct} van \mathbf{R}^3 bestaande uit de drie vectoren uit de standaardbasis en hun tegengestelden. Als je drie elementen van X_{oct} bekijkt die op drie verschillende coördinaat-assen liggen dan vormen die drie punten de hoekpunten van een gelijkzijdige driehoek.

Omdat er 8 van zulke drietallen zijn vormen die driehoeken samen een regelmatig achthoek of octaëder. We kunnen narekenen welke elementen van $SO(3)$ de verzameling X_{oct} ten in zichzelf overvoeren en komen dan uit op

de volgende lijst.

$$\begin{array}{cccc}
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, & \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\
\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix} \\
\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, & \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \\
\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\
\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, & \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}
\end{array}$$

We kunnen dat samenvatten als de matrices van de vorm

$$\begin{array}{ccc}
\begin{pmatrix} \kappa & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \kappa\lambda \end{pmatrix}, & \begin{pmatrix} 0 & 0 & \kappa \\ \lambda & 0 & 0 \\ 0 & \kappa\lambda & 0 \end{pmatrix}, & \begin{pmatrix} 0 & \kappa & 0 \\ 0 & 0 & \lambda \\ \kappa\lambda & 0 & 0 \end{pmatrix} \\
\begin{pmatrix} \kappa & 0 & 0 \\ 0 & 0 & \lambda \\ 0 & -\kappa\lambda & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & \kappa \\ 0 & \lambda & 0 \\ -\kappa\lambda & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & \kappa & 0 \\ \lambda & 0 & 0 \\ 0 & 0 & -\kappa\lambda \end{pmatrix}
\end{array}$$

met $\kappa\lambda \in \{+1, -1\}$.

De zojuist beschreven groep van rotatie-symmetriën van het octaëder noemt men de octaëdergroep en heeft Schoenfliess-notatie \mathcal{O} . Door vergelijken met de lijst in Voorbeeld 2.8 blijkt dat $\mathcal{T} \subset \mathcal{O}$.

Opmerking 2.10. Een orthogonale transformatie die X_{oct} in zichzelf overvoert zal ook de verzameling gevormd door de middelpunten van diens 8 zijvlakken in zichzelf overvoeren. Dat blijft zo wanneer we die 8 punten allen met een factor 3 vermenigvuldigen. We krijgen dan precies de verzameling X_{hex} bestaande uit de 8 vectoren waarvan alle drie coördinaten absolute waarde 1 hebben. Deze 8 punten vormen de hoekpunten van een regelmatig zesvlak, ook wel hexaëder of kubus genoemd.

Omgekeerd zal elke orthogonale transformatie die X_{hex} in zichzelf overvoert ook de verzameling van middelpunten van 6 (vierkante) zijvlakken

van de kubus in zichzelf overvoeren. Dat is precies de verzameling X_{oct} bestaande uit de 6 hoekpunten van het octaëder.

We zien dus dat de rotatie-symmetriegroep van het octaëder en van het hexaëder hetzelfde zijn. Het feit dat $\mathcal{T} \subset \mathcal{O}$ wordt verklaard door de omstandigheid dat X_{hex} precies bestaat uit de vier punten A, B, C, D van X_{tet} en hun tegengestelden.

Voorbeeld 2.11. Zij $\tau = \frac{1+\sqrt{5}}{2} = 1.618\dots$ de gulden snede. Dat is de positieve oplossing van de vergelijking $x^2 = x + 1$. De negatieve oplossing $-\tau^{-1} = 1 - \tau = \frac{1-\sqrt{5}}{2} = -0.618\dots$ noemen we voortaan τ^* . Bekijk de deelverzameling X_{ico} van \mathbf{R}^3 bestaande uit de 4 punten $(\pm 1 \pm \tau, 0)$, de 4 punten $(0, \pm 1, \pm \tau)$ en de 4 punten $(\pm \tau, 0, \pm 1)$.

Voor elk $p \in X_{ico}$ zijn er precies 5 punten $q \in X_{ico}$ die afstand 2 hebben tot p , namelijk de 5 punten die liggen in het vlak $\{q \in \mathbf{R}^3; \langle q, p \rangle = \tau\}$. Deze 5 punten vormen een regelmatige vijfhoek in dat vlak, waarvan de afstand tussen opeenvolgende hoekpunten ook steeds 2 is. In p komen dus 5 gelijkzijdige driehoeken samen. Als we p alle elementen van X_{ico} laten doorlopen komen we elke driehoek 3 keer tegen, zodat er in totaal $\frac{12 \cdot 5}{3} = 20$ dergelijke driehoeken zijn. Samen vormen deze een regelmatig 20-vlak of *icosaëder*. We beschrijven nu een aantal rotatie-symmetrieën van deze figuur:

- Voor elke $p \in X_{ico}$ is er een rotatie $T_{5,p}$ over een hoek $\frac{2\pi}{5}$ om de lijn door p . De k -de macht daarvan is een rotatie over $\frac{2\pi k}{5}$. Deze transformaties verwisselen de vijf punten van de boven beschreven vijfhoek op een cyclische manier. Als we p de verzameling X_{ico} en k de verzameling $\{1, 2, 3, 4\}$ laten doorlopen krijgen we $12 \cdot 4 = 48$ combinaties. Aangezien $T_{5,-p}$ steeds de inverse (ofwel vierde macht) van $T_{5,p}$ is, vinden we in totaal $48/2 = 24$ verschillende matrices. We vinden zo de matrices

$$\frac{1}{2} \begin{pmatrix} 1 & -\kappa\tau^* & \lambda\tau \\ -\kappa\mu\tau^* & \mu\tau & -\kappa\lambda\mu \\ -\lambda\mu\tau & \kappa\lambda\mu & -\mu\tau^* \end{pmatrix}, \quad \frac{1}{2} \begin{pmatrix} -\mu\tau^* & -\lambda\mu\tau & \kappa\lambda\mu \\ \lambda\tau & 1 & -\kappa\tau^* \\ -\kappa\lambda\mu & -\kappa\mu\tau^* & \mu\tau \end{pmatrix},$$

$$\text{en } \frac{1}{2} \begin{pmatrix} \mu\tau & -\kappa\lambda\mu & -\kappa\mu\tau^* \\ \kappa\lambda\mu & -\mu\tau^* & -\lambda\mu\tau \\ -\kappa\tau^* & \lambda\tau & 1 \end{pmatrix},$$

steeds met $\kappa, \lambda, \mu \in \{+1, -1\}$. Inderdaad een totaal 24 matrices.

- Als p het midden is van een van de 20 zijvlakken, dan is er een rotatie $T_{3,p}$ over een hoek $\frac{2\pi}{3}$ om de lijn door p . De k -de macht daarvan is een rotatie over $\frac{2\pi k}{3}$. Deze transformaties verwisselen de drie punten van de gelijkzijdige driehoek op een cyclische manier. Als we p de verzameling middens van driehoeken en k de verzameling $\{1, 2\}$ laten

doorlopen vinden we zo $\frac{20 \cdot 2}{2} = 20$ matrices, aangezien $T_{3,-p}$ steeds de inverse (ofwel tweede macht) is van $T_{3,p}$. We vinden zo de matrices

$$\begin{aligned} & \frac{1}{2} \begin{pmatrix} -1 & -\kappa\tau^* & \lambda\tau \\ \kappa\tau^* & \tau & -\kappa\lambda \\ -\lambda\tau & -\kappa\lambda & \tau^* \end{pmatrix}, \quad \frac{1}{2} \begin{pmatrix} \tau^* & -\lambda\tau & -\kappa\lambda \\ \lambda\tau & -1 & -\kappa\tau^* \\ -\kappa\lambda & \kappa\tau^* & \tau \end{pmatrix} \\ & \frac{1}{2} \begin{pmatrix} \tau & -\kappa\lambda & \kappa\tau^* \\ -\kappa\lambda & \tau^* & -\lambda\tau \\ -\kappa\tau^* & \lambda\tau & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & \kappa \\ \lambda & 0 & 0 \\ 0 & \kappa\lambda & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \kappa & 0 \\ 0 & 0 & \lambda \\ \kappa\lambda & 0 & 0 \end{pmatrix} \end{aligned}$$

steeds met $\kappa, \lambda \in \{+1, -1\}$. Inderdaad een totaal van 20 matrices.

- Als p het midden is van een van de 30 ribben, dan is er er een rotatie $T_{2,p}$ om een hoek π om de lijn door p , dus een spiegeling ten opzichte van deze lijn. Deze transformatie verwisselt de beide eindpunten van deze ribbe, en eveneens de beide zijvlakken die aan deze ribbe grenzen (en dus ook hun toppen). Als we p de verzameling middens van ribben laten doorlopen vinden we zo $\frac{30}{2} = 15$ matrices, aangezien $T_{2,-p}$ steeds gelijk is aan $T_{2,p}$. We vinden zo de matrices

$$\begin{aligned} & \frac{1}{2} \begin{pmatrix} -1 & -\kappa\tau^* & \lambda\tau \\ -\kappa\tau^* & -\tau & \kappa\lambda \\ \lambda\tau & \kappa\lambda & -\tau^* \end{pmatrix}, \quad \frac{1}{2} \begin{pmatrix} -\tau^* & \lambda\tau & \kappa\lambda \\ \lambda\tau & -1 & -\kappa\tau^* \\ \kappa\lambda & -\kappa\tau^* & -\tau \end{pmatrix}, \\ & \frac{1}{2} \begin{pmatrix} -\tau & \kappa\lambda & -\kappa\tau^* \\ \kappa\lambda & -\tau^* & \lambda\tau \\ -\kappa\tau^* & \lambda\tau & -1 \end{pmatrix}, \quad \begin{pmatrix} \kappa & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \kappa\lambda \end{pmatrix} \end{aligned}$$

steeds met $\kappa, \lambda \in \{+1, -1\}$, maar in het laatste geval met κ en λ niet allebei $+1$. Inderdaad een totaal van 15 matrices.

Tesamen met de identieke afbeelding geeft dit $24 + 20 + 15 + 1 = 60$ rotatiesymmetrieën van het isosaëder. De zojuist beschreven groep van rotaties noemt men de icoesaëdergroep en heeft Schoenfliess-notatie \mathcal{I} . Door vergelijken met de lijst in Voorbeeld 2.8 blijkt dat $\mathcal{T} \subset \mathcal{I}$.

Opmerking 2.12. Een orthogonale transformatie die X_{ico} in zichzelf overvoert zal ook de verzameling gevormd door de middelpunten van diens 20 zijvlakken in zichzelf overvoeren. Deze punten vormen de hoekpunten van een regelmatig 12-vlak of dodecaëder. Op dezelfde wijze levert elke rotatiesymmetrie van het dodecaëder er een van het icoesaëder. We zien dus dat de rotatie-symmetriegroep van het icoesaëder en van het dodecaëder hetzelfde zijn.

We gaan nu beginnen met een opsomming van de groepen van orthogonale transformaties van \mathbf{R}^3 die niet alleen uit rotaties bestaan. We gebruiken twee constructies om deze groepen te fabriceren. Beide constructies

maken gebruik van de *pariteits*-operator $P: \mathbf{R}^3 \rightarrow \mathbf{R}^3$ gedefinieerd door $P(x) = -x$. Deze afbeelding wordt ook wel *centrale inversie* genoemd, en heeft als matrix

$$P = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Hij is duidelijk wel orthogonaal, maar van determinant -1 .

Voorbeeld 2.13. Voor de eerste constructie moet gegeven zijn een groep van rotaties A , en we maken daaruit een nieuwe groep $G(A)$ van orthogonale transformaties door de samenstellingen met P toe te voegen:

$$G(A) = A \cup \{P \circ T; T \in A\}$$

Merk op dat $P \in G(A)$. We gebruiken deze constructie in de volgende gevallen:

- Het geval $A = \mathcal{C}_n$. Het resultaat heeft Schoenfliess naam \mathcal{C}_{nh} als n even is, en Schoenfliess naam \mathcal{S}_{2n} als n oneven is.
- Het geval $A = \mathcal{D}_n$. Het resultaat heeft Schoenfliess naam \mathcal{D}_{nh} als n even is, en Schoenfliess naam \mathcal{D}_{nd} als n oneven is.
- Het geval $A = \mathcal{T}$. Dat levert een groep van 24 orthogonale transformaties. Het resultaat heeft Schoenfliess naam \mathcal{T}_h .
- Het geval $A = \mathcal{O}$. Het resultaat heeft Schoenfliess naam \mathcal{O}_h .
- Het geval $A = \mathcal{I}$. Het resultaat heeft Schoenfliess naam \mathcal{I}_h .

Voorbeeld 2.14. Voor de tweede constructie moet gegeven zijn een groep van rotaties A , en een deelverzameling $B \subset A$ die ook een groep van rotaties is, maar een die half zoveel elementen heeft als A .

We maken een nieuwe groep van transformaties $G(A, B)$ door de elementen van A die *niet* in B zitten samen te stellen met P :

$$G(A, B) = B \cup \{P \circ T; T \in A, T \notin B\} \quad (1)$$

Merk op dat $P \notin G(A, B)$. We gebruiken deze constructie in de volgende gevallen:

- Het geval $A = \mathcal{C}_{2n}$ en $B = \mathcal{C}_n$. Het resultaat heeft Schoenfliess naam \mathcal{S}_{2n} als n even is, en Schoenfliess naam \mathcal{C}_{nh} als n oneven. Voor \mathcal{S}_2 schrijft men echter \mathcal{C}_i en voor \mathcal{C}_{1h} schrijft men \mathcal{C}_s .
- Het geval $A = \mathcal{D}_{2n}$ en $B = \mathcal{D}_n$. Het resultaat heeft Schoenfliess naam \mathcal{D}_{nd} als n even is, en Schoenfliess naam \mathcal{D}_{nh} als n oneven is.

- Het geval $A = \mathcal{D}_n$ en $B = \mathcal{C}_n$. Het resultaat heeft Schoenfliess naam \mathcal{C}_{nv} , voor alle n
- Het geval $A = \mathcal{O}$ en $B = \mathcal{T}$. Het resultaat heeft Schoenfliess naam \mathcal{T}_d .

Het is trouwens op dit moment niet duidelijk dat deze algemene constructie altijd een groep van transformaties oplevert, hoewel het in bovenstaande concrete gevallen gemakkelijk expliciet is te controleren. We komen op deze kwestie in een later Hoofdstuk nog terug.

Opmerking 2.15. De wijze van naamgeving ziet er op het eerste gezicht een beetje merkwaardig uit. De systematiek zit erin dat er gekeken wordt of de groep spiegelingen bevat ten opzichte van een vlak, en zo ja wat de stand is van dat vlak.

- De groepen \mathcal{S}_{2n} bevatten geen spiegelingen ten opzichte van een vlak.
- De groepen \mathcal{C}_{nh} , \mathcal{D}_{nh} , \mathcal{T}_h , \mathcal{O}_h en \mathcal{I}_h bevatten een spiegeling ten opzichte van het ‘horizontale’ vlak, met matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

- De groepen \mathcal{C}_{nv} bevatten geen spiegeling ten opzichte van het horizontale vlak, maar wel een spiegeling ten opzichte van het ‘verticale’ vlak, met matrix

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- De groepen \mathcal{D}_{nd} bevatten geen spiegeling ten opzichte van het horizontale vlak, of het verticale vlak, maar wel een spiegeling ten opzichte van een ‘diagonaal’ vlak,

We kunnen nu het volgende overzicht maken van groepen van orthogonale transformaties van \mathbf{R}^3 .

Naam	Alleen rotaties	Aantal elementen	Naam	Alleen rotaties	Aantal elementen
\mathcal{C}_n	Ja	n	\mathcal{T}	Ja	12
\mathcal{D}_n	Ja	$2n$	\mathcal{O}	Ja	24
\mathcal{C}_{nh}	Nee	$2n$	\mathcal{I}	Ja	60
\mathcal{S}_{2n}	Nee	$2n$	\mathcal{T}_h	Nee	24
\mathcal{C}_{nv}	Nee	$2n$	\mathcal{O}_h	Nee	48
\mathcal{D}_{nh}	Nee	$4n$	\mathcal{T}_d	Nee	24
\mathcal{D}_{nd}	Nee	$4n$	\mathcal{I}_h	Nee	120

We zullen later bewijzen dat dit op een basis-transformaties na de enige mogelijkheden zijn.

Bij het bestuderen van de symmetrieën van kristallen hebben we niet alleen te maken met rotaties en spiegelingen. In het geïdealiseerde geval waarin we ons het kristal oneindig uitgebreid denken is de groep van symmetrieën een groep van bewegingen (zie Voorbeeld 1.9) die translaties bevat over drie onafhankelijke vectoren. We zullen later bewijzen dat dit tot gevolg heeft dat er geen rotatie-symmetrieën mogelijk zijn over andere hoeken dan $\frac{2k\pi}{n}$ met $n = 1, 2, 3, 4$ of 6 .

Dat maakt dat er van bovenstaande lijst precies 32 exemplaren overblijven. In de kristallografie gebruikt men een eigen notatie, de zogenaamde Hermann-Mauguin notatie. We geven nu een overzicht van de 32 mogelijkheden, met hun H-M symbool:

S symbool	H-M symbool	S symbool	H-M symbool
C_1	1	C_{2v}	$mm2$
C_2	2	C_{3v}	$3m$
C_3	3	C_{4v}	$4mm$
C_4	4	C_{6v}	$6mm$
C_6	6	D_{2h}	mmm
D_2	222	D_{3h}	$\bar{6}2m$
D_3	32	D_{4h}	$4/mmm$
D_4	422	D_{6h}	$6/mmm$
D_6	62	D_{2d}	$\bar{4}2m$
$C_{1h} = C_s$	m	D_{3d}	$\bar{3}m$
C_{2h}	$2/m$	\mathcal{T}	23
C_{3h}	$3/m$	\mathcal{T}_d	$\bar{4}3m$
C_{4h}	$4/m$	\mathcal{T}_h	$m\bar{3}$
C_{6h}	$6/m$	\mathcal{O}	432
$S_2 = C_i$	$\bar{1}$	\mathcal{O}_h	$m\bar{3}m$
S_4	$\bar{4}$		
S_6	$\bar{3}$		

Opmerking 2.16. Uit de in dit Hoofdstuk beschreven voorbeelden in lage dimensie kunnen we vele voorbeelden maken in hogere dimensie door gebruik te maken van constructie 1.11. Zo kun je $C_k \times C_m$ (voor willekeurige k en m) opvatten als een groep van transformaties van $\mathbf{R}^2 \times \mathbf{R}^2 = \mathbf{R}^4$, en $\mathcal{T} \times \mathcal{O}$ als een groep van transformaties van \mathbf{R}^6 .

3 Groepen en ondergroepen

Als we ons afvragen of in twee geheel verschillende situaties misschien dezelfde symmetrie voorhanden is dan moeten we dan moeten we een gedeelte van de gegevens (te weten de verzameling X) voorlopig ‘vergeten’ en ons concentreren op de manier hoe twee symmetrieën (afbeeldingen uit G) tot een nieuwe gecombineerd worden. Dit motiveert de volgende definitie. We schrijven de eisen eerst nogal formeel op en komen later terug op de betekenis.

Definitie 3.1. Een (abstracte) *groep* is een verzameling G tezamen met een afbeelding $M: G \times G \rightarrow G$ die aan de volgende eigenschappen voldoet:

- (G1) $M(M(a, b), c) = M(a, M(b, c))$ voor alle $a, b, c \in G$. Men noemt $M(a, b)$ wel het *product* van a en b in de groep G .
- (G2) Er is een $e \in G$ met $M(e, a) = a$ en $M(a, e) = a$ voor alle $a \in G$. Een dergelijk element heet *eenheids-element* of *neutraal element*. We zullen straks controleren dat er maar één dergelijk element e kan zijn. Daarom is de volgende eis ook zinvol:
- (G3) Voor elke $a \in G$ is er een element $a' \in G$ met $M(a, a') = e$ en $M(a', a) = e$. Een dergelijk element heet een *inverse* van a .

Opmerking 3.2. Als G eindig is wordt deze situatie geheel beschreven door een vierkante tabel die de waarden van M geeft, de zogenaamde *groeps-tabel*. De volgende tabellen geven twee wezenlijk verschillende mogelijkheden voor de afbeelding M als G een verzameling van vier elementen $\{e, f, g, h\}$ is.

	e	f	g	h			e	f	g	h
e	e	f	g	h	of	e	e	f	g	h
f	f	g	h	e		f	f	e	h	g
g	g	h	e	f		g	g	h	e	f
h	h	e	f	g		h	h	g	f	e

Hierbij hebben we de volgende conventie aangehouden

	b
a	$M(a, b)$

Opmerking 3.3. Voor de afbeelding die we hierboven M noemden wordt bijna altijd een infix notatie gebruikt, bijvoorbeeld $a * b$ of $a \cdot b$ of $a \times b$. Heel vaak wordt het symbool voor deze binaire operatie zelfs helemaal weggelaten, zodat $M(a, b)$ wordt genoteerd als ab .

Verder is men gewoonlijk wat slordig en spreekt men over ‘de groep G ’ in plaats van ‘de verzameling G met de vermenigvuldiging M ’. Dit gebeurt met name als duidelijk is met welke vermenigvuldigings-afbeelding de genoemde verzameling wordt uitgerust.

Nu de beloofde uniciteit.

Propositie 3.4. *Elke groep G bevat slechts één eenheids-element.*

Bewijs. Stel dat e_1 en e_2 allebei eenheids-element zijn. Dan hebben we enerzijds

$$M(e_1, a) = a \text{ en } M(a, e_1) = a \text{ voor alle } a \in G$$

en anderzijds

$$M(e_2, b) = b \text{ en } M(b, e_2) = b \text{ voor alle } b \in G$$

Vullen we $a = e_2$ en $b = e_1$ in dan vinden we $e_2 = M(e_1, e_2) = e_1$ •

We kunnen dus voortaan spreken over *het* eenheids-element van een groep G , en we noteren dat element vaak als 1. Analoog hebben we:

Propositie 3.5. *Elk element a van een groep G heeft slechts één inverse.*

Bewijs. Stel dat b_1 en b_2 allebei inverse van a zijn. Dan hebben we enerzijds

$$M(a, b_1) = e \text{ en } M(b_1, a) = e$$

en anderzijds

$$M(a, b_2) = e \text{ en } M(b_2, a) = e$$

Uit bovenstaande formules en eisen (G1) en (G2) vinden we $b_2 = M(e, b_2) = M(M(b_1, a), b_2) = M(b_1, M(a, b_2)) = M(b_1, e) = b_1$ •

We kunnen dus voortaan spreken over *de* inverse van een element a van de groep G , en we noteren dat element gewoonlijk als a^{-1} .

De conditie (G1) heet de *associatieve* eigenschap. Deze eigenschap impliceert dat in een herhaald product de uitkomst niet afhangt van de plaatsing van de haakjes. We lichten dit nu toe. Laten we $p_m(a_1, \dots, a_m)$ schrijven voor het standaard product van de elementen a_1, \dots, a_m waar we telkens de meest linkse factoren het eerst uitvermenigvuldigen. Formeel:

$$\begin{cases} p_1(a_1) = a_1 \\ p_m(a_1, \dots, a_m) = p_{m-1}(a_1, \dots, a_{m-1})a_m \quad \text{voor } m > 1 \end{cases}$$

Propositie 3.6. *Zij $b \in G$ een willekeurig product van $a_1, \dots, a_n \in G$, met de factoren in deze volgorde maar met haakjes op willekeurige wijze geplaatst. Dan is b gelijk aan het standaard product $p_n(a_1, \dots, a_n)$*

Bewijs. In drie stappen.

- We bewijzen eerst met inductie naar m dat

$$a_1 p_{m-1}(a_2, \dots, a_m) = p_m(a_1, \dots, a_m)$$

Voor $m = 2$ staat aan beide kanten $a_1 a_2$, en voor $m \geq 3$ geldt:

$$\begin{aligned} a_1 p_{m-1}(a_2, \dots, a_m) &= a_1 (p_{m-2}(a_2, \dots, a_{m-1}) a_m) = \\ &= (a_1 p_{m-2}(a_2, \dots, a_{m-1})) a_m = p_{m-1}(a_1, \dots, a_{m-1}) a_m = \\ &= p_m(a_1, \dots, a_m) \end{aligned}$$

- Vervolgens bewijzen we met inductie naar j dat

$$p_j(a_1, \dots, a_j) p_k(a_{j+1}, \dots, a_{j+k}) = p_{j+k}(a_1, \dots, a_{j+k})$$

Het geval $j = 1$ is zojuist bewezen, en voor $j \geq 2$ geldt:

$$\begin{aligned} p_j(a_1, \dots, a_j) p_k(a_{j+1}, \dots, a_{j+k}) &= \\ &= (a_1 p_{j-1}(a_2, \dots, a_j)) p_k(a_{j+1}, \dots, a_{j+k}) = \\ &= a_1 (p_{j-1}(a_2, \dots, a_j) p_k(a_{j+1}, \dots, a_{j+k})) = \\ &= a_1 p_{j-1+k}(a_2, \dots, a_{j+k}) = p_{j+k}(a_1, \dots, a_{j+k}) \end{aligned}$$

- Nu het algemene geval. Bij de vermenigvuldiging die het laatst wordt uitgevoerd vermenigvuldigt men (voor zekere j):
 - Het product van a_1, \dots, a_j met een of andere positie van de haakjes. Bij inductie-hypothese is dat product gelijk aan het standaard product $p_j(a_1, \dots, a_j)$.
 - Het product van a_{j+1}, \dots, a_n met een of andere positie van de haakjes. Bij inductie-hypothese is dat product gelijk aan het standaard product $p_{n-j}(a_{j+1}, \dots, a_n)$

De vorige stap (met $k = n - j$) zegt precies dat hun product gelijk is aan $p_n(a_1, \dots, a_n)$.

•

Definitie 3.7. Zij a een element van een groep G en zij $n \in \mathbf{Z}$. Dan bedoelen we met a^n het volgende element van G :

- Als $n > 0$ dan is $a^n = p_n(a, a, a, \dots, a)$. Met andere woorden a^n is recursief gedefinieerd door $a^1 = a$ en $a^n = a^{n-1} a$ voor $n > 1$. Het is het product van n factoren die allen a zijn.
- Als $n = 0$ dan is $a^n = e$
- Als $n < 0$ dan is $a^n = (a^{-1})^{-n}$.

De motivatie voor de axiomas G1-G3 wordt gevormd door de volgende opmerking

Opmerking 3.8. Zij X een verzameling die niet leeg is, en zij G een groep van transformaties van X . Dan kunnen we G de structuur van (abstracte) groep geven als volgt:

- De binaire operatie is het samenstellen van afbeeldingen:

$$M(\sigma, \tau) = \sigma \circ \tau \quad (2)$$

- Het eenheidselement is de identieke afbeelding $e: X \rightarrow X$, $e(x) = x$ voor alle $x \in X$.
- De inverse van $\sigma \in G$ is de inverse afbeelding van de bijectie σ .

Elk voorbeeld van een groep van transformaties levert dus een voorbeeld van een abstracte groep. Sommigen daarvan kunnen we ook op een andere manier handig beschrijven:

- (Zie Voorbeelden 1.3 en 1.4) Zij $\mathbf{F} = \mathbf{Q}, \mathbf{R}$ of \mathbf{C} en zij X een eindig-dimensionale vectorruimte over \mathbf{F} . In dat geval levert X een groep $\text{GL}(X)$.

Als $X = \mathbf{F}^n$ dan kunnen we aan elke lineaire afbeelding $A: \mathbf{F}^n \rightarrow \mathbf{F}^n$ toevoegen zijn matrix ten opzichte van de standaard-basis van \mathbf{F}^n . Omgekeerd is elke matrix afkomstig van precies één dergelijke lineaire afbeelding. Door deze correspondentie kunnen we elementen van $\text{GL}(X)$ opvatten als $n \times n$ inverteerbare matrices met determinant ongelijk 0. De binaire operatie M correspondeert nu met matrix-vermenigvuldiging, en het eenheids-element e met de $n \times n$ eenheids-matrix I_n .

Dezelfde situatie geeft ook een groep $\text{SL}(X)$ op, die we voor $X = \mathbf{F}^n$ wederom als groep van matrices kunnen opvatten, nu steeds met determinant 1.

- Zij nu X een eindig-dimensionale vector-ruimte over \mathbf{R} en zij B een scalaire product op V . Uit deze gegevens verkrijgen we een groep $\text{O}(X, B)$. Veronderstel nu dat $X = \mathbf{R}^n$ en B het Euclidische scalaire product. De elementen van $\text{O}(X, B)$ corresponderen nu met de matrices $\alpha \in \text{GL}(n, \mathbf{R})$ waarvoor geldt dat $\alpha^T \alpha = I_n$. Hier staat α^T voor de gespiegelde matrix van α , en I_n voor de $n \times n$ eenheids-matrix.

De volgende drie voorbeelden zijn oude situaties gezien vanuit een nieuw gezichtspunt.

Voorbeeld 3.9. Zij $\mathbf{F} = \mathbf{Z}, \mathbf{Q}, \mathbf{R}$ of \mathbf{C} . De *additieve groep* van \mathbf{F} is als verzameling gelijk aan \mathbf{F} met als groepsoperatie optellen. De vermenigvuldiging wordt dan vergeten.

Voorbeeld 3.10. Zij $\mathbf{F} = \mathbf{Q}, \mathbf{R}$ of \mathbf{C} . Een vectorruimte V over \mathbf{F} is een groep ten aanzien van optellen van vectoren. De scalaire vermenigvuldiging wordt dan vergeten.

Voorbeeld 3.11. Zij $\mathbf{F} = \mathbf{Q}, \mathbf{R}$ of \mathbf{C} . De *multiplicatieve groep* van \mathbf{F} is als verzameling gelijk aan $\mathbf{F}^* := \mathbf{F} \setminus \{0\}$ met als groepsoperatie vermenigvuldigen. De optelling wordt dan vergeten.

Voorbeeld 3.12. Zij G het interval $(-1, +1)$ in \mathbf{R} . We definiëren $M: G \times G \rightarrow G$ door

$$M(x, y) = \frac{x + y}{1 + xy}$$

Dit komt voor als de formule voor het combineren van relatieve snelheden in de Speciale Relativiteits Theorie, in eenheden waarin de lichtsnelheid 1 bedraagt.

De groepen uit de twee tabellen en uit de laatste vier voorbeelden hebben een mooie extra eigenschap:

Definitie 3.13. Een groep G heet *abels* of *commutatief* als bovendien geldt:

$$(G4) \quad M(a, b) = M(b, a) \text{ voor alle } a, b \in G.$$

Opmerking 3.14. In een abelse groep wordt noemt men $M(a, b)$ wel de *som* van a en b en gebruikt men daar voor de ‘additieve’ notatie $a + b$. In dat geval noemt men e ook wel *nul-element* van G , genoteerd als 0. Tenslotte noemt men a' dan de *tegengestelde* van a , genoteerd als $-a$.

Uit de berekening in Voorbeeld 1.2 blijkt dat S_3 niet abels is.

Zoals in de inleidende zin van dit hoofdstuk is gezegd concentreren we ons hier op de manier waarop bij twee elementen x en y van de verzameling G een nieuw element $M(x, y)$ hoort, en we vergeten een eventuele interpretatie van die elementen als afbeeldingen van X .

In het bijzonder speelt de naamgeving van de elementen geen rol. Dit inspireert tot de volgende definitie.

Definitie 3.15. Een *isomorfisme* van een abstracte groep (G_1, M_1) naar een abstracte groep (G_2, M_2) is een bijectie $\phi: G_1 \rightarrow G_2$ met de eigenschap dat $M_2(\phi(x), \phi(y)) = \phi(M_1(x, y))$ voor alle $x, y \in G_1$. Als een dergelijke ϕ bestaat heten de twee groepen isomorf, en we noteren $G_1 \cong G_2$.

Groepen die isomorf zijn beschouwen we als niet wezenlijk verschillend.

Voorbeeld 3.16. In de situatie van Opmerking 1.10 is er een isomorfisme ϕ van de abstracte groep G naar de abstracte groep H , gegeven door $\phi(f) = \beta \circ f \circ \beta^{-1}$.

In het bijzonder zij Y een verzameling van n elementen, en kies een aftelling van de elementen van Y , met andere woorden een bijectie van $\{1, 2, \dots, n\}$ naar Y . Dan krijgen we zo een isomorfisme tussen de abstracte groepen S_n en $\text{Sym}(Y)$. Een andere aftelling geeft gewoonlijk een ander isomorfisme.

Maar ook als je groepen van transformaties hebt van verzamelingen die niet even groot zijn dan kunnen de bijbehorende abstracte groepen isomorf zijn:

Voorbeeld 3.17. We kunnen een isomorfisme $\phi: C_n \rightarrow C_n$ definiëren door de formule

$$\phi \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ of kortweg } \phi(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$$

Voorbeeld 3.18. Net zo kunnen we een isomorfisme $\phi: D_n \rightarrow D_n$ definiëren door de formule

$$\phi(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \det(\alpha) \end{pmatrix}$$

Voorbeeld 3.19. Elke afbeelding $f: \mathbf{R}^3 \rightarrow \mathbf{R}^3$ die in \mathcal{O} zit levert door beperken een bijectieve afbeelding $X_{\text{oct}} \rightarrow X_{\text{oct}}$. Dus ‘beperken’ is op te vatten als een afbeelding $\phi: \mathcal{O} \rightarrow \text{Sym}(X_{\text{oct}})$. Deze afbeelding is injectief want een lineaire transformatie wordt bepaald door zijn waarden op de standaard basisvectoren van \mathbf{R}^3 , en dus zeker door zijn waarden op X_{oct} .

Het beeld G_{oct} van deze afbeelding is gesloten onder samenstellen en inverteren en is dus ook een groep van transformaties van X_{oct} . De afbeelding $\phi: \mathcal{O} \rightarrow G_{\text{oct}}$ is bijectief en respecteert samenstellingen. Het is dus een isomorfisme.

Op dezelfde wijze vinden we een isomorfisme tussen \mathcal{O} en een groep van transformaties van de (eindige!) verzameling X_{hex} .

Voorbeeld 3.20. Als $B \subset A \subset \text{SO}(3)$ voldoen aan de voorwaarden voor de constructie van $G(A, B)$, dan is er een isomorfisme $\phi: A \rightarrow G(A, B)$ dat gegeven wordt door

$$\phi(T) = \begin{cases} T & \text{als } T \in B \\ P \circ T & \text{als } T \notin B \end{cases}$$

In het bijzonder zijn er isomorfismen

$$\begin{aligned}\mathcal{S}_{2n} &\cong \mathcal{C}_{2n} \text{ en } \mathcal{D}_{nd} \cong \mathcal{D}_{2n} \text{ voor } n \text{ even} \\ \mathcal{C}_{nh} &\cong \mathcal{C}_{2n} \text{ en } \mathcal{D}_{nh} \cong \mathcal{D}_{2n} \text{ voor } n \text{ oneven} \\ \mathcal{C}_{nv} &\cong \mathcal{D}_n \text{ voor elke } n \\ \mathcal{T}_d &\cong \mathcal{O}\end{aligned}$$

Voorbeeld 3.21. Er is een isomorfisme ϕ van de additieve groep van \mathbf{R} naar de groep uit Voorbeeld 3.12. De afbeelding $\phi: \mathbf{R} \rightarrow (-1, +1)$ is de tangens hyperbolicus.

Je kunt je afvragen of we in de eisen G1-G3 niet iets vergeten zijn: je zou je kunnen voorstellen dat het begrip ‘abstracte groep’ zo ruim is dat het veel meer voorbeelden toelaat dan we bedoeld hadden, namelijk die welke ‘geleverd’ worden door opmerking 3.8. De volgende Stelling geeft aan dat we niets vergeten hebben.

Stelling 3.22. (Cayley) *Elke abstracte groep G is isomorf met een groep van transformaties van een zekere verzameling X .*

Bewijs. Als verzameling X nemen we G zelf. Gegeven een $a \in G$ beschouwen we de afbeelding $L_a: G \rightarrow G$ gegeven door $L_a(g) = M(a, g)$. Noteer G^* voor de verzameling $\{L_a; a \in G\}$ van al dergelijke afbeeldingen. We gaan nu na dat G^* voldoet aan de eisen voor een groep van transformaties van X :

- Het element L_e ligt in G^* , en het is de identieke afbeelding 1_X , immers $L_e(g) = M(e, g) = g = 1_X(g)$.
- Voor elke $a \in G$ is de afbeelding L_a inverteerbaar. Een inverse wordt namelijk gevormd door de afbeelding $L_{a^{-1}} \in G^*$, zoals blijkt uit de volgende berekening:

$$\begin{aligned}(L_{a^{-1}} \circ L_a)(x) &= L_{a^{-1}}(L_a(x)) = M(a^{-1}, M(a, x)) \\ &= M(M(a^{-1}, a), x) = M(e, x) = x \\ (L_a \circ L_{a^{-1}})(x) &= L_a(L_{a^{-1}}(x)) = M(a, M(a^{-1}, x)) \\ &= M(M(a, a^{-1}), x) = M(e, x) = x\end{aligned}$$

- Als $f = L_a \in G^*$ en $g = L_b \in G^*$ dan is $f \circ g = L_{M(a,b)} \in G^*$ zoals blijkt uit de volgende berekening:

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) = L_a(L_b(x)) = M(a, L_b(x)) \\ &= M(a, M(b, x)) = M(M(a, b), x) = L_{M(a,b)}(x)\end{aligned}$$

Vervolgens maken we een afbeelding $\phi: G \rightarrow G^*$ door $\phi(a) = L_a$. We gaan nu na dat ϕ voldoet aan de eisen voor een isomorfisme:

- De afbeelding ϕ is bijectief. Een inverse wordt namelijk gevormd door de afbeelding $\psi: G^* \rightarrow G$ gegeven door $\psi(f) = f(e)$. Dit blijkt uit de volgende berekening:

$$\begin{aligned}(\psi \circ \phi)(a) &= \psi(\phi(a)) = \psi(L_a) = L_a(e) = M(a, e) = a \\(\phi \circ \psi)(L_a) &= \phi(\psi(L_a)) = \phi(L_a(e)) = \phi(M(a, e)) = \phi(a) = L_a\end{aligned}$$

- Er is voldaan aan de eis $M_2(\phi(x), \phi(y)) = \phi(M_1(x, y))$ waar M_1 de gegeven vermenigvuldiging M in G is, en M_2 de operatie ‘samenstellen van afbeeldingen’ in G^* is. Dit blijkt uit de berekening

$$\begin{aligned}M_2(\phi(x), \phi(y))(z) &= M_2(L_x, L_y)(z) = (L_x \circ L_y)(z) = L_x(L_y(z)) \\&= M(x, L_y(z)) = M(x, M(y, z)) = M(M(x, y), z) \\&= L_{M(x, y)}(z) = \phi(M(x, y))(z)\end{aligned}$$

Hiermee hebben we bewezen dat G isomorf is met G^* . •

Opmerking 3.23. In de voorbeelden in Hoofdstuk 1 bekeken we groepen van transformaties van een verzameling X die bestonden uit de bijecties $f: X \rightarrow X$ die een bepaalde structuur op X behielden, bijvoorbeeld de structuur van vectorruimte. Dit betekent dat we naar bijecties f kijken die aan een bepaalde formule voldoen. Ook hier kunnen we de elementen f van G^* onderscheiden onder alle bijecties van X doordat ze aan een bepaalde formule (of lijst van formules) voldoen. De eis is

$$f(M(x, y)) = M(f(x), y) \text{ voor alle } x, y \in G$$

Ga zelf na f van de vorm L_a is d.e.s.d. als hij aan bovenstaande eis voldoet.

In bovenstaande voorbeelden zijn we enkele keren de situatie tegengekomen dat een deelverzameling van een groep G met ‘dezelfde’ binaire operatie (nauwkeuriger: een beperking van de oorspronkelijke operatie) weer een groep werd. We gaan nu vaststellen wat daar precies voor nodig is.

Definitie 3.24. Een *ondergroep* van een groep G is een deelverzameling $H \subset G$ met

1. $e \in H$,
2. $a, b \in H \implies ab \in H$,
3. $a \in H \implies a^{-1} \in H$.

We noteren $H < G$.

Indien $H < G$ dan is H op natuurlijke manier weer een groep door beperking van de vermenigvuldiging in G tot elementen van H .

Voorbeeld 3.25. Voor iedere groep G zijn $\{e\}$ en G ondergroepen. Dit zijn de triviale ondergroepen van G .

Voorbeeld 3.26. Vergelijken we Definitie 3.24 met het verhaal in Hoofdstuk 1 dan zien we dat wat we een ‘groep van transformaties van X ’ hebben genoemd niets anders is dan een ondergroep van $\text{Sym}(X)$.

Voorbeeld 3.27. Wat betreft de in Hoofdstuk 1 genoemde groepen hebben we verder: $\text{SO}(n) < \text{O}(n) < \text{E}(n)$ en $\text{SL}(n) < \text{GL}(n) < \text{Aff}(n)$ en bovendien $\text{SO}(n) < \text{SL}(n)$ en $\text{O}(n) < \text{GL}(n)$ en $\text{E}(n) < \text{Aff}(n)$.

Voorbeeld 3.28. Wat we in het vorige Hoofdstuk hebben gedaan is een opsomming geven van ondergroepen van $\text{SO}(2)$, $\text{O}(2)$, $\text{SO}(3)$ en $\text{O}(3)$. De eis voor de constructie in Voorbeeld 2.14 is dat B een ondergroep is van A .

Voorbeeld 3.29. Wat betreft de in Hoofdstuk 2 genoemde groepen hebben we verder:

- $\mathcal{C}_n < \mathcal{D}_n$ voor alle n en bovendien $\mathcal{C}_{jn} < \mathcal{C}_n$ en $\mathcal{D}_{jn} < \mathcal{D}_n$ voor alle j .
- $\mathcal{T} < \mathcal{O}$ en $\mathcal{T} < \mathcal{I}$ maar *niet* $\mathcal{O} < \mathcal{I}$.
- $\mathcal{C}_n < \mathcal{C}_{nh}$ en $\mathcal{C}_n < \mathcal{S}_{2n}$ en $\mathcal{C}_n < \mathcal{C}_{nv}$ voor alle n

en vele andere combinaties.

Voorbeeld 3.30. Zij I een willekeurige verzameling, en zij voor elke $i \in I$ gegeven een ondergroep H_i van de groep G . Dan is $\bigcap_{i \in I} H_i$ weer een ondergroep van G . In andere woorden: de doorsnede van een aantal ondergroepen is weer een ondergroep, en hiervoor is het niet relevant of dat aantal eindig is.

Bewijs. Opgave! •

Propositie 3.31. Zij G een groep, en zij $X \subset G$ een niet-lege deelverzameling. Dan is er onder alle ondergroepen van G die X bevatten een kleinste ondergroep, die we voortaan als $\langle X \rangle$ noteren. Deze kan op de volgende manieren beschreven worden:

- $\langle X \rangle$ is de doorsnede van alle ondergroepen die X bevatten.
- $\langle X \rangle$ bestaat precies uit alle elementen die te schrijven zijn als herhaald product van elementen van $X \cup X^{-1}$, waarbij $X^{-1} = \{x^{-1} ; x \in X\}$.

We noemen $\langle X \rangle$ de ondergroep voortgebracht door de verzameling X , en omgekeerd heet X een stelsel voortbrengers van die ondergroep.

Bewijs. Dat de vereiste doorsnede zinvol is en een ondergroep oplevert volgt uit Voorbeeld 3.30. In dit geval is

$$I = \{A \subset G ; X \subseteq A \text{ én } A \text{ is een ondergroep}\}$$

Dat de resulterende ondergroep van het goede soort is, en bevat in alle andere ondergroepen van de goede soort volgt direct uit de definitie.

Voor de tweede bewering moeten we voornamelijk nagaan dat de verzameling van zulke herhaalde producten voldoet aan de drie eisen voor een ondergroep. Maak zelf het bewijs af! •

Voorbeeld 3.32. Zij G een groep en zij $x \in G$. We bestuderen de ondergroep $\langle x \rangle$ voortgebracht door $\{x\}$. Er zijn twee mogelijkheden:

- Alle elementen x^j met $j \in \mathbf{Z}$ zijn verschillend. Dan is de afbeelding $\phi: \mathbf{Z} \rightarrow \langle x \rangle$ gedefinieerd door $\phi(j) = x^j$ een bijectie, en in feite een isomorfisme van de optelgroep van \mathbf{Z} naar $\langle x \rangle$.
- De elementen x^j zijn niet allen verschillend. Dan is een $j > 0$ met $x^j = e$ (waarom?). Zij n de kleinste dergelijke j . Dan zijn de elementen $e, x, x^2, \dots, x^{n-1}$ verschillend en precies alle elementen van $\langle X \rangle$. Er is een afbeelding $\phi: \mathbf{C}_n \rightarrow \langle x \rangle$ welke gedefinieerd wordt door $\phi(r_n^j) = x^j$, en deze afbeelding is een isomorfisme.

Stel dat $\langle x \rangle = G$, wat betekent G wordt voortgebracht door een enkel element. Dan noemt men de groep G *cyclisch*. Een cyclische groep is klaarblijkelijk isomorf met met \mathbf{Z} als hij oneindig is, en met zekere \mathbf{C}_n als hij eindig is.

Propositie 3.33. *Beschouw de optelgroep \mathbf{Z} van de gehele getallen, en zij H een ondergroep ongelijk $\{0\}$. Dan is H oneindig cyclisch.*

Bewijs. Er is een $n \in H$ die niet 0 is, en dan is n of $-n$ positief. Dat betekent dat verzameling $\{n \in H ; n > 0\}$ niet leeg is, en dus een kleinste element d heeft. We gaan laten zien dat $H = \langle d \rangle$. Het is alvast duidelijk dat $\langle d \rangle \subseteq H$.

Zij $x \in H$. Dan kunnen we schrijven $x = qd + r$ met $0 \leq r < d$. Stel je voor dat r niet nul was. Dan was $r = x - qd$ een positief element van H dat kleiner dan d was, in tegenspraak met de definitie van d . Dus $r = 0$ en $x = qd \in \langle d \rangle$. Dit laat zien dat $H \subseteq \langle d \rangle$. •

Voorbeeld 3.34. Laat a en b twee positieve gehele getallen zijn. Dan is $\langle a, b \rangle = \{ka + mb ; k \in \mathbf{Z}, m \in \mathbf{Z}\}$ een ondergroep van \mathbf{Z} en dus van de vorm $\langle d \rangle$. In de opgaven gaan we na dat d precies de *grootste gemene deler* is van a en b zoals besproken in de cursus Getallen.

Definitie 3.35. Het aantal elementen $\#(G)$ van een groep G heet de *orde* van G . De *orde* van een element $a \in G$ is de orde van de cyclische groep $\langle a \rangle$ voortgebracht door a .

Volgens bovenstaand verhaal is de orde van a gelijk aan de kleinste $n \in \mathbf{N}^*$ waarvoor $a^n = e$.

Een element $a \in G$ heeft orde 1 dan en slechts dan als a het eenheidselement e is. De rotatie r in de diëdergroep D_n van orde $2n$ heeft orde n , en de spiegelingen $t, rt, \dots, r^{n-1}t$ hebben alle orde 2.

Opmerking 3.36. Zij G een (abstracte) groep, met K als vermenigvuldiging. Zij ook H een groep, met L als vermenigvuldiging. Dan kunnen we de verzameling $G \times H$ de structuur van groep geven door een vermenigvuldiging M te definiëren als:

$$M((g_1, h_1), (g_2, h_2)) = (K(g_1, g_2), L(h_1, h_2))$$

4 Werkingen van groepen.

We onderzoeken nu de vraag wat we zijn ‘kwijtgeraakt’ bij de overgang van een transformatie-groep naar de onderliggende abstracte groep. Anders gezegd: gegeven is een abstracte groep G en we vragen ons af op wat voor manieren deze afkomstig kan zijn van een transformatie-groep op een zekere verzameling X .

Om dat soort vragen aan te kunnen pakken is het nuttig een begrip in te voeren dat een eerder ingevoerd begrip omvat:

Definitie 4.1. Zij G en H beide groepen. Een afbeelding $\phi: G \rightarrow H$ heet een *homomorfisme* als $\phi(ab) = \phi(a)\phi(b)$ voor alle $a, b \in G$.

Het verschil met Definitie 3.15 is dus dat we niet langer eisen dat de afbeelding ϕ een bijectie is. Een isomorfisme is dus niets anders dan een bijectief homomorfisme.

Propositie 4.2. Stel $\phi: G \rightarrow H$ een homomorfisme van groepen. Dan is $\phi(e) = e$ en $\phi(a^{-1}) = \phi(a)^{-1}$ voor alle $a \in G$.

Bewijs. Uit $\phi(e) = \phi(ee) = \phi(e)\phi(e)$ volgt dat $\phi(e) = e$. Ook geldt $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e$ en evenzo $\phi(a^{-1})\phi(a) = e$ voor alle $a \in G$. •

Propositie 4.3. Als $\phi: G \rightarrow H$ een homomorfisme is dan is zijn beeldverzameling $\text{Im}(\phi)$ een ondergroep van H . Als ϕ een injectief homomorfisme is dan is deze ondergroep isomorf met G .

Bewijs. Stel dat $x, y \in \text{Im}(\phi)$. Dat betekent dat er $a, b \in G$ zijn met $x = \phi(a)$ en $y = \phi(b)$. Nu is $xy = \phi(a)\phi(b) = \phi(ab) \in \text{Im}(\phi)$. Verder is $x^{-1} = \phi(a)^{-1} = \phi(a^{-1}) \in \text{Im}(\phi)$. Tenslotte is $e = \phi(e) \in \text{Im}(\phi)$. Dus $\text{Im}(\phi)$ is een ondergroep van H .

Als we ϕ zien als een afbeelding naar $\text{Im}(\phi)$ in plaats van H dan is hij surjectief. De injectiviteit en de homomorfie-eigenschap blijven ongewijzigd, dus deze afbeelding is een bijectief homomorfisme en dus een isomorfisme. •

Voorbeeld 4.4. De determinant levert een homomorfisme $\text{GL}(n, \mathbf{F}) \rightarrow \mathbf{F}^*$ (zie Voorbeeld 3.11), en een homomorfisme $\text{O}(n, \mathbf{R}) \rightarrow \{+1, -1\}$.

Voorbeeld 4.5. Zij $\phi: \text{SU}(2) \rightarrow \text{GL}(3, \mathbf{R})$ de afbeelding gedefiniëerd door

$$\begin{aligned} & \phi \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \\ &= \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2bc - 2ad & 2ac + 2bd \\ 2bc + 2ad & a^2 - b^2 + c^2 - d^2 & 2cd - 2ab \\ 2bd - 2ac & 2ab + 2cd & a^2 - b^2 - c^2 + d^2 \end{pmatrix} \end{aligned}$$

Je kunt narekenen dat ϕ een homomorfisme is, en dat hij in feite in $\text{SO}(3)$ terechtkomt.

Het is eveneens nuttig om Definitie 1.1 op een soortgelijke manier te verruimen:

Definitie 4.6. Laat G een abstracte groep en X een niet-lege verzameling zijn. Een werking van G op X is een homomorfisme $\phi: G \rightarrow \text{Sym}(X)$.

Ga na dat in deze situatie de beeldverzameling van ϕ een groep van transformaties van X is. Dus als de afbeelding ϕ toevallig injectief is, dan is G isomorf met (de onderliggende abstracte groep van) een groep van transformaties van X .

Een andere, equivalente, beschrijving van bovenstaand begrip is echter meer gebruikelijk:

Definitie 4.7. Een *linksactie* of *linkswerking* van G op X is een afbeelding $\lambda: G \times X \rightarrow X$ die aan de volgende eigenschappen voldoet

- $a(bx) = (ab)x$ voor alle $a, b \in G$ en voor alle $x \in X$.
- $ex = x$ voor alle $x \in X$.

Hier hebben we $\lambda(g, x)$ gemakshalve als gx genoteerd, en evenzo de notatie voor de vermenigvuldiging in G onderdrukt.

Opmerking 4.8. Zij gegeven een linkswerking $\lambda: G \times X \rightarrow X$. Dan hoort bij iedere $a \in G$ een afbeelding $\lambda_a: X \rightarrow X$ door middel van de formule $\lambda_a(x) = \lambda(a, x)$. Dit heet de *links-vermenigvuldiging* behorende bij a . Laten we a variëren dan vinden we zo een afbeelding $\phi: G \rightarrow \text{Sym}(X)$ met behulp van de formule $\phi(a) = \lambda_a$. Ga zelf na dat deze afbeelding een homomorfisme is, en dus een werking oplevert.

Het voorkomen van het woord ‘links’ in bovenstaand verhaal suggereert dat er ook een gespiegelde versie bestaat:

Definitie 4.9. In analogie met Definitie 4.7 is een *rechtsactie* of *rechtswerking* van G op X een afbeelding $\rho: X \times G \rightarrow X$ die aan de volgende eigenschappen voldoet:

- $(xa)b = x(ab)$ voor alle $a, b \in G$ en voor alle $x \in X$.
- $xe = x$ voor alle $x \in X$.

Opmerking 4.10. In analogie met Opmerking 4.10 krijgen we uit een rechtswerking $\rho: X \times G \rightarrow X$ voor elke $a \in G$ een *rechtsvermenigvuldiging* $\rho_a: X \rightarrow X$ door $\rho_a(x) = \rho(x, a)$. Laten we a variëren dan vinden we zo een afbeelding $\phi: G \rightarrow \text{Sym}(X)$ met behulp van de formule $\phi(a) = \rho_a$. Ga na dat dit *geen* homomorfisme is en dus geen werking, maar dat de afbeelding $\phi: G \rightarrow \text{Sym}(X)$ gedefinieerd door $\phi(a) = \rho_a^{-1}$ dat wel is.

Ga tenslotte na dat omgekeerd een werking $\phi: G \rightarrow \text{Sym}(X)$ een linkswerking en een rechtswerking oplevert. Wat is de relatie tussen die twee?

Voorbeeld 4.11. Zoals al aangestipt is elke groep van transformaties van een verzameling X op te vatten als een werking van G op X (en dus ook als linkswerking of rechtswerking).

In het bijzonder als V een vectorruimte is dan is er een werking van $\text{GL}(V)$ op V . De linkswerking van $\text{GL}(n, \mathbf{R})$ op \mathbf{R}^n is niets anders dan matrixvermenigvuldiging van een $n \times n$ -matrix en een kolomvector.

Als V ook nog voorzien is van een scalair product B dan is er een werking van $\text{O}(V, B)$ op V .

De in Hoofdstuk 2 besproken voorbeelden van groepen van transformaties van \mathbf{R}^3 zijn even zovele voorbeelden van linkswerkingen van abstracte groepen op \mathbf{R}^3 .

Voorbeeld 4.12. Als H een ondergroep van G is dan werkt H op G door linksvermenigvuldiging: $\lambda_a(b) = ab$ voor $a \in H$ en $b \in G$.

Voorbeeld 4.13. Zij G een groep. Dan is er een linkswerking λ van de groep G op de verzameling G gedefinieerd door

$$\lambda(g, x) = gxg^{-1}$$

Dit heet de werking door *conjugatie*.

Definitie 4.14. Zij gegeven een linkswerking van G op X . Voor $p \in X$ definiëren we de *stabilizator* of *isotropiegroep* van p in G door

$$\text{Stab}_G(p) = \{g \in G; gp = p\}$$

Zoals de naam al suggereert is de isotropiegroep van p in G een ondergroep van G . Als het heel G is dan betekent dit dat $gp = p$ voor alle $g \in G$. In dat geval noemen we p een *vast punt* van de werking.

Voorbeeld 4.15. In de situatie van Voorbeeld 4.13 is de isotropiegroep van x de groep

$$Z_G(x) = \{g \in G; gxg^{-1} = x\} = \{g \in G; gx = xg\}$$

Dit heet de *centralizator* van x in G .

Merk op dat in ieder geval $\langle x \rangle \subseteq Z_G(x)$. In het bijzonder is $Z_G(x)$ niet-triviaal als G niet-triviaal is.

Voorbeeld 4.16. De symmetriegroep van de kubus \mathcal{O}_h is bevat in $\text{O}(3)$ en dus in $\text{GL}(3)$ en komt dus voorzien van een linkswerking op \mathbf{R}^3 . We bepalen de isotropiegroep voor elke $p = (x, y, z) \in \mathbf{R}^3$:

- Als $|x|$, $|y|$ en $|z|$ verschillend en ongelijk nul zijn dan bestaat de isotropiegroep alleen uit het eenheids-element.

- Als $|x| = |y|$ en $|z|$ verschillend zijn en ongelijk nul dan bestaat de isotropiegroep uit twee elementen

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & \eta & 0 \\ \eta & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

waar $\eta = \frac{y}{x}$. Iets soortgelijks treedt op als $|y| = |z|$ of $|x| = |z|$.

- Als $|x| = |y| = |z|$ ongelijk nul is dan bestaat de isotropiegroep uit 6 elementen:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & \eta & 0 \\ \eta & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & \zeta \\ 0 & 1 & 0 \\ \zeta & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \eta\zeta \\ 0 & \eta\zeta & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & \zeta \\ \eta & 0 & 0 \\ 0 & \eta\zeta & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \eta & 0 \\ 0 & 0 & \eta\zeta \\ \zeta & 0 & 0 \end{pmatrix}$$

waar $\eta = \frac{y}{x}$ en $\zeta = \frac{z}{x}$.

- Als $|x|$ en $|y|$ verschillend en ongelijk nul zijn maar $z = 0$ dan bestaat de isotropiegroep uit 2 elementen:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Iets soortgelijks treedt op als $x = 0$ of $y = 0$.

- Als $|x| = |y|$ ongelijk nul is maar $z = 0$ dan bestaat de isotropiegroep uit 4 elementen:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & \eta & 0 \\ \eta & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & \eta & 0 \\ \eta & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

waar $\eta = \frac{y}{x}$. Iets soortgelijks treedt op als $x = 0$ of $y = 0$.

- Als $|x|$ ongelijk nul is maar $y = z = 0$ dan bestaat de isotropiegroep uit 8 elementen:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

- Als $x = y = z = 0$ dan is de isotropiegroep heel \mathcal{O}_h .

Definitie 4.17. Zij gegeven een linkswerking $\lambda: G \times X \rightarrow X$. We noteren ax voor $\lambda(a, x)$. Met de *baan* Gp van een punt $p \in X$ bedoelen we de verzameling $\{ap; a \in G\}$.

We kunnen dit ook beschrijven in termen van equivalentie-relaties:

Lemma 4.18. *We definiëren een relatie \sim op X door $x \sim y$ dan en slechts dan als er $a \in G$ bestaat met $x = ay$. Met andere woorden $x \sim y \iff x \in Gy$. Dan is de relatie \sim op X een equivalentierelatie.*

Bewijs. We moeten drie eisen controleren.

- Er geldt $x \sim x$ voor alle $x \in X$ aangezien $x = ex$.
- Als $x \sim y$ dan is $x = ay$ voor zekere $a \in G$. Linksvermenigvuldiging met a^{-1} geeft $a^{-1}x = a^{-1}(ay) = (a^{-1}a)y = ey = y$, en dus volgt $y \sim x$.
- Tenslotte stel $x \sim y$ en $y \sim z$. Dan is $x = ay$ en $y = bz$ voor zekere $a, b \in G$. Dus $x = a(bz) = (ab)z$ waaruit volgt $x \sim z$.

Merk op dat de equivalentieklasse van een $y \in X$ precies Gy is. •

Definitie 4.19. De collectie van banen van G op X heet het *quotiënt* van X naar G , en wordt genoteerd met $G \backslash X$. Voor een rechtsactie van G op X gaat alles mutatis mutandis door. Het quotiënt van X naar G wordt dan aangegeven met X/G .

Voorbeeld 4.20. De symmetrische groep $\text{Sym}(X)$ heeft op X precies één baan. Als $1 \leq \dim(V) < \infty$ dan heeft $\text{GL}(V)$ twee banen op V , namelijk $\{0\}$ en $V \setminus \{0\}$. De banen van de orthogonale groep $\text{O}(n, \mathbf{R})$ op \mathbf{R}^n voor $n \geq 1$ zijn de (holle) bollen met straal r voor $0 \leq r < \infty$.

Voorbeeld 4.21. In de situatie van Voorbeeld 4.13 is de baan van $x \in G$ de verzameling

$$C(x) = \{g x g^{-1}; g \in G\}$$

Dit heet de *conjugatie-klasse* van x in G .

Een speciaal geval van quotiënt-vorming is van bijzonder belang:

Definitie 4.22. De actie van G op X heet *vrij* als $\text{Stab}_G(p) = \{e\}$ voor alle $p \in X$. In dat geval krijgen we een bijectie van G met elke baan. De bijectie $G \rightarrow Gp$ wordt gegeven door $a \mapsto ap$.

Voorbeeld 4.23. Omdat $\mathcal{T} \subset \mathcal{I}$ werkt \mathcal{T} op X_{ico} . Men rekent gemakkelijk na dat deze werking vrij is. Bovendien bestaat X_{ico} uit één enkele baan.

Voorbeeld 4.24. Zij G een groep en H een ondergroep. De baan $Ha = \{ba; b \in H\}$ van H door a voor de actie van linksvermenigvuldiging van H op G heet de *rechternevenklasse* van $a \in G$ naar H . Evenzo heet de baan $aH = \{ab; b \in H\}$ van H door a voor de actie van rechtsvermenigvuldiging van H op G de *linkernevenklasse* van $a \in G$ naar H . We noteren $H \backslash G$ voor de collectie van rechternevenklassen en G/H voor de collectie van linkernevenklassen in G naar H .

Stelling 4.25. Voor een vrije actie van een eindige groep G op een eindige verzameling X geldt:

$$\#(X) = \#(G) \cdot \#(G \backslash X)$$

Hier staat $\#(X)$ voor de cardinaliteit (het aantal elementen) van de verzameling X .

Bewijs. Voor een vrije actie van G op X is iedere baan in X in bijectie met G . De bewering volgt nu door de elementen van X baan voor baan te tellen. •

Gevolg 4.26. Voor $H < G$ en $\#(G) < \infty$ geldt: $\#(G/H) = \frac{\#(G)}{\#(H)}$.

Bewijs. Pas de bovenstaande stelling toe voor de actie van rechtsvermenigvuldiging van H op G . •

Het getal $\#(G/H)$ heet ook wel de *index* van H in G , en wordt vaak genoteerd met $[G : H]$.

Gevolg 4.27. (*Stelling van Lagrange*). Voor een eindige groep G is de orde van ieder element een deler van de orde van de groep. Anders gezegd: Zij a een element van een groep G van n elementen. Dan is $a^n = 1$.

Bewijs. Zij $a \in G$ en pas Gevolg 4.26 toe op $H = \langle a \rangle$, de ondergroep voortgebracht door a . •

Gevolg 4.28. (*Fermat*). Zij p een priemgetal, en zij $k \in \mathbf{Z}$ niet deelbaar door p . Dan is $k^{p-1} - 1$ deelbaar door p .

Bewijs. Beschouw de optelgroep van \mathbf{Z} . De verzameling van veelvouden van p vormt een ondergroep $p\mathbf{Z}$. Vorm de verzameling van nevenklassen $\mathbf{Z}/p\mathbf{Z}$, met p elementen. De verzameling van niet-triviale nevenklassen $(\mathbf{Z}/p\mathbf{Z})^*$ vormt een groep onder de bewerking die afkomstig is van vermenigvuldiging van gehele getallen. Deze groep heeft $p - 1$ elementen. Pas nu bovenstaand gevolg toe op de klasse van k . •

Deze stelling en verfijningen ervan zijn van groot belang voor het construeren van snelle algoritmes die gehele getallen testen op priem zijn.

Stelling 4.29. *Er is een standaard bijectie van $G/\text{Stab}_G(p)$ naar Gp . Deze beeldt de linkernevenklasse $a\text{Stab}_G(p)$ af naar ap .*

Bewijs. Noteer H voor $\text{Stab}_G(p)$. We proberen een afbeelding $\phi: G/H \rightarrow Gp$ te definiëren door de formule $\phi(aH) = ap$. Om te zien dat dit een afbeelding definieert moeten we controleren dat $aH = bH \Rightarrow ap = bp$.

Stel dat $aH = bH$. Dan is $b \in aH$, wat betekent dat er een $h \in H$ is met $b = ah$. Nu is $bp = (ah)p = a(hp) = ap$ immers $hp = p$ aangezien $h \in \text{Stab}_G(p)$. De afbeelding ϕ is dus welgedefinieerd.

Stel omgekeerd dat $ap = bp$. Dan is $a^{-1}bp = a^{-1}ap = ep = p$, wat betekent dat $a^{-1}b \in \text{Stab}_G(p) = H$. Nu geldt:

- Als $h \in H$ dan is $bh = a(a^{-1}bh) \in aH$. Dit betekent dat $bH \subset aH$.
- Als $h \in H$ dan is $ah = b((a^{-1}b)^{-1}h) \in bH$. Dit betekent dat $aH \subset bH$.

Samengevat $aH = bH$. De afbeelding ϕ is dus injectief. Hij is ook duidelijk surjectief, want zijn beeld bestaat uit de ap met $a \in G$, en dat is juist Gp . •

Gevolg 4.30. *Voor een actie van een eindige groep G op een eindige verzameling X geldt:*

$$\#(Gp) = \frac{\#(G)}{\#(\text{Stab}_G(p))}$$

Bewijs. Combineer Gevolg 4.26 met Stelling 4.29. •

Zo geldt in Voorbeeld 4.16 dat de baan van p in de besproken gevallen respectievelijk 48, 24, 8, 24, 12, 6 of 1 punt telt.

Voorbeeld 4.31. Door bovenstaande formule toe te passen op de situatie van Voorbeeld 4.13 vinden we

$$\#G = \#Z_G(g) \cdot \#C(g)$$

voor elke $g \in G$.

5 Groepen van orthogonale transformaties.

In Hoofdstuk 2 is bewezen dat de daar gegeven opsomming van groepen van orthogonale transformaties van \mathbf{R}^2 en \mathbf{R}^3 volledig was. In dit Hoofdstuk gaan we dat bewijzen. We behandelen eerst de ondergroepen van $\text{SO}(2)$ en $\text{SO}(3)$, en aan het eind van dit Hoofdstuk de overblijvende ondergroepen van $\text{O}(2)$ en $\text{O}(3)$.

De inhoud van dit Hoofdstuk maakt geen deel uit van de tentamenstof. Het is ter informatie en illustratie.

Stelling 5.1. *Zij G een eindige ondergroep van $\text{SO}(2)$. Dan is $G = C_n$ voor zekere n .*

Bewijs. Schrijf $G = \{g_1, g_2, \dots, g_n\}$. Volgens Propositie 12.16 is elk element van G te schrijven in de vorm

$$r(\phi) = \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix}$$

voor zekere $\phi \in \mathbf{R}$ met $0 < \phi \leq 2\pi$. We kunnen dus schrijven $g_i = r(\phi_i)$ voor zekere ϕ_i met $0 < \phi_i \leq 2\pi$.

Door vernummernen mogen we aannemen dat

$$0 < \phi_1 < \phi_2 < \dots < \phi_n = 2\pi.$$

Nu geldt voor $k = 2, \dots, n$:

- Enerzijds $r(\phi_k - \phi_{k-1}) = r(\phi_k)r(\phi_{k-1})^{-1} = g_k g_{k-1}^{-1} \in G$ en $0 < \phi_k - \phi_{k-1} \leq 2\pi$. Hieruit volgt dat $\phi_k - \phi_{k-1}$ onder de ϕ_i voorkomt. In het bijzonder $\phi_k - \phi_{k-1} \geq \phi_1$.
- Anderzijds $r(\phi_{k-1} + \phi_1) = r(\phi_{k-1})r(\phi_1) = g_{k-1}g_1 \in G$ en $\phi_{k-1} + \phi_1 \leq \phi_k \leq 2\pi$. Hieruit volgt dat $\phi_{k-1} + \phi_1$ onder de ϕ_i voorkomt, en wel die met $i > k - 1$. In het bijzonder is $\phi_{k-1} + \phi_1 \geq \phi_k$.

Samengevat hebben we $\phi_k = \phi_{k-1} + \phi_1$ voor elke $k \geq 2$. Bij inductie volgt nu dat $\phi_k = k\phi_1$. In het bijzonder is $\phi_1 = \frac{\phi_n}{n} = \frac{2\pi}{n}$ en $r(\phi_1) = r\left(\frac{2\pi}{n}\right) = r_n$. We zien dus dat $G = \langle r_n \rangle = C_n$. •

Gevolg 5.2. *Zij G een eindige ondergroep van $\text{SO}(2)$ van orde m . Als $y \in \mathbf{R}^2$ dan is de baan van y onder G een regelmatige m -hoek óf $\{0\}$.*

Bewijs. Als $y \neq 0$ dan zijn de punten $y_k = r_{m,k}y = (r_m)^k y$ voor $k = 0, 1, \dots, m-1$ allemaal verschillend. Immers als $0 \leq j < k \leq m-1$ dan volgt uit $y_k = y_j$ dat $(r_m)^{k-j}y = y$. Maar dat kan niet want $r_m^{k-j} - 1$ heeft determinant $2 - 2\cos(2(k-j)\pi/m) \neq 0$. •

Gevolg 5.3. *Zij F een eindige ondergroep van $\text{SO}(3)$ die e_3 als vast punt heeft. Dan is $F = \mathcal{C}_m$ voor zekere m .*

Bewijs. Stel $f \in F \subset \text{SO}(3)$ wordt beschreven door de matrix (α_{ij}) . Dat betekent dat $f(e_j) = \sum_i \alpha_{ij} e_i$ voor elke j . In het bijzonder betekent $f(e_3) = e_3$ dat $\alpha_{13} = 0$ en $\alpha_{23} = 0$ en $\alpha_{33} = 1$. Uit het feit dat f orthogonaal is volgt dat

$$\begin{aligned} 0 &= \langle e_1, e_3 \rangle = \langle f(e_1), f(e_3) \rangle \\ &= \langle \alpha_{11} e_1 + \alpha_{21} e_2 + \alpha_{31} e_3, e_3 \rangle \\ &= \alpha_{11} \langle e_1, e_3 \rangle + \alpha_{21} \langle e_2, e_3 \rangle + \alpha_{31} \langle e_3, e_3 \rangle = \alpha_{31} \end{aligned}$$

en evenzo $\alpha_{32} = 0$. Dus f is van de vorm $j(g)$ voor zekere $g \in \text{SO}(2)$, waar $j: \text{SO}(2) \rightarrow \text{SO}(3)$ de afbeelding is gegeven door

$$j \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{12} & \alpha_{22} \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & 0 \\ \alpha_{12} & \alpha_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Dit betekent dat F het j -beeld is van een eindige ondergroep van $\text{SO}(2)$, namelijk van $G = \{g \in \text{SO}(2); j(g) \in F\}$. Volgens Stelling 5.1 moet deze G van de vorm \mathcal{C}_m zijn voor zekere m . Dus is F zelf $j(\mathcal{C}_m) = \mathcal{C}_m$. •

Gevolg 5.4. *Zij $y \in \mathbf{R}^3$. Als $r = \|(y_1, y_2)\|$ positief is dan is de baan van y onder \mathcal{C}_m een regelmatige m -hoek met straal r , liggend in het vlak $V = \{z \in \mathbf{R}^3; z_3 = y_3\}$. Als $r = 0$ dan bestaat de baan uit alleen y zelf.*

Bewijs. Stel dat z in de baan van y zit, zeg $z = f(y)$ met $f = j(g)$ en $g \in \mathcal{C}_m$. De formule

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = j(g) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

betekent precies hetzelfde als

$$z_3 = y_3 \quad \text{en} \quad \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = g \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

Het resultaat volgt nu door toepassing van Gevolg 5.2. •

Gevolg 5.5. *Zij $p \in \mathbf{R}^3$ met $\|p\| = 1$. Zij H een eindige ondergroep van $\text{SO}(3)$ die p als vast punt heeft. Dan is er een $T \in \text{SO}(3)$ en een m met $H = T\mathcal{C}_m T^{-1}$. In het bijzonder is H cyclisch van orde m .*

Bewijs. Kies een basis van de vectorruimte $V = p^\perp = \{x \in \mathbf{R}^3; \langle x, p \rangle = 0\}$ en pas daarop het Gramm-Schmidt procédé toe. Dat levert een orthonormale basis $\{f_1, f_2\}$ van V . Tesaamen met $f_3 = p$ levert dat een orthonormale basis van \mathbf{R}^3 .

Zij $T: \mathbf{R}^3 \rightarrow \mathbf{R}^3$ de unieke lineaire afbeelding met $T(e_i) = f_i$ voor $i = 1, 2, 3$. Dan is T een orthogonale transformatie. In het bijzonder is $\det(T) \in \{+1, -1\}$. Door zo nodig de rollen van f_1 en f_2 te verwisselen kunnen we er bovendien voor zorgen dat $\det(T) = +1$.

Noteer $F = T^{-1}HT = \{T^{-1}hT; h \in H\}$. Als $f \in F$ dan is er $h \in H$ met $f = T^{-1}hT$ dus $f(e_3) = T^{-1}hTe_3 = T^{-1}hf_3 = T^{-1}hp = T^{-1}p = T^{-1}f_3 = e_3$. Dus F voldoet aan de voorwaarden van het vorige gevolg en is dus van de vorm \mathcal{C}_m voor zekere m . Nu is $H = TFT^{-1} = TC_mT^{-1}$. •

Gevolg 5.6. Zij $q \in \mathbf{R}^3$ met $\|q\| = 1$ en zij p en H als boven. Als $q \notin \{p, -p\}$ dan is de baan van q in \mathbf{R}^3 onder H een regelmatige m -hoek liggend in het vlak $W = \{w \in \mathbf{R}^3; \langle w, p \rangle = \langle q, p \rangle\}$. Als $q \in \{p, -p\}$ dan bestaat de baan uit één punt.

Bewijs. Zij T als in het voorgaande bewijs, en schrijf $y = T^{-1}q$. Dan is de baan van q gelijk aan $Hq = TC_mT^{-1}q = TC_my$ dus het T -beeld van de baan van y onder \mathcal{C}_m . Volgens Gevolg 5.4 is het dus meestal het T -beeld van een regelmatige m -hoek in het vlak $V = \{z \in \mathbf{R}^3; z_3 = y_3\}$. Maar het T -beeld van het vlak V is het vlak W . •

Zij G een eindige ondergroep van $\text{SO}(3)$. Om de mogelijkheden voor G de onderzoeken bekijken we hoe deze groep werkt op het boloppervlak $S = \{p \in \mathbf{R}^3; \|p\| = 1\}$.

Stelling 5.7. Zij G een ondergroep van $\text{SO}(3)$ van cardinaliteit $n < \infty$.

Dan zijn er natuurlijke getallen r en n_1, n_2, \dots, n_r zo dat

$$2(n-1) = \sum_{i=1}^r \frac{n}{n_i} (n_i - 1) \quad (3)$$

Bewijs. Bekijk de verzameling $Y = \{(a, p) \in G \times S; a(p) = p, a \neq e\}$. We tellen de elementen op twee manieren:

- Bij elke $a \in G - \{e\}$ zijn er twee mogelijkheden voor p . Het aantal elementen van Y is dus $2(n-1)$.
- Voor een gegeven $p \in S$ is er alleen een bijdrage als $\text{Stab}_G(p) \neq \{e\}$; we noemen p dan een *pool* van G . In dat geval zijn er $\#(\text{Stab}_G(p)) - 1$ mogelijkheden voor a .

Schrijf \mathcal{P} voor de verzameling van polen van G . We krijgen dan de formule

$$2(n-1) = \sum_{p \in \mathcal{P}} (\#(\text{Stab}_G(p)) - 1)$$

We gaan dit nog wat herschrijven.

Stel dat $p \in \mathcal{P}$ is en dat $q = g(p)$ met $g \in G$. Men rekent eenvoudig na dat $\text{Stab}_G(q) = g \text{Stab}_G(p) g^{-1} \neq \{e\}$. Dus is ook $q \in \mathcal{P}$. De werking van G op \mathbf{R}^3 voert dus \mathcal{P} in zichzelf over en levert een werking van G op \mathcal{P} . Bovendien levert elke q in de baan van p dezelfde bijdrage aan bovenstaande som.

Schrijf \mathcal{P} als disjuncte vereniging van G -banen \mathcal{P}_i en kies een representant $p_i \in \mathcal{P}_i$ voor $i = 1, 2, \dots, r$. Noteer $F_i = \text{Stab}_G(p_i)$ en $n_i = \#(F_i)$. Volgens Gevolg 4.30 is $\#(\mathcal{P}_i) = n/n_i$. Elk punt $p \in \mathcal{P}_i$ levert een bijdrage $(n_i - 1)$ aan bovenstaande som. •

Opmerking 5.8. Volgens Gevolg 5.5 is F_i cyclisch van orde n_i . Stel dat een verzameling Z bestaande uit vectoren van lengte 1 door F_i in zichzelf wordt overgevoerd (bijvoorbeeld als $Z = \mathcal{P}_i$). Dan hebben we te maken met een werking van F_i op Z . Volgens Gevolg 5.6 bestaat Z dan uit een aantal regelmatige n_i -hoeken (elk liggend in een vlak loodrecht op p_i), eventueel het punt p_i en eventueel het punt $-p_i$.

In het bijzonder is de cardinaliteit van Z een veelvoud van n_i plus 0, 1 of 2.

Stelling 5.9. *De enige oplossingen van vergelijking (3) met $n_1 \leq n_2 \leq \dots$ zijn:*

- $r = 1$ en $n = 1$.
- $r = 2$, $n_1 = n_2 = n$ met n willekeurig.
- $r = 3$, $n_1 = 2$, $n_2 = 2$, $n_3 = k$ en $n = 2k$ met k willekeurig.
- $r = 3$, $n_1 = 2$, $n_2 = 3$, $n_3 = 3$, $n = 12$.
- $r = 3$, $n_1 = 2$, $n_2 = 3$, $n_3 = 4$, $n = 24$.
- $r = 3$, $n_1 = 2$, $n_2 = 3$, $n_3 = 5$, $n = 60$.

Bewijs. We kunnen de vergelijking herschrijven als

$$2 - \frac{2}{n} = r - \sum_{i=1}^r \frac{1}{n_i}$$

Nu is $n_i \geq 2$ anders was p_i geen pool, dus

$$2 > 2 - \frac{2}{n} \geq r - \sum_{i=1}^r \frac{1}{2} = \frac{r}{2}$$

wat betekent dat $r < 4$.

- Als $r = 1$ dan is $\frac{2}{n} = 1 + \frac{1}{n_1} \geq 1 + \frac{1}{n}$, dus $n \leq 1$, en dus $n = 1$.

- Als $r = 2$ dan is $\frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} \geq \frac{1}{n} + \frac{1}{n}$, dus $n_1 = n_2 = n$.
- Als $r = 3$ dan staat er

$$\frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} - 1$$

Als $n_1 \geq 3$ dan $n_2 \geq 3$ en $n_3 \geq 3$ en dan is het rechterlid niet positief, een tegenspraak. Een soortgelijke tegenspraak volgt als $n_1 = 2$ maar $n_2 \geq 4$. Tenslotte volgt een soortgelijke tegenspraak als $n_1 = 2$ en $n_2 = 3$ maar $n_3 \geq 6$.

Dit laat alleen de vermelde mogelijkheden over. •

Zij G een eindige ondergroep van $\text{SO}(3)$, en zij $T \in \text{SO}(3)$. Dan is $TGT^{-1} = \{TgT^{-1} ; g \in G\}$ eveneens een eindige ondergroep van $\text{SO}(3)$. Bovendien hoort bij deze ondergroep hetzelfde rijtje (n_1, \dots, n_r) als bij G .

We gaan nu aantonen dat omgekeerd bij elk van de rijtjes (n_1, \dots, n_r) een eindige ondergroep van $\text{SO}(3)$ hoort die uniek is tot op het zojuist beschreven ‘conjugeren’ na.

Voorbeeld 5.10. Geval $n_1 = 2$ $n_2 = 3$, $n_3 = 3$, $n = 12$.

Volgens Opmerking 5.6 toegepast op F_3 bestaat $Z = \mathcal{P}_3$ uit een aantal regelmatig 3-hoeken, eventueel het punt p_3 , en eventueel het punt $-p_3$.

Omdat \mathcal{P}_3 uit $n/n_3 = 4$ punten bestaat en het punt p_3 bevat kan hij het punt $-p_3$ niet bevatten. De overige 3 punten liggen dus even ver van elkaar, en even ver van p_3 .

Omdat de keuze van p_3 willekeurig was betekent dit dat alle 4 punten van \mathcal{P}_3 even ver van elkaar liggen, en dus de hoekpunten vormen van een regelmatig viervlak.

Kies nu $a \in \text{SO}(3)$ zo dat $\mathcal{P}_3 = a(X_{tet})$. Dan voert elk element van $a^{-1}Ga$ de verzameling X_{tet} in zichzelf over en zit dus ook in \mathcal{T} . Maar $a^{-1}Ga$ en \mathcal{T} hebben allebei orde 12. Dus de inclusie is een gelijkheid: $a^{-1}Ga = \mathcal{T}$ oftewel $G = a\mathcal{T}a^{-1}$.

De baan \mathcal{P}_1 van p_1 correspondeert nu met de 6 middens van de ribben van het viervlak. De baan \mathcal{P}_2 van p_2 correspondeert met de vier middens van de zijvlakken van het viervlak; deze vormen ook weer hoekpunten van een regelmatig viervlak.

Voorbeeld 5.11. Geval $n_1 = 2$ $n_2 = 3$, $n_3 = 4$, $n = 24$.

Volgens Opmerking 5.6 toegepast op F_3 bestaat $Z = \mathcal{P}_3$ uit een aantal regelmatige 4-hoeken, eventueel het punt p_3 , en eventueel het punt $-p_3$.

Omdat \mathcal{P}_3 uit $n/n_3 = 6$ punten bestaat en het punt p_3 bevat moet hij het punt $-p_3$ ook bevatten. De overige 4 punten vormen een vierkant en liggen even ver van p_3 . In het bijzonder vormen ze twee paren tegengestelden.

Omdat de keuze van p_3 willekeurig was betekent dit dat de 6 punten van \mathcal{P}_3 de hoekpunten vormen van een regelmatig achthoek. Zoals in het vorige voorbeeld volgt hieruit dat G na een conjugatie samenvalt met \mathcal{O} .

De baan \mathcal{P}_1 van p_1 correspondeert nu met de 12 middens van de ribben van het viervlak, de baan \mathcal{P}_2 van p_2 met de 8 middens van de zijvlakken van het achthoek; deze vormen de hoekpunten van een kubus.

Voorbeeld 5.12. Geval $n_1 = 2$ $n_2 = 3$, $n_3 = 5$, $n = 60$.

Volgens Opmerking 5.6 toegepast op F_3 bestaat $Z = \mathcal{P}_3$ uit een aantal regelmatig 5-hoeken, eventueel het punt p_3 , en eventueel het punt $-p_3$.

Omdat \mathcal{P}_3 uit $n/n_3 = 12$ punten bestaat en het punt p_3 bevat moet hij het punt $-p_3$ ook bevatten. De overige 10 punten vormen twee regelmatige vijfhoeken elk liggend in een vlak loodrecht op p_3 .

Omdat de keuze van p_3 willekeurig was vinden we zoveel gelijkheden voor afstanden tussen punten van \mathcal{P}_3 dat hieruit valt aft te leiden dat deze punten de hoekpunten vormen van een regelmatig twintigvlak. Zoals in het vorige voorbeeld volgt hieruit dat G na een conjugatie samenvalt met \mathcal{I} .

De baan \mathcal{P}_1 van p_1 correspondeert nu met de 30 middens van de ribben van het twintigvlak. De baan \mathcal{P}_2 van p_2 met de 20 middens van de zijvlakken van het twintigvlak; deze vormen de hoekpunten van een regelmatig twaalfvlak.

Voorbeeld 5.13. Geval $n_1 = 2$ $n_2 = 2$, $n_3 = k$, $n = 2k$.

Volgens Opmerking 5.6 toegepast op F_3 bestaat \mathcal{P}_3 uit een aantal regelmatige k -hoeken, eventueel het punt p_3 , en eventueel het punt $-p_3$. Omdat \mathcal{P}_3 uit $n/n_3 = 2$ punten bestaat en het punt p_3 bevat moet hij het punt $-p_3$ ook bevatten. Dus \mathcal{P}_3 is precies $\{p_3, -p_3\}$.

Volgens Opmerking 5.6 toegepast op F_3 bestaat \mathcal{P}_1 uit een aantal regelmatige k -hoeken, eventueel het punt p_3 , en eventueel het punt $-p_3$. Omdat \mathcal{P}_1 uit $n/n_1 = k$ punten bestaat en het punt p_3 niet bevat kan hij het punt $-p_3$ niet bevatten. Dus \mathcal{P}_1 bestaat uit punten in een regelmatige k -hoek die even ver van p_3 af liggen, en ook even ver van $-p_3$.

We mogen wel aannemen dat $p_3 = e_3$ en $p_1 = e_1$. De elementen van G zijn rotaties die \mathcal{P}_1 in \mathcal{P}_1 en bovendien \mathcal{P}_3 in \mathcal{P}_3 overvoeren. Zulke rotaties vormen de groep \mathcal{D}_k . Omdat de ordes gelijk zijn moet $G = \mathcal{D}_k$ zijn.

De baan \mathcal{P}_2 van p_2 tenslotte bestaat uit de k middens van de ribben van de regelmatige k -hoek. Deze vormen eveneens een regelmatige k -hoek.

Voorbeeld 5.14. Geval $n_1 = n_2 = n$.

In dit geval bestaat \mathcal{P}_1 uit $n/n_1 = 1$ punt, namelijk p_1 . Evenzo bestaat \mathcal{P}_2 uit alleen het punt p_2 . We moeten dus lichtelijk anders te werk gaan dan

in de voorgaande gevallen. Merk op dat G samenvalt met F_1 (en met F_2) en dus cyclisch is.

Bekijk een punt q dat geen pool is en dus ongelijk is aan p_1 of p_2 . Dan is de baan B van dat punt een regelmatige n -hoek, waarvan de punten even ver van p_2 liggen.

Alle elementen van G zijn nu rotaties die p_1 in p_1 overvoeren, bovendien p_2 in p_2 overvoeren, en tenslotte B in B overvoeren. Het kan dus niet zo zijn dat p_1 en p_2 onafhankelijk zijn. We mogen dus wel aannemen dat $p_1 = e_3$, $p_2 = -e_3$ en dat $e_1 \in B$. De rotaties die aan deze drie eisen voldoen vormen de groep C_n . Omdat de ordes gelijk zijn moet nu $G = C_n$ zijn.

In het voorgaande hebben we de eindige ondergroepen van $SO(2)$ en $SO(3)$ bepaald. We gaan nu de resterende eindige ondergroepen van $O(2)$ en $O(3)$ bepalen.

Stelling 5.15. *Zij G een eindige ondergroep van $O(2)$, maar niet van $SO(2)$. Dan is er een $v \in O(2)$ zodat $G = v D_n v^{-1}$ voor zekere n .*

Bewijs. Kies $s \in G$ met $s \notin SO(2)$. Dan is $st \in SO(2)$, dus is er $\theta \in \mathbf{R}$ met $st = r(\theta)$ en dus

$$s = r(\theta)t = r(\theta/2)^2t = r(\theta/2)tr(-\theta/2)$$

Merk op dat uit $t^2 = e$ volgt dat $s^2 = e$. We bewijzen nu dat $v = r(\theta/2)$ de gewenste eigenschap heeft.

Volgens Stelling 5.1 is $G \cap SO(2) = C_n$ voor zekere n . Als $a \in G$ en $\det(a) = -1$ dan is $sa \in G$ en $\det(sa) = \det(s)\det(a) = (-1)(-1) = 1$ en dus is $sa \in C_n$. Dat betekent dat sa van de vorm r_n^j is voor zekere j . Nu is

$$\begin{aligned} G &= C_n \cup (G - C_n) \\ &= \{r^j; j = 1, 2, \dots, n\} \cup \{vtr^{-1}r^j; j = 1, 2, \dots, n\} \\ &= v D_n v^{-1} \end{aligned}$$

immers $D_n = \{r^j; j = 1, 2, \dots, n\} \cup \{tr^j; j = 1, 2, \dots, n\}$ en $vr = rv$. •

Propositie 5.16. *Zij G een eindige ondergroep van $O(3)$ die niet binnen $SO(3)$ ligt. Dan is zijn er twee mogelijkheden:*

- $G = G(B)$ voor zekere $B < SO(3)$
- $G = G(A, B)$ voor zekere $B < A < SO(3)$ met $[A : B] = 2$.

Bewijs. We definiëren $B = G \cap \text{SO}(3)$ en $A = B \cup \{Pg; g \in G - B\}$. Dan is B in ieder geval een eindige ondergroep van $\text{SO}(3)$.

Het product van twee elementen van $G - B$ is in G en heeft determinant $(-1)(-1) = 1$, dus ligt in B . Omdat P commuteert met alle elementen van $\text{O}(3)$ volgt nu gemakkelijk dat ook A gesloten is onder vermenigvuldigen. Verder heeft elk element van A determinant 1. In feite is dus ook A een eindige ondergroep van $\text{SO}(3)$. Kijk nu naar de vereniging in de definitie van A ; er zijn twee mogelijkheden:

- Als $P \in G$ dan zijn beide delen van de vereniging hetzelfde en is $A = B$.
Nu is $G = B \cup (G - B) = B \cup \{Pb; b \in B\} = G(B)$.
- Als $P \notin G$ dan zijn beide delen van de vereniging disjunct en is de orde van A twee keer de orde van B . In dit geval is $G = B \cup (G - B) = B \cup \{Pa; a \in A - B\} = G(A, B)$.

•

Door alle mogelijkheden voor een eindige ondergroep van $\text{SO}(3)$ na te lopen, en voor elk daarvan alle mogelijkheden voor een ondergroep van index 2 na te lopen vinden we tenslotte alle eindige ondergroepen van $\text{O}(3)$.

6 Normaaldelers en factorgroepen

Veronderstel dat G een groep en H een ondergroep van G is. Indien G abels is dan is iedere linkernevenklasse in G naar H tevens rechternevenklasse naar H en omgekeerd, immers

$$aH = \{ah; h \in H\} = \{ha; h \in H\} = Ha$$

Echter indien G niet abels is behoeft dit niet langer zo te zijn.

Voorbeeld 6.1. Zij G de diëdergroep D_n van orde $2n$ met voortbrengers r en t als in Voorbeeld 2.2. Nemen we voor $H = \langle t \rangle = \{e, t\}$ dan is $rH = \{r, rt\}$ en $Hr = \{r, tr\}$. Deze twee vallen alleen samen als $rt = tr$, dus als $r = trt^{-1} = r^{-1}$, wat niet het geval is voor $n \geq 3$.

Definitie 6.2. Een ondergroep N van G heet een *normaal* $aN = Na$ voor alle $a \in G$. Een normale ondergroep noemt men ook wel *normaaldeler*. We noteren $N \triangleleft G$.

Een ondergroep N is dus normaaldeler d.e.s.d. als $ana^{-1} \in N$ voor elke $a \in G$ en $n \in N$.

De ondergroepen $\{e\}$ en G van G zijn normaaldelers. Ook is iedere ondergroep van een abelse groep een normaaldeler. Verder geldt:

Propositie 6.3. *Als $H < G$ van index 2 dan is $H \triangleleft G$.*

Bewijs. Voor elke $a \in G - H$ geldt $aH = G - H = Ha$. •

Voorbeeld 6.4. Zo is

- C_n normaal in D_n , en ook
- \mathcal{T} normaal in \mathcal{O} , en
- evenzo $SO(n)$ normaal in $O(n)$.

Zie ook Voorbeeld 6.19.

Stelling 6.5. *Als $N < G$ normaal is dan definieert de formule*

$$M(aN, bN) = (ab)N \text{ voor } a, b \in G$$

een structuur van groep op de verzameling G/N . Deze groep G/N heet de factorgroep van G naar N . Verder is de afbeelding $\pi: G \rightarrow G/N$ gedefinieerd door $\pi(x) = xN$ een surjectief homomorfisme.

Als echter $N < G$ niet normaal is dan definieert bovenstaande formule voor M geen afbeelding.

Bewijs. Als de formule een afbeelding $M: (G/N) \times (G/N) \rightarrow (G/N)$ definieert dan moeten we zeker hebben

$$(ana^{-1})N = M(anN, a^{-1}N) = M(aN, a^{-1}N) = (aa^{-1})N = eN$$

en dus $ana^{-1} \in N$ voor $a \in G, n \in N$. Dit betekent dat N normaal is.

Veronderstel nu dat N een normale ondergroep van G is. Als $a_1N = a_2N$ en $b_1N = b_2N$ dan zijn $m, n \in N$ met $a_2 = a_1m$ en $b_2 = b_1n$. Verder is $k = b_1^{-1}nb_1 \in N$ omdat N normaal is. Nu is $a_2b_2 = a_1mb_1n = (a_1b_1)kn$ met $kn \in N$, en dus is $(a_2b_2)N = (a_1b_1)N$. Dit betekent dat de afbeelding M wel-gedefinieerd is.

Verder geldt voor $a, b, c \in G$

$$\begin{aligned} M(M(aN, bN), cN) &= M((ab)N, cN) = ((ab)c)N = (a(bc))N \\ &= M(aN, (bc)N) = M(aN, M(bN, cN)) \\ M(eN, aN) &= (ea)N = aN = (ae)N = M(aN, eN) \\ M(aN, a^{-1}N) &= (aa^{-1})N = eN = (a^{-1}a)N = M(a^{-1}N, aN) \end{aligned}$$

Dus eN is het neutrale element, en $a^{-1}N$ is de inverse van aN . •

Voorbeeld 6.6. Zij H ondergroep van de optelgroep \mathbf{Z} van de gehele getallen, en stel dat $H \neq \{0\}$. Dan bevat H een $n \in \mathbf{Z}$ met $n \neq 0$. Door n eventueel te vervangen door $-n$ zien we dat H een positief geheel getal bevat. Omdat \mathbf{N}^* wel-geordend is bevat de niet-lege deelverzameling $H \cap \mathbf{N}^*$ een kleinste element m .

Is $n \in H$ dan schrijven we $n = qm + r$ met $q, r \in \mathbf{Z}$ en $0 \leq r < m$. Echter $r = n - qm \in H$ en dus $r = 0$ vanwege de keuze van m . Dit bewijst dat H gelijk is aan $\{mq; q \in \mathbf{Z}\}$, wat we als $m\mathbf{Z}$ noteren.

We hebben bewezen dat elke niet-triviale ondergroep H van \mathbf{Z} van de vorm $m\mathbf{Z}$ is voor zekere $m \in \mathbf{N}^*$. Omdat \mathbf{Z} abels is, is H gegarandeerd normaal en kunnen we de factorgroep $\mathbf{Z}/m\mathbf{Z}$ vormen. Deze factorgroep is cyclisch met als voortbrenger de nevenklasse $1 + m\mathbf{Z}$ van $1 \in \mathbf{Z}$. Er is een isomorfisme $\phi: \mathbf{Z}/m\mathbf{Z} \rightarrow C_m$ dat gegeven wordt door $\phi(k + m\mathbf{Z}) = r_m^k$.

Voorbeeld 6.7. Het element $[a, b] := aba^{-1}b^{-1} \in G$ heet de *commutator* van $a, b \in G$. De ondergroep van G voortgebracht door alle commutatoren heet de *commutator ondergroep* van G , en wordt genoteerd met $[G, G]$. Voor $a, b, c \in G$ geldt $a[b, c]a^{-1} = [aba^{-1}, aca^{-1}]$ waaruit gemakkelijk is af te leiden dat $[G, G] \triangleleft G$.

Opmerking 6.8. De factorgroep $G_{ab} = G/[G, G]$ is abels. Als immers α en β de nevenklassen zijn van $a \in G$ respectievelijk $b \in G$, dan is $\alpha\beta\alpha^{-1}\beta^{-1}$ de nevenklasse van $[a, b]$ en dus het triviale element van G_{ab} .

Stel nu dat ϕ een homomorfisme is van G naar een abelse groep A . Dan geldt $\phi([a, b]) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} = 1$. We kunnen dan een afbeelding

$\psi: G_{ab} \rightarrow A$ definiëren door de formule $\psi(x[G, G]) = \phi(x)$, en men ziet gemakkelijk dat ψ een homomorfisme is. In het bijzonder geldt dit als A een factorgroep van G is. In zekere zin is G_{ab} dus de grootste abelse factorgroep van G .

Voorbeeld 6.9. Om rechtstreeks de commutatorondergroep te bepalen kan wat bewerkelijk zijn: je moet eerst een tabel maken van alle waarden van $[a, b]$ en vervolgens onderzoeken welke elementen je daaruit door herhaald vermenigvuldigen kunt krijgen. Als je al een idee hebt wat er uit komt kan het soms wat sneller. We bepalen de commutatorgroep van \mathcal{T} .

Het is direct te zien dat de eerste rij matrices in Voorbeeld 2.8 een ondergroep V vormt; we beweren dat dit de commutatorgroep is. Uit de berekening

$$\left[\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \kappa & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \kappa\lambda \end{pmatrix} \right] = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \kappa\lambda & 0 \\ 0 & 0 & \kappa \end{pmatrix}$$

voor $\kappa, \lambda \in \{+1, -1\}$ blijkt dat deze vier matrices commutatoren zijn en dus zeker in de commutatorondergroep zitten.

We bewijzen nu de omgekeerde inclusie. We kunnen een afbeelding $\phi: \mathcal{T} \rightarrow C_3$ definiëren door de matrices in de eerste rij naar 1, die in de tweede rij naar r , en die in de derde rij naar r^2 af te beelden. Het is gemakkelijk na te rekenen dat ϕ een homomorfisme is. Omdat C_3 abels is worden alle commutatoren door ϕ naar 1 afgebeeld. Dus de commutatorgroep is bevat in de kern van ϕ namelijk V .

Voorbeeld 6.10. We bewijzen evenzo dat de commutatorondergroep van \mathcal{O} precies \mathcal{T} is. De ene kant op volgt door berekeningen zoals

$$\left[\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \kappa & 0 \\ \lambda & 0 & 0 \\ 0 & 0 & -\kappa\lambda \end{pmatrix} \right] = \begin{pmatrix} 0 & 0 & \lambda \\ -\kappa & 0 & 0 \\ 0 & -\kappa\lambda & 0 \end{pmatrix}$$

De andere kant op volgt uit het bestaan van een homomorfisme $\phi: \mathcal{O} \rightarrow C_2$ dat \mathcal{T} naar 1 en de rest naar f afbeeldt.

Propositie 6.11. *Stel $\phi: G \rightarrow H$ een homomorfisme van groepen. Dan is $\text{Ker}(\phi) = \{a \in G; \phi(a) = e\}$ een normaaldeeler van G .*

Bewijs. Voor $a, b \in \text{Ker}(\phi)$ geldt: $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = ee = e$, en dus $\text{Ker}(\phi) < G$. Voor $a \in G, b \in \text{Ker}(\phi)$ geldt: $\phi(aba^{-1}) = \phi(a)\phi(b)\phi(a)^{-1} = \phi(a)\phi(a)^{-1} = e$, en dus $\text{Ker}(\phi) \triangleleft G$. •

De volgende Stelling is misschien wel de belangrijkste stelling uit dit vak:

Stelling 6.12. *(Homomorfiestelling) Is $\phi: G \rightarrow H$ een homomorfisme van groepen dan geldt $G/\text{Ker}(\phi) \cong \text{Im}(\phi)$.*

Bewijs. Voor $a, b \in G$ geldt:

$$\begin{aligned}\phi(a) = \phi(b) &\iff \phi(b)^{-1}\phi(a) = e \iff \\ b^{-1}a \in \text{Ker}(\phi) &\iff a \in b\text{Ker}(\phi) \iff \\ a\text{Ker}(\phi) = b\text{Ker}(\phi).\end{aligned}$$

De conclusie is dat de afbeelding $\bar{\phi}: G/\text{Ker}(\phi) \rightarrow \text{Im}(\phi)$ gegeven door $\bar{\phi}(a\text{Ker}(\phi)) = \phi(a)$ welgedefinieerd en bijectief is. Voor alle $a, b \in G$ geldt

$$\begin{aligned}\bar{\phi}(a\text{Ker}(\phi)b\text{Ker}(\phi)) &= \bar{\phi}(ab\text{Ker}(\phi)) = \phi(ab) = \\ \phi(a)\phi(b) &= \bar{\phi}(a\text{Ker}(\phi))\bar{\phi}(b\text{Ker}(\phi)).\end{aligned}$$

Dus is $\bar{\phi}: G/\text{Ker}(\phi) \rightarrow \text{Im}(\phi)$ een isomorfisme. •

Voorbeeld 6.13. Voor \mathbf{F} een lichaam is de determinant $\det: \text{GL}(n, \mathbf{F}) \rightarrow \mathbf{F}^*$ een surjectief homomorfisme met kern $\text{SL}(n, \mathbf{F})$. Vanwege de homomorfiestelling volgt $\text{GL}(n, \mathbf{F})/\text{SL}(n, \mathbf{F}) \cong \mathbf{F}^*$.

Voorbeeld 6.14. De standaard diëdergroep D_n werkt op \mathbf{R}^2 en voert de hoekpunten-verzameling $X = \{p_1, p_2, \dots, p_n\}$ in zichzelf over. Als we die werking beperken tot X dan vinden we een homomorfisme $\phi: D_n \rightarrow \text{Sym}(X)$. Identificeren we de hoekpunten met hun nummers dan is dit te zien als een homomorfisme $\phi: D_n \rightarrow S_n$ dat voor de voortbrengers r, t van D_n de vorm heeft:

$$\begin{aligned}\phi(r) &= \begin{pmatrix} 1 & 2 & \dots & i & \dots & n-1 & n \\ 2 & 3 & \dots & i+1 & \dots & n & 1 \end{pmatrix} \\ \phi(t) &= \begin{pmatrix} 1 & 2 & \dots & i & \dots & n-1 & n \\ n-1 & n-2 & \dots & n-i & \dots & 1 & n \end{pmatrix}\end{aligned}$$

Voor $n \geq 3$ is $\phi: D_n \hookrightarrow S_n$ injectief en voor $n = 3$ krijgen we $D_3 \cong S_3$.

Definitie 6.15. We voeren nu een aantal gerelateerde begrippen in:

- Een isomorfisme van een groep G op zichzelf heet een *automorfisme* van G , en de collectie van alle automorfismen van G noteren we met $\text{Aut}(G)$. Men gaat eenvoudig na dat $\text{Aut}(G) < \text{Sym}(G)$.
- Voor $a \in G$ heet de afbeelding $c_a: G \rightarrow G$ gedefinieerd door $c_a(b) = aba^{-1}$ *conjugeren* met a . Aangezien $c_a(bc) = c_a(b)c_a(c)$ voor alle $a, b, c \in G$ is $c_a: G \rightarrow G$ een homomorfisme. Voorts is $c_a: G \rightarrow G$ bijectief want $c_{a^{-1}}$ is de inverse van c_a . Dus c_a is een automorfisme van G . Een automorfisme van G van de vorm c_a heet *inwendig*, en de collectie van alle inwendige automorfismen van G noteren we met $\text{Int}(G)$.

- Verder volgt uit $c_a c_b = c_{ab}$ voor alle $a, b \in G$ dat de afbeelding $G \rightarrow \text{Aut}(G)$ gegeven door $a \mapsto c_a$ een homomorfisme is met als beeld $\text{Int}(G) < \text{Aut}(G)$ en als kern

$$Z(G) = \{a \in G ; ab = ba \text{ voor alle } b \in G\} \triangleleft G,$$

het *centrum* van G . Vanwege de homomorfiestelling geldt

$$G/Z(G) \cong \text{Int}(G).$$

- In feite is de ondergroep $\text{Int}(G)$ van $\text{Aut}(G)$ zelfs normaal, immers als $\phi \in \text{Aut}(G)$ dan is $\phi \circ c_a \circ \phi^{-1} = c_{\phi(a)}$ zoals blijkt uit de volgende berekening:

$$\begin{aligned} (\phi \circ c_a \circ \phi^{-1})(b) &= \phi(c_a(\phi^{-1}(b))) = \phi(a\phi^{-1}(b)a^{-1}) \\ &= \phi(a)\phi(\phi^{-1}(b))\phi(a)^{-1} = \phi(a)b\phi(a)^{-1} = c_{\phi(a)}(b) \end{aligned}$$

De factorgroep $\text{Aut}(G)/\text{Int}(G)$ noteert men $\text{Out}(G)$.

Op de jacht naar normale ondergroepen is het volgende begrip soms nuttig:

Definitie 6.16. Een ondergroep K van een groep G heet *karakteristiek* als $\phi(K) = K$ voor elke $\phi \in \text{Aut}(G)$.

Dit is een sterkere eis dan normaal zijn, want dan eist men $\phi(K) = K$ alleen voor $\phi \in \text{Int}(G)$.

Voorbeeld 6.17. De commutatorgroep $[G, G]$ en het centrum $Z(G)$ zijn karakteristieke ondergroepen van G . Dat ligt daaraan dat voor een element van G het lidmaatschap van $Z(G)$ of van $[G, G]$ helemaal wordt uitgedrukt in de vermenigvuldiging van G , en die blijft bewaard onder een automorfisme. Een andere karakteristieke ondergroep van G is bijvoorbeeld de ondergroep voortgebracht door alle derde machten.

Merk trouwens op dat de *verzameling* van derde machten zelf niet noodzakelijk een ondergroep vormt. Dit blijkt uit het voorbeeld van $\mathcal{T}_h \cong S_4$, immers daar zijn 16 van de 24 elementen derde machten.

Het nut van dit begrip blijkt uit:

Propositie 6.18. *Als N normaal is in G , en K karakteristiek is in N , dan is K normaal in G .*

Bewijs. Zij $a \in G$. Dan voert c_a de ondergroep N in zichzelf over. Dus de beperking ϕ van c_a tot N is een automorfisme van N . Maar dan voert ϕ de ondergroep K in zichzelf over, dat wil zeggen $c_a(K) = K$. •

Dat het niet voldoende is als K slechts normaal is in N blijkt uit het volgende voorbeeld:

Voorbeeld 6.19. De groep \mathcal{D}_2 bestaat uit e en de drie elementen a, b, c van \mathcal{T} die van orde 2 zijn. Daaruit blijkt dat \mathcal{D}_2 karakteristiek is in \mathcal{T} en dus zeker normaal.

De groep \mathcal{D}_2 is abels: in feite is de vermenigvuldigingstabel de rechters-tabel uit Voorbeeld 3.2. Dat impliceert dat \mathcal{C}_2 een normale ondergroep is van \mathcal{D}_2 . Echter \mathcal{C}_2 is niet normaal in \mathcal{T} zoals men gemakkelijk narekent.

Definitie 6.20. We noemen een groep G het (inwendige) *directe product* van zijn ondergroepen A en B als aan de volgende eisen voldaan is:

1. $A \cap B = \{e\}$.
2. De verzameling $AB = \{ab; a \in A, b \in B\}$ is heel G .
3. A en B zijn allebei normale ondergroepen van G .

Opmerking 6.21. De eerste eis betekent precies dat elk element van G op hoogstens één manier te schrijven is als ab met $a \in A$ en $b \in B$. Immers als $a_1b_1 = a_2b_2$ met $a_1, a_2 \in A$ en $b_1b_2 \in B$ dan is $a_1a_2^{-1} = b_2b_1^{-1} \in A \cap B = \{e\}$.

De tweede eis betekent precies dat elke element op minstens één manier zo te schrijven is. De eerste twee eisen tesamen zeggen dus dat elk element van G op precies één manier zo te schrijven is.

Opmerking 6.22. Als aan de eerste eis voldaan is dan zijn alle ab met $a \in A$ en $b \in B$ verschillend. In dat geval is $\#(AB) = \#(A) \cdot \#(B)$.

Dus als G eindig is dan is aan de tweede eis al voldaan zodra $\#(G) = \#(A) \cdot \#(B)$.

Opmerking 6.23. Als aan de eerste twee eisen voldaan is dan is de derde eis equivalent met

$$ab = ba \text{ voor alle } a \in A, b \in B$$

Stel namelijk dat A en B normaal zijn en beschouw de commutator $aba^{-1}b^{-1}$ met $a \in A$ en $b \in B$. Enerzijds is dat het product van $a \in A$ en $(bab^{-1})^{-1} \in A$ en dus in A . Anderzijds is dat het product van $aba^{-1} \in B$ en $b^{-1} \in B$ en dus in B . Dus in feite ligt die commutator in $A \cap B$ en is dus e , wat betekent dat $ab = ba$.

Stel nu dat $ab = ba$ voor alle $a \in A$ en $b \in B$. Om te laten zien dat A normaal is in G moeten we controleren dat $xyx^{-1} \in A$ als $y \in A$ en $x \in G$. Vanwege de tweede eis is x te schrijven als $y = ab$ met $a \in A$ en $b \in B$. We krijgen dus $xyx^{-1} = abyb^{-1}a^{-1} = aya^{-1} \in A$. Evenzo is B normaal in G .

Voorbeeld 6.24. Als n oneven is dan is $G = O(n)$ het direct product van $A = SO(n)$ en $B = \{I, P\}$.

Voorbeeld 6.25. De in Voorbeeld geconstrueerde $G(A)$ is het direct product van A en $\{I, P\}$. Zo is bijvoorbeeld \mathcal{T}_h het direct product van \mathcal{T} en $\{I, P\}$.

Voorbeeld 6.26. Neem aan dat $k, m \in \mathbf{N}^*$ relatief priem zijn. Dan is $G = C_{km}$ het direct product van C_k en C_m . Dat aan de normaliteits-eis en de cardinaliteits-eis voldaan is is duidelijk. De doorsnede-eis ook want

$$\begin{aligned} C_m \cap C_k &= \{r_m^a; a = 0, 1, \dots, m-1\} \cap \{r_k^b; b = 0, 1, \dots, k-1\} \\ &= \{r_{mk}^{ak}; a = 0, 1, \dots, m-1\} \cap \{r_{mk}^{bk}; b = 0, 1, \dots, k-1\} = \{e\} \end{aligned}$$

want een getal dat een veelvoud van k en van m is is een veelvoud van km .

Voorbeeld 6.27. De groep $\mathcal{D}_2 = \{e, a, b, c\}$ is direct product van $\{e, a\}$ en $\{e, b\}$. Hij is bijvoorbeeld ook direct product van $\{e, a\}$ en $\{e, c\}$.

Voorbeeld 6.28. Zij $k, m \in \mathbf{N}$ en zij $n = k + m$. Beschouw $n \times n$ matrices $X = (x_{ij})$ met de eigenschap

$$x_{ij} = 0 \text{ als } i > k, j \leq k \text{ of } i \leq k, j > k$$

Een dergelijke matrix wordt geheel vastgelegd door de $k \times k$ matrix $Y = (y_{rs})$ en de $m \times m$ matrix $Z = (z_{uv})$ waar $y_{rs} = x_{rs}$ en $z_{uv} = x_{k+u, k+v}$. Schematisch:

$$X = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{pmatrix} = \begin{pmatrix} y_{11} & \dots & y_{1k} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ y_{k1} & \dots & y_{kk} & 0 & \dots & 0 \\ 0 & & 0 & z_{11} & \dots & z_{1m} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & z_{m1} & \dots & z_{mm} \end{pmatrix} = \begin{pmatrix} Y & 0 \\ 0 & Z \end{pmatrix}$$

We zeggen dat de matrix X een (k, m) blokvorm heeft met blokken Y en Z .

Stel dat een X als boven inverteerbaar is. Door uit te schrijven wat het betekent dat een $n \times n$ matrix W een inverse is van X blijkt;

- De $k \times k$ matrix Y is inverteerbaar met als inverse het $k \times k$ linkerboven-deel van W
- De $m \times m$ matrix Z is inverteerbaar met als inverse het $m \times m$ rechterbeneden-deel van W

Omgekeerd is duidelijk: als Y en Z inverteerbaar is dan is X het ook en zijn inverse heeft een (k, m) blokvorm met blokken Y^{-1} en Z^{-1} .

Het is nu duidelijk dat de verzameling G van alle inverteerbare matrices in (k, m) blokvorm een ondergroep vormt van de groep $\mathrm{GL}(n, \mathbf{R})$ van alle $n \times n$ inverteerbare matrices. Schrijf nu

$$A = \left\{ \begin{pmatrix} Y & 0 \\ 0 & I_m \end{pmatrix}; Y \in \mathrm{GL}(k, \mathbf{R}) \right\}$$

$$B = \left\{ \begin{pmatrix} I_k & 0 \\ 0 & Z \end{pmatrix}; Z \in \mathrm{GL}(m, \mathbf{R}) \right\}$$

Dan zijn A en B ondergroepen van G , en G is het directe product van A en B . Dit volgt uit de berekening

$$\begin{pmatrix} Y & 0 \\ 0 & Z \end{pmatrix} = \begin{pmatrix} Y & 0 \\ 0 & I_m \end{pmatrix} \begin{pmatrix} I_k & 0 \\ 0 & Z \end{pmatrix} = \begin{pmatrix} I_k & 0 \\ 0 & Z \end{pmatrix} \begin{pmatrix} Y & 0 \\ 0 & I_m \end{pmatrix}$$

Bovendien is A isomorf met $\mathrm{GL}(k, \mathbf{R})$, en is B isomorf met $\mathrm{GL}(m, \mathbf{R})$.

Voorbeeld 6.29. Zij $p = (1, \tau, 0) \in X_{ico}$. Dan is er voor elke $g \in \mathcal{I}$ een unieke $h \in \mathcal{T}$ zo dat $h(p) = g(p)$; zie Voorbeeld 4.23. Dit betekent dat $h^{-1}g \in \mathrm{Stab}_{\mathcal{I}}(p) = \langle T_{5,p} \rangle$. De ondergroepen \mathcal{T} en $\langle T_{5,p} \rangle$ van \mathcal{I} voldoen dus wel aan eisen 1 en 2 van Definitie 6.20 maar allerminst aan de derde: beide ondergroepen zijn niet normaal.

Opmerking 6.30. Zij nu gegeven twee abstracte groepen A en B . Dan kunnen we een abstracte groep G fabriceren die een direct product is van ondergroepen A^* en B^* , en wel zó dat A^* isomorf is met A en B^* isomorf is met B .

Als verzameling is G de verzameling van paren (a, b) met $a \in A$ en $b \in B$. De vermenigvuldiging M op G wordt gegeven door

$$M((a, b), (u, v)) = (M_A(a, u), M_B(b, v))$$

waar M_A de vermenigvuldiging in A is, en M_B de vermenigvuldiging in B . Ga zelf na dat dit inderdaad een groep oplevert.

De verzameling A^* bestaat uit alle paren $(a, 1_B)$ waar $a \in A$ en waar 1_B heet neutrale element van B is. Ga zelf na dat A^* een ondergroep van G is en dat de afbeelding $a \mapsto (a, 1_B)$ een isomorfisme $A \rightarrow A^*$ is. Evenzo bestaat B^* uit alle paren $(1_A, b)$ waar $b \in B$ en waar 1_A het neutrale element van A is. Dan is B^* een ondergroep van G die isomorf is met B . Ga tenslotte na dat G het directe product is van A^* en B^* .

Definitie 6.31. Bovenstaande constructie heet het *uitwendige directe product* van A en B , en wordt genoteerd als $A \times B$.

Opmerking 6.32. Als een groep G het inwendige directe product is van ondergroepen A en B dan kunnen we het uitwendige directe product $A \times B$ vormen, en er is een isomorfisme $\phi: A \times B \rightarrow G$ dat gegeven wordt door $\phi(a, b) = ab = ba$.

Omgekeerd: als gegeven zijn groepen A , B en G en een isomorfisme $\phi: A \times B \rightarrow G$ dan is G het inwendige directe product van $\phi(A^*)$ en $\phi(B^*)$.

Voorbeeld 6.33. In Voorbeeld 2.13 wordt voor diverse A een groep $G(A)$ geconstrueerd als het directe product van A en $\{1, P\}$. Dus is $G(A)$ isomorf met $A \times \{1, P\}$. Zo is bijvoorbeeld $\mathcal{O}_h = G(\mathcal{O})$ isomorf met $\mathcal{O} \times \{1, P\}$. Omdat bovendien \mathcal{O} isomorf is met S_4 (Zie Hoofdstuk 8) en $\{1, P\}$ met de cyclische groep C_2 mogen we concluderen dat \mathcal{O}_h isomorf is met $S_4 \times C_2$. Hieronder volgt in tabelvorm een dergelijk eenvoudig model voor elk van de eindige ondergroepen van $O(3)$. Hierbij is gebruik gemaakt van de isomorfismen $G(A, B) \cong A$ (Zie Voorbeeld 3.20) en $\mathcal{C}_n \cong C_n$, $\mathcal{D}_n \cong D_n$. Voor de groepen S_4 , A_4 en A_5 zie het einde van Hoofdstuk 8.

Naam	Geval	Constructie	Directe factoren	Isomorf model
\mathcal{C}_n	elke n	-	-	C_n
\mathcal{D}_n	elke n	-	-	D_n
\mathcal{T}	-	-	-	A_4
\mathcal{O}	-	-	-	S_4
\mathcal{I}	-	-	-	A_5
\mathcal{C}_{nh}	n even	$G(\mathcal{C}_n)$	\mathcal{C}_n en $\{1, P\}$	$C_n \times C_2$
\mathcal{C}_{nh}	n oneven	$G(\mathcal{C}_{2n}, \mathcal{C}_n)$	-	C_{2n}
\mathcal{S}_{2n}	n even	$G(\mathcal{C}_{2n}, \mathcal{C}_n)$	-	C_{2n}
\mathcal{S}_{2n}	n oneven	$G(\mathcal{C}_n)$	\mathcal{C}_n en $\{1, P\}$	$C_n \times C_2$
\mathcal{D}_{nh}	n even	$G(\mathcal{D}_n)$	\mathcal{D}_n en $\{1, P\}$	$D_n \times C_2$
\mathcal{D}_{nh}	n oneven	$G(\mathcal{D}_{2n}, \mathcal{D}_n)$	-	D_{2n}
\mathcal{D}_{nd}	n even	$G(\mathcal{D}_{2n}, \mathcal{D}_n)$	-	D_{2n}
\mathcal{D}_{nd}	n oneven	$G(\mathcal{D}_n)$	\mathcal{D}_n en $\{1, P\}$	$D_n \times C_2$
\mathcal{C}_{nv}	elke n	$G(\mathcal{D}_n, \mathcal{C}_n)$	-	D_n
\mathcal{T}_h	-	$G(\mathcal{T})$	\mathcal{T} en $\{1, P\}$	$A_4 \times C_2$
\mathcal{O}_h	-	$G(\mathcal{O})$	\mathcal{O} en $\{1, P\}$	$S_4 \times C_2$
\mathcal{I}_h	-	$G(\mathcal{I})$	\mathcal{I} en $\{1, P\}$	$A_5 \times C_2$
\mathcal{T}_d	-	$G(\mathcal{O}, \mathcal{T})$	-	S_4

7 Sylow theorie.

De inhoud van dit Hoofdstuk maakt geen deel uit van de tentamenstof. Het is ter informatie en illustratie.

Lemma 7.1. *Zij G een abelse groep van orde n . en zij p een priemgetal dat n deelt. Dan bevat G een element van orde p .*

Bewijs. We gebruiken volledige inductie naar n/p . Als $n = p$ dan is er niets te bewijzen. We mogen dus aannemen dat het Lemma waar is voor alle kleinere waarden van n/p .

Kies $a \in G$ met $a \neq e$. Als de door a voortgebrachte ondergroep C heel G is, dan is a van orde n en dan is $a^{n/p}$ een element als gewenst. Zo niet, dan is C een voorbeeld van een ondergroep H van G met $H \neq \{e\}, G$. We kunnen dan uit alle ondergroepen H van G met $H \neq \{e\}, G$ er een kiezen met maximale orde. Er zijn nu twee mogelijkheden:

- Als p de orde van H deelt dan bevat H volgens de inductie-hypothese een element van orde p , en dan bevat G datzelfde element.
- Als p de orde van H niet deelt dan kiezen we een $b \in G$, $b \notin H$. Schrijf B voor de ondergroep $\langle b \rangle$ voortgebracht door b .

De ondergroep HB van G voortgebracht door H en b moet heel G zijn, omdat er anders een tegenspraak met de definitie van H ontstaat. Beschouw nu de de formule

$$\#(G) = \#(HB) = \#(H)\#(B)/\#(H \cap B)$$

Uit deze formule blijkt dat p de orde $m = \#(B)$ van b deelt. Nu is $b^{m/p}$ een element als gewenst.

In beide gevallen hebben we een element gevonden als gewenst. •

Stelling 7.2. *Zij G een groep van orde $p^m q$, waar p een priemgetal is dat q niet deelt. Dan heeft G een ondergroep van orde p^m , een zogenaamde p -Sylow-groep.*

Bewijs. We gebruiken volledige inductie naar de orde van G . Als G orde 1 heeft dan is er niets te bewijzen. We mogen dus aannemen dat de stelling waar is voor alle groepen van lagere orde.

Merk op dat de conjugatie-klasse $C(a)$ van een $a \in G$ cardinaliteit 1 heeft alleen als a in het centrum $Z(G)$ zit. Schrijf G als disjuncte vereniging $Z(G) \cup \bigcup_{i=1}^k C(a_i)$ voor zekere $a_i \in G$. Dan is er voor elke i een bijectie $C(a_i) \cong G/Z(a_i)$, waar $Z(a_i)$ de centralisator van a_i is. Nu zijn er twee mogelijkheden

- *Er is een j waarvoor de cardinaliteit van $C(a_j)$ geen p -voud is.*
In dat geval deelt p^m de orde van $Z(a_j)$. Deze orde kleiner dan die van G , want $\#(Z(a_j)) = \#(G)/\#(C(a_j))$, en $\#(C(a_j)) > 1$. Bij inductie-hypothese heeft $Z(a_j)$ dus een ondergroep S van orde p^m . Nu is S een ondergroep van G van orde p^m .
- *Voor alle i is de cardinaliteit van $C(a_i)$ een p -voud.*
Omdat $\#(Z(G)) = \#(G) - \sum_{i=1}^k \#(C(a_i))$ moet de orde van $Z(G)$ ook een p -voud zijn. Volgens het Lemma bevat de abelse groep $Z(G)$ dan een element y van orde p . Schrijf Y voor de daardoor voortgebrachte cyclische ondergroep $\langle y \rangle$ van orde p .
Omdat G/Y orde $p^{m-1}q$ heeft zegt de inductie-hypothese nu dat G/Y een ondergroep T van orde p^{m-1} heeft. Het origineel $\pi^{-1}(T)$ onder de klasse-vormende afbeelding $\pi: G \rightarrow G/Y$ is nu een ondergroep van orde p^m .

In beide gevallen hebben we een ondergroep als gewenst. •

Opmerking 7.3. Hetzelfde bewijs laat zien dat als de orde van G gelijk is aan p^m , het centrum $Z(G)$ niet-triviaal is.

Ga zelf na dat hieruit volgt dat een groep van orde p^2 (met p priem) noodzakelijk abels is.

Opmerking 7.4. Stel dat een priem p de orde van een groep G deelt. Dan heeft G een p -Sylow-groep S . Deze S heeft een centrum Z waarvan de orde een positieve p -macht is. En Z bevat weer een element van orde p . Dus bevat G dan een element van orde p .

Stelling 7.5. *Als A en B twee p -Sylowgroepen van G zijn dan is er $g \in G$ met $B = gAg^{-1}$.*

Bewijs. Beschouw de linkswerking van $A \times B$ op G . gedefinieerd door

$$\lambda(a, b), g) = agb^{-1}$$

Schrijf G als disjuncte vereniging van banen:

$$G = \cup_{i=1}^k Ag_iB$$

Elementen tellen aan beide zijden levert

$$\#(G) = \sum_{i=1}^r \frac{\#(A) \cdot \#(B)}{\#(D_i)} \text{ waar } D_i = g_i^{-1}Ag_i \cap B$$

De orde van D_i is een deler van de orde van B , zeg p^{e_i} . Er staat nu

$$p^m q = \sum_{i=1}^r p^{2m-e_i} \text{ ofwel } q = \sum_{i=1}^r p^{m-e_i}$$

Aangezien het linkerlid q niet deelbaar is door p kunnen niet alle termen p^{m-e_i} van het rechterlid deelbaar zijn door p . Er moet dus een i zijn met $e_i = m$ en dus $\#(B) = \#(D_i) = \#(g_i^{-1}Ag_i)$. Dit betekent dat $B = D_i = g_i^{-1}Ag_i$. •

Opmerking 7.6. Hetzelfde bewijs laat zien dat als $\#(B) = p^b$ en $\#(A) = p^m$ er een $g \in G$ is met $B \subset gAg^{-1}$. Met andere woorden: elke ondergroep van geschikte orde is bevat in een Sylow-ondergroep.

Stelling 7.7. *Het aantal p -Sylowgroepen van een groep G van orde $p^m q$ is 1 modulo p (en deelt q).*

Bewijs. Beschouw de collectie van p -Sylowgroepen van G . Hierop werkt G door conjugatie. Volgens de vorige Stelling is er maar één baan. De isotropiegroep van p -Sylowgroep A onder deze werking is $N = \{x \in G ; xAx^{-1} = A\}$, de normalisator van A . Het aantal p -Sylowgroepen is dus $\ell = \#(G)/\#(N)$. Noteer $k = \#(G)/\#(N)$; dan is $q = k\ell$.

Als in het vorige bewijs schrijven we G als disjuncte vereniging van dubbele nevenklassen

$$G = \cup_{i=1}^r Ag_i N, \text{ met } g_1 = e$$

Als we p^{e_i} schrijven voor de orde van $D_i = g_i^{-1}Ag_i \cap N$ dan levert dit

$$p^m k \ell = \sum_{i=1}^r p^{2m-e_i} \ell \quad \text{ofwel} \quad k = \sum_{i=1}^r p^{m-e_i}$$

Stel je voor dat $p^{m-e_j} = 1$ voor zekere j . Dan is $g_j^{-1}Ag_j = D_j$ een ondergroep van N , en dus een p -Sylowgroep van N . Maar omdat A normaal is in N heeft N geen andere p -Sylowgroep dan A . Dus $g_j^{-1}Ag_j = A$ met andere woorden $g_j \in N$. Per definitie van de g_i is dit alleen toegestaan als $i = 1$.

Dus alle termen in bovenstaande som zijn p -vouden, behalve de eerste term, die 1 bedraagt. •

Voorbeeld 7.8. Zij G een groep van orde 200. Dan is het aantal 5-Sylowgroepen van G zowel 1 modulo 5 als een deler van 200, en dus noodzakelijk 1. De 5-Sylowgroep is dus normaal; dit betekent dat G een semidirect product is.

8 De symmetrische groep.

Beschouw een eindige verzameling X van cardinaliteit n . De symmetrische groep $\text{Sym}(X)$ bestaat uit alle bijecties $X \rightarrow X$, ook wel genoemd permutaties van X .

Definitie 8.1. Zij $k \geq 2$. Een permutatie $\sigma \in \text{Sym}(X)$ heet een k -cykel als de werking van de groep $\langle \sigma \rangle$ op X één baan van k elementen heeft, en verder alleen vaste punten heeft.

Propositie 8.2. De permutatie σ is een k -cykel is d.e.s.d. als er onderling verschillende elementen $x_1, x_2, \dots, x_k \in X$ bestaan met

- $\sigma(x_j) = x_{j+1}$ voor $1 \leq j \leq k-1$,
- $\sigma(x_k) = x_1$ en
- $\sigma(x) = x$ voor $x \in X - \{x_1, x_2, \dots, x_k\}$.

Men noteert gewoonlijk $\sigma = (x_1 \ x_2 \ \dots \ x_k)$.

Bewijs. Kies een element x van die niet-triviale baan, en noteer $x_m = \sigma^{m-1}(x)$ voor $m \in \mathbf{N}$.

- De elementen x_m voor $m = 1, 2, \dots, k$ zijn verschillend. Als immers $x_a = x_b$ met $1 \leq a < b \leq k$ dan is $\sigma^{b-a}(x) = x$. Elk element van de baan van x is dan van de vorm x_m met $m \leq b-a < k$. De baan van x bevat dan minder dan k elementen, in tegenspraak met de definitie van k .
- Stel dat $x_{k+1} \neq x$. Dan volgt uit een soortgelijke redenering als boven dat de x_m voor $m = 1, 2, \dots, k+1$ verschillend zijn. In dit geval bevat de baan van x meer dan k elementen, weer in tegenspraak met de betekenis van k .

De baan van x is dus $\{x_1, x_2, \dots, x_k\}$. Bij aanname laat σ alle overige punten van X vast. •

Het is duidelijk dat de orde van een k -cykel gelijk is aan k . Een 1-cykel is de identieke afbeelding. Een 2-cykel noemt men ook wel een *verwisseling* of *transpositie*.

Voorbeeld 8.3. De permutatie

$$\sigma = \begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}$$

is een 3-cykel die we kunnen schrijven als $\sigma = (a \ d \ c)$ maar ook als $(d \ c \ a)$ of $(c \ a \ d)$. Dezelfde permutatie kan blijkbaar door meerdere notaties beschreven worden, omdat er een keuze gedaan wordt van een element in de niet-triviale baan dat vooraan gezet wordt.

Als X voorzien komt van een totale ordening, en met name als $X = \{1, 2, \dots, n\}$ dan krijgen we een standaard notatie door af te spreken het kleinste element van de baan voorop te zetten.

Definitie 8.4. Twee cykels $\sigma = (x_1 \ x_2 \dots x_k)$ en $\tau = (y_1 \ y_2 \dots y_\ell)$ heten *disjunct* als $\{x_1, x_2, \dots, x_k\} \cap \{y_1, y_2, \dots, y_\ell\} = \emptyset$.

Het is duidelijk dat disjuncte cykels commuteren: hun werking is op disjuncte verzamelingen en dus is de volgorde van uitvoering irrelevant.

Voorbeeld 8.5. Zij $\sigma \in S_{10}$ gegeven door

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 4 & 3 & 8 & 9 & 7 & 10 & 2 & 1 \end{pmatrix} \in S_{10}$$

Dan is σ te schrijven als een product van disjuncte cykels:

$$\sigma = (1 \ 5 \ 8 \ 10)(2 \ 6 \ 9)(3 \ 4)(7).$$

Stelling 8.6. *Iedere permutatie van een eindige verzameling X is te schrijven als product van onderling disjuncte cykels. Deze schrijfwijze is uniek op de volgorde van de factoren na (maar 1-cykels schrijven we gewoonlijk niet op).*

Bewijs. Zij $\sigma \in \text{Sym}(X)$. Dan werkt de groep $G = \langle \sigma \rangle$ op X . Dus X is een eindige vereniging van banen Y_1, \dots, Y_q .

Zij Y_j zo'n baan, kies een representant $p_j \in Y_j$, en schrijf $x_{j,i} = \sigma^{i-1}(p_j)$. Omdat X eindig is is er een grootste k_j zodat $x_{j,1}, \dots, x_{j,k_j}$ verschillend zijn. De baan $Y_j = Gp_j$ van p_j is dan $Y_j = \{x_{j,1}, x_{j,2}, \dots, x_{j,k_j}\}$. Definieer nu $\tau_j \in \text{Sym}(X)$ door

$$\tau_j(a) = \begin{cases} \sigma(a) & \text{als } a \in Y_j \\ a & \text{als } a \notin Y_j \end{cases}$$

dan is τ_j een k_j -cykel, en wel $(x_{j,1} \ x_{j,2} \ \dots \ x_{j,k_j})$.

In het bijzonder wordt Y_ℓ door τ_j in zichzelf afgebeeld, en voor de beperking $\tau_j | Y_\ell$ geldt:

$$\tau_j | Y_\ell = \begin{cases} \sigma | Y_\ell & \text{als } \ell = j \\ 1_{Y_\ell} & \text{als } \ell \neq j \end{cases}$$

Daaruit volgt dat voor de samenstelling $\tau = \tau_1 \tau_2 \dots \tau_q$ geldt dat $\tau(a) = \sigma(a)$. Met andere woorden $\sigma = \tau$ en we hebben σ in de gewenste vorm geschreven.

Stel nu omgekeerd dat σ op een of andere manier geschreven is als product van disjuncte cykels, zeg $\sigma = \tau'_1 \tau'_2 \dots \tau'_r$. Dat betekent dat $\tau'_j = (x'_{j,1} \ x'_{j,2} \ \dots \ x'_{j,m_j})$ voor zekere m_j en voor zekere $x'_{j,i}$, en dat de verzamelingen $Y'_j = \{x'_{j,1}, x'_{j,2}, \dots, x'_{j,m_j}\}$ disjunct zijn. Als de vereniging van de

Y'_j niet heel X is dan vullen we die cykels aan met 1-cykels behorende bij de ontbrekende elementen. Uit de disjunctie volgt dat $\tau'_j(Y'_\ell) \subset Y'_\ell$ en dat geldt:

$$\tau'_j | Y'_\ell = \begin{cases} \sigma | Y'_\ell & \text{als } \ell = j \\ 1_{Y'_\ell} & \text{als } \ell \neq j \end{cases}$$

Nu is Y'_j gelijk is aan de baan van x'_{j1} onder $\langle \tau'_j \rangle$ en dus aan de baan van dat punt onder $\langle \sigma \rangle = G$. Maar de baan van een punt onder G is noodzakelijk een zekere Y_ℓ . Dus Y'_j is zekere Y_ℓ , en $m_j = k_\ell$. Omdat de totale cardinaliteit van alle Y' -tjes samen gelijk is aan de cardinaliteit van alle Y -tjes samen zijn de Y' -tjes in feite een permutatie van de Y -tjes. Verder moet x'_{j1} dan van de vorm $x_{\ell i}$ zijn voor zekere $i \leq k_\ell$, en

$$\begin{aligned} \tau'_j &= (x'_{j1} \ x'_{j2} \ \dots \ x'_{jm_j}) = (x'_{j1} \ \sigma(x'_{j1}) \ \dots \ \sigma^{m_j-1}(x'_{j1})) \\ &= (x_{\ell i} \ \sigma(x_{\ell i}) \ \dots \ \sigma^{k_\ell-1}(x_{\ell i})) = (x_{\ell i} \ x_{\ell i+1} \ \dots \ x_{\ell k_\ell} \ x_{\ell 1} \ \dots \ x_{\ell i-1}) \\ &= (x_{\ell 1} \ \dots \ x_{\ell i-1} \ x_{\ell i} \ x_{\ell i+1} \ \dots \ x_{\ell k_\ell}) = \tau_\ell \end{aligned}$$

Dus de gegeven cykels zijn precies die uit de eerste helft van het bewijs. •

Stelling 8.7. *Is $\sigma \in \text{Sym}(X)$ geschreven als product van onderling disjuncte cykels, dan is de orde van σ het kleinste gemene veelvoud van de ordes van deze cykels.*

Bewijs. Stel $\sigma = \sigma_1 \sigma_2 \dots \sigma_m$ met $\sigma_1, \sigma_2, \dots, \sigma_m$ onderling disjuncte cykels. Voor $j \in \mathbf{N}$ geldt dan $\sigma^j = \sigma_1^j \sigma_2^j \dots \sigma_m^j$ vanwege het onderling commuteren. Elke σ_i^j werkt triviaal op de punten die niet in de cykel σ_i voorkomen. Dus geldt

$$\begin{aligned} \sigma^j &= e \iff \\ \sigma_i^j &= e \text{ voor alle } i \iff \\ j &\text{ is een veelvoud van de orde van } \sigma_i \text{ voor alle } i \end{aligned}$$

De orde van σ is de kleinste $j \in \mathbf{N}$ met $\sigma^j = e$, en dus gelijk aan het kleinste gemene veelvoud van de ordes van σ_i . •

Definitie 8.8. Zij $\sigma \in \text{Sym}(X)$. met $\sigma = \sigma_1 \sigma_2 \dots \sigma_m$ het product van disjuncte cykels. Zeg σ_i is een k_i -cykel met $k_i \in \mathbf{N}$. Zorg er nu voor dat

- $k_1 \geq k_2 \geq \dots \geq k_m$. Dat kunnen we bereiken door zo nodig de volgorde van de factoren te wijzigen. en
- $\sum_1^m k_i = n$. Dat kunnen we bereiken door alle 1-cykels daadwerkelijk op te schrijven. Ze corresponderen met de vaste punten van σ .

De partitie (k_1, k_2, \dots, k_m) van het getal n heet het *cykeltype* van de permutatie σ .

Stelling 8.9. *Het cykeltype induceert een bijectie tussen de conjugatieklassen van $\text{Sym}(X)$ en de partities van het getal n .*

Bewijs. Zij $\sigma \in \text{Sym}(X)$ van cykeltype (k_1, k_2, \dots, k_m) , zeg

$$\sigma = \sigma_1 \sigma_2 \dots \sigma_m \text{ met } \sigma_j = (x_{j1} \ x_{j2} \ \dots \ x_{jk_j})$$

Zij verder $\tau \in \text{Sym}(X)$ een willekeurige permutatie. Dan is $\sigma' = \tau \sigma \tau^{-1}$ weer van cykeltype (k_1, k_2, \dots, k_m) , namelijk

$$\sigma' = \sigma'_1 \sigma'_2 \dots \sigma'_m \text{ met } \sigma'_j = \tau \sigma_j \tau^{-1} = (y_{j1} \ y_{j2} \ \dots \ y_{jk_j})$$

waarbij $y_{ji} = \tau(x_{ji})$. Inderdaad is

$$\begin{aligned} \sigma'_j(y_{ji}) &= (\tau \sigma_j \tau^{-1})(\tau(x_{ji})) = \tau(\sigma_j(x_{ji})) \\ &= \tau(x_{j,i+1}) = y_{j,i+1} \text{ voor } i < k_j \\ \sigma'_j(y_{jk_j}) &= y_{j1} \end{aligned}$$

Stel omgekeerd dat zekere σ' cykeltype (k_1, k_2, \dots, k_m) heeft, zeg

$$\sigma' = \sigma'_1 \sigma'_2 \dots \sigma'_m \text{ met } \sigma'_j = (y_{j1} \ y_{j2} \ \dots \ y_{jk_j})$$

We definiëren nu een afbeelding τ door

$$\tau(x_{ji}) = y_{ji} \text{ voor } i = 1, 2, \dots, k_j \text{ en } j = 1, 2, \dots, m$$

dan is τ een bijectie en $\sigma' = \tau \sigma \tau^{-1}$. •

Opmerking 8.10. In de tweede helft van het bewijs hebben we nog een zekere vrijheid in het kiezen van τ . Zo kunnen we τ vervangen door $\tau\gamma$ waar γ een willekeurig permutatie is die met σ commuteert. Met name mag γ de vaste punten van σ willekeurig permuteren.

Voorbeeld 8.11. We bepalen de conjugatieklassen en hun cardinaliteit voor de groep S_6 . Zij $\underline{k} = (k_1, \dots, k_m)$ een partitie van 6, dat wil zeggen $k_1 \geq k_2 \geq \dots \geq k_m \geq 1$ en $\sum_1^m k_i = 6$. We krijgen dan de volgende tabel:

m	$\underline{k} = (k_1, \dots, k_m)$	representant van de klasse	cardinaliteit van de klasse
1	(6)	(1 2 3 4 5 6)	120
2	(5, 1)	(1 2 3 4 5)	144
2	(4, 2)	(1 2 3 4)(5 6)	90
2	(3, 3)	(1 2 3)(4 5 6)	40
3	(4, 1, 1)	(1 2 3 4)	90
3	(3, 2, 1)	(1 2 3)(4 5)	120
3	(2, 2, 2)	(1 2)(3 4)(5 6)	15
4	(3, 1, 1, 1)	(1 2 3)	40
4	(2, 2, 1, 1)	(1 2)(3 4)	45
5	(2, 1, 1, 1, 1)	(1 2)	15
6	(1, 1, 1, 1, 1, 1)	e	1

Stelling 8.12. De groep S_n wordt voortgebracht door de naburige verwisselingen $\sigma_1 = (1\ 2)$, $\sigma_2 = (2\ 3)$, \dots , $\sigma_{n-1} = (n-1\ n)$.

Bewijs. We weten al dat elke permutatie te schrijven is als product van cyclen. Voorts is elke k -cykel te schrijven als product van verwisselingen:

$$(i_1 i_2 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k)$$

Voor $i < j - 1$ geldt tenslotte

$$(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j)$$

zodat we met inductie naar $j - i$ inzien dat iedere verwisseling $(i\ j)$ te schrijven is als product van naburige verwisselingen. •

Voorbeeld 8.13. De conjugatieklasse C van het element $a = (1\ 2)(3\ 4)$ in S_4 is $C = \{a, b, c\}$, waar $b = (1\ 3)(2\ 4)$ en $c := (1\ 4)(2\ 3)$. Dan is

$$a^2 = b^2 = c^2 = e, \quad ab = ba = c, \quad bc = cb = a, \quad ca = ac = b$$

Hieruit volgt dat $V := \{e, a, b, c\}$ een abelse ondergroep van S_4 is. Aangezien V een vereniging van conjugatieklassen is geldt dat $V \triangleleft S_4$. Door het isomorfisme van S_4 met \mathcal{T}_h correspondeert V in feite met \mathcal{D}_2 , en komt de situatie hier dus overeen met de situatie besproken in Voorbeeld 6.19.

Door beperken van het conjugatie homomorfisme (zie Definitie 6.15) tot de klasse C krijgen we een homomorfisme

$$\phi: S_4 \rightarrow \text{Sym}(C), \quad \phi(\sigma) = c_\sigma|_C$$

We hebben

$$\begin{aligned} \phi(2\ 3)(a) &= c_{(2\ 3)}((1\ 2)(3\ 4)) \\ &= (2\ 3)(1\ 2)(3\ 4)(2\ 3)^{-1} = (1\ 3)(2\ 4) = b \end{aligned}$$

en evenzo is $\phi(2\ 3)(b) = a$ en $\phi(2\ 3)(c) = c$. Dit betekent dat $\phi(2\ 3) = (a\ b)$. Evenzo is $\phi(3\ 4) = (b\ c)$. Hieruit blijkt dat ϕ surjectief is.

Vanwege de homomorfiestelling geldt $S_4 / \text{Ker}(\phi) \cong \text{Sym}(C)$, en dus is de orde van $\text{Ker}(\phi)$ gelijk aan 4. Aangezien V abels is is $V \subset \text{Ker}(\phi)$. Omdat V ook orde 4 heeft moet die inclusie een gelijkheid zijn. De conclusie is dat $S_4 / V \cong \text{Sym}(C) \cong S_3$.

De ondergroepen-structuur van S_n voor $n < 4$ is gemakkelijk te bepalen. We gaan nu op zoek naar de normale ondergroepen van S_n voor $n > 4$.

Propositie 8.14. Er is een uniek homomorfisme $\varepsilon: S_n \rightarrow \{+1, -1\}$ zodat $\varepsilon(\sigma) = -1$ voor elke 2-cykel.

Bewijs. Het Aanhangsel bevat twee constructies voor ε . •

Gevolg 8.15. *De verzameling van even permutaties*

$$A_n = \{\sigma \in S_n ; \varepsilon(\sigma) = 1\}$$

is een normaaldeler van S_n . De groep A_n heet de alternerende groep.

Propositie 8.16. *Voor $n \geq 3$ wordt de groep A_n voortgebracht door de $(n-2)$ vele 3-cykels $(1\ 2\ i)$ met $i = 3, 4, \dots, n$.*

Bewijs. Zij H_n de ondergroep van S_n voortgebracht door de 3-cykels $(1\ 2\ i)$ met $i = 3, 4, \dots, n$. Evident is dat $H_n \subset A_n$. We bewijzen dat $A_n \subset H_n$ met inductie naar n . Voor $n = 3$ is dit duidelijk want A_3 is cyclisch van orde 3 met voortbrenger $(1\ 2\ 3)$. Zij nu $n \geq 4$ en $\sigma \in A_n$. We onderscheiden een aantal gevallen, al naar gelang de waarde van $s := \sigma(n)$.

- Als $s = n$ dan $\sigma \in A_{n-1}$, en vanwege de inductieveronderstelling $\sigma \in H_{n-1} \subset H_n$.
- Als $s = 1$ dan stellen we $\tau := (1\ 2\ n)^2\sigma$. Dan is $\tau(n) = n$, en dus $\tau \in A_{n-1} \subset H_n$. Maar dan ook $\sigma = (1\ 2\ n)^2\tau \in H_n$.
- Als $s = 2$ dan stellen we $\tau = (1\ 2\ n)\sigma$. Dan is $\tau(n) = n$, en dus $\tau \in A_{n-1} \subset H_n$. Maar dan ook $\sigma = (1\ 2\ n)^2\tau \in H_n$.
- Tenslotte als $3 \leq s \leq n-1$ dan stellen we $\tau = (1\ 2\ n)^2(1\ 2\ s)\sigma$. Dan is $\tau(n) = n$, en dus $\tau \in A_{n-1} \subset H_n$. Maar dan ook $\sigma = (1\ 2\ s)^2(1\ 2\ n)\tau \in H_n$.

•

Propositie 8.17. *Zij $n \geq 3$ en zij N een normaaldeler van A_n die een 3-cykel bevat. Dan is $N = A_n$.*

Bewijs. Door hernaummering mogen we aannemen dat N een normaaldeler van A_n is die de cykel $\sigma := (1\ 2\ 3)$ bevat. Stellen we voor $i \geq 4$ het element $\rho := (1\ 2)(3\ i) \in A_n$, dan volgt

$$\rho\sigma^2\rho^{-1} = (1\ 2)(3\ i)(1\ 3\ 2)(1\ 2)(3\ i) = (1\ 2\ i) \in N.$$

Dus bevat N de 3-cykels $(1\ 2\ i)$ voor $i = 3, 4, \dots, n$. Uit de vorige propositie concluderen we dat $N = A_n$.

•

Definitie 8.18. Een groep G heet *simpel* of *enkelvoudig* als $\#(G) > 1$ en G geen niet-triviale normaaldelers heeft.

Voor elk priemgetal p is de cyclische groep C_p van orde p een voorbeeld van een simpele groep.

Stelling 8.19. *Voor $n \geq 5$ is de alternerende groep A_n simpel.*

Bewijs. Zij $n \geq 5$ en N een normaaldeler van A_n verschillend van $\{e\}$. We zullen bewijzen dat N een 3-cykel bevat.

Kies een niet-triviale σ in N die zoveel mogelijk getallen vast laat. Formeel gezegd: kies een $\sigma \in N \setminus \{e\}$ waarvoor

$$c := \#\{i \in \{1, 2, \dots, n\} ; \sigma(i) \neq i\}$$

minimaal is. We zullen bewijzen dat $c = 3$, of anders gezegd dat σ een 3-cykel is.

- Stel eerst $c = 4$. Dan heeft σ na eventuele hernummering de vorm $\sigma := (1\ 2)(3\ 4)$, want het alternatief $(1\ 2\ 3\ 4)$ is een oneven permutatie en zit dus niet in N . Aangezien $n \geq 5$ is $\rho := (3\ 4\ 5) \in A_n$, en conjugeren met ρ levert $\tau := \rho\sigma\rho^{-1} = (1\ 2)(4\ 5) \in N$. Maar dan ook $\sigma\tau = (3\ 4\ 5) \in N$. Tegenspraak met $c = 4$.
- Stel nu $c = 5$. Dan heeft σ na eventuele hernummering de vorm $\sigma := (1\ 2\ 3\ 4\ 5)$, want het alternatief $(1\ 2\ 3)(4\ 5)$ is een oneven permutatie. Conjugeren met $\rho := (2\ 3\ 4) \in A_n$ levert $\tau := \rho\sigma\rho^{-1} = (1\ 3\ 4\ 2\ 5) \in N$. Maar dan ook $\sigma^{-1}\tau = (1\ 2\ 4) \in N$. Tegenspraak met $c = 5$.
- Stel tenslotte $c \geq 6$. Dan heeft σ na eventuele hernummering één van de volgende vier gedaanten

$$\begin{aligned}\sigma &= (1\ 2\ 3\ 4\dots)\dots \\ \sigma &= (1\ 2\ 3)(4\ 5\ 6)\dots \\ \sigma &= (1\ 2\ 3)(4\ 5)(6\ 7)\dots \\ \sigma &= (1\ 2)(3\ 4)(5\ 6)(7\ 8)\dots\end{aligned}$$

Hierbij is σ geschreven als product van disjuncte cyclen met de volgorde van de factoren gerangschikt naar dalende orde. Conjugeren met $\rho := (2\ 3\ 4) \in A_n$ levert $\tau := \rho\sigma\rho^{-1} \in N$. In de genoemde vier gevallen geeft dit respectievelijk

$$\begin{aligned}\tau &= (1\ 3\ 4\ 2\dots)\dots \\ \tau &= (1\ 3\ 4)(2\ 5\ 6)\dots \\ \tau &= (1\ 3\ 4)(2\ 5)(6\ 7)\dots \\ \tau &= (1\ 3)(4\ 2)(5\ 6)(7\ 8)\dots\end{aligned}$$

In het eerste en vierde geval geldt $\sigma^{-1}\tau(i) = i$ voor $i \geq 5$. In het tweede geval geldt $\sigma^{-1}\tau(i) = i$ voor $i = 5$ en $i \geq 7$. In het derde geval geldt $\sigma^{-1}\tau(i) = i$ voor $i \geq 6$. We vinden dus steeds een tegenspraak met $c \geq 6$.

•

Opmerking 8.20. Bovenstaande stelling ligt aan de geboorte van de groepentheorie. De oplossingen van de algemene tweedegraads vergelijking

$$ax^2 + bx + c = 0$$

worden gegeven door de bekende formule $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Voor de algemene derde- en vierdegraads vergelijking

$$\begin{aligned} ax^3 + bx^2 + cx + d &= 0 \\ ax^4 + bx^3 + cx^2 + dx + e &= 0 \end{aligned}$$

bestaan er analoge expliciete (maar wel ingewikkelde) formules voor de oplossingen in termen van worteltrekken. Deze formules zijn gevonden in de 16^e eeuw door de Italiaanse wiskundigen Scipione del Ferro, Tartaglia en Cardano. Voor $n \geq 5$ bewees de Franse wiskundige Galois rond 1830 dat er geen expliciete formule in termen van worteltrekken bestaat voor de oplossingen van de algemene vergelijking van graad n . De Galoistheorie geeft een vertaling van het probleem over oplossingen van vergelijkingen naar een probleem in de groepentheorie. De onmogelijkheid van een wortelformule voor de oplossingen van de algemene vergelijking van graad n met $n \geq 5$ volgt dan uiteindelijk uit bovenstaande stelling.

We gaan nu in op de relatie tussen de symmetriegroepen van regelmatige veelvlakken en de alternerende groepen.

Opmerking 8.21. In Voorbeeld 2.8 hebben we de tetraëdergroep \mathcal{T} gedefinieerd als $\{g \in \text{SO}(3) ; g(X_{tet}) = X_{tet}\}$. Het homomorfisme $\mathcal{T} \rightarrow \text{Sym}(X_{tet})$ dat aan $g \in \mathcal{T}$ toevoegt zijn beperking tot X_{tet} is injectief en is dus een isomorfisme naar een ondergroep van orde 12. De acht rotaties over $\pm \frac{2\pi}{3}$ worden overgevoerd in 3-cykels en de drie rotaties over $\pm\pi$ worden overgevoerd in permutaties van cykeltype $(2, 2)$. De genoemde ondergroep is dus precies de ondergroep van de even permutaties. Na nummering van de vier elementen van X_{tet} krijgen we dus een isomorfisme $\mathcal{T} \rightarrow A_4$.

Opmerking 8.22. In Voorbeeld 2.9 hebben we de octaëdergroep \mathcal{O} gedefinieerd als $\{g \in \text{SO}(3) ; g(X_{oct}) = X_{oct}\}$, en geconstateerd dat dat samenvalt met $\{g \in \text{SO}(3) ; g(X_{hex}) = X_{hex}\}$. De acht punten van X_{hex} (de hoekpunten van de kubus) vallen uiteen in vier paren van de vorm $\{x, -x\}$, geassocieerd met lichaamsdiagonalen van de kubus. Omdat een g als boven lineair is zal hij een dergelijk paar weer in een dergelijk paar overvoeren. Op deze wijze levert elke $g \in \mathcal{O}$ een permutatie van de verzameling Y van paren. Het zo verkregen homomorfisme $\mathcal{O} \rightarrow \text{Sym}(Y)$ blijkt bijtief te zijn en levert na nummering van de paren een isomorfisme $\mathcal{O} \rightarrow S_4$.

Opmerking 8.23. Als $g \in \mathcal{O}$ dan is $g(X_{tet})$ gelijk aan hetzij X_{tet} hetzij $X_{hex} - X_{tet}$. In het eerste geval is $g \in \mathcal{T}$. In het laatste geval volgt voor

$g' = P \circ g$ dat $g'(X_{tet}) = X_{tet}$ en dus $g' \in \mathcal{T}$. Op deze manier verkrijgen we een afbeelding $\mathcal{O} \cong G(\mathcal{O}, \mathcal{T}) = \mathcal{T}_d \rightarrow \text{Sym}(X_{tet})$. Dit is een ander gezichtspunt op het isomorfisme van de vorige opmerking. De relatie wordt gelegd door het feit dat elk paar $\{x, -x\}$ precies één representant heeft in X_{tet} .

Opmerking 8.24. Zij gegeven $a, b \in X_{ico}$ op afstand 2, zodat ze de eindpunten vormen van een ribbe r . Dan vormen $-a$ en $-b$ de eindpunten van een ribbe r' .

Er zijn twee punten $c, d \in X_{ico}$ op afstand 2 van zowel a als b : dit zijn de toppen van de twee driehoeken die r als gemeenschappelijke basis hebben. Nu vormen c en $-d$ de eindpunten van een ribbe s en evenzo $-c$ en d de eindpunten van een ribbe s' .

Tenslotte zijn er twee punten $e, f \in X_{ico}$ op afstand 2 van zowel a als $-b$. Deze vormen de eindpunten van een ribbe t . Nu liggen $-e$ en $-f$ op afstand 2 van $-a$ en b en ze vormen de eindpunten van een ribbe t' .

De lijn door het midden $\frac{1}{2}(a + b)$ van r , die door het midden $\frac{1}{2}(c + d)$ van s en die door het midden $\frac{1}{2}(e + f)$ van t staan nu loodrecht op elkaar. Een dergelijke verzameling van drie lijnen noemen we een driebeen.

Zo geeft elke ribbe r aanleiding tot een driebeen, maar er zijn steeds zes ribben die aanleiding geven tot hetzelfde driebeen. Dit geeft een totaal van $\frac{30}{6} = 5$ driebeenen. Elk element van \mathcal{I} permuteert deze verzameling Z van vijf driebeenen. Dit geeft aanleiding tot een homomorfisme $\mathcal{I} \rightarrow \text{Sym}(Z)$. Dit homomorfisme blijkt injectief te zijn en de even permutaties als beeld te hebben. Na nummering krijgen we dus een isomorfisme $\mathcal{I} \cong A_5$.

9 Representaties.

Definitie 9.1. Een *representatie* van een groep G op een complexe vectorruimte V is een homomorfisme $\rho: G \rightarrow \text{GL}(V)$.

Voorbeeld 9.2. Definieer $\rho: G \rightarrow \text{GL}_1(\mathbf{C}) = \mathbf{C}^\times$ door $\rho(a) = 1$ voor alle $a \in G$. Dit heet de zogenaamde *triviale representatie* van G .

Voorbeeld 9.3. Zij $G = \langle a \rangle$ een cyclische groep van orde n . Definieer $\rho_k: G \rightarrow \text{GL}_1(\mathbf{C})$ door $\rho_k(a^j) = \exp(2\pi ijk/n)$ voor $j, k = 1, \dots, n$. Dan is ρ_k een representatie van G op \mathbf{C} .

Voorbeeld 9.4. Zij $\phi: H \rightarrow G$ een homomorfisme van groepen, en zij ρ een representatie van G op V . Dan is $\rho \circ \phi$ een representatie van H op V .

Voorbeeld 9.5. Zij $G < \text{O}_n(\mathbf{R})$ een eindige ondergroep dan krijgen we vanwege $\text{O}_n(\mathbf{R}) < \text{GL}_n(\mathbf{C})$ een representatie $\rho: G \rightarrow \text{GL}_n(\mathbf{C})$ van G op \mathbf{C}^n . Dit is de zogenaamde *standaardrepresentatie* van G op \mathbf{C}^n . Zo hebben de groepen C_n en D_n een standaardrepresentatie op \mathbf{C}^2 , en de groepen $\text{C}_n, \text{C}_{nh}, \text{C}_{nv}, \text{D}_n, \text{D}_{nh}, \text{D}_{nd}, \text{S}_n, \text{T}, \text{T}_h, \text{T}_d, \text{O}, \text{O}_h, \text{I}$ en I_h hebben een standaardrepresentatie op \mathbf{C}^3 .

Voorbeeld 9.6. Zij X een eindige verzameling en noteer $\mathbf{C}X$ voor de verzameling van alle functies $f: X \rightarrow \mathbf{C}$. Zij nu gegeven een linkswerking $\alpha: G \times X \rightarrow X$ van een groep G op X . Dan krijgen we een representatie van G op $\mathbf{C}X$ door

$$(\rho(g)f)(x) = f(\alpha(g^{-1}, x))$$

In het bijzondere geval dat $X = G$ en α de groepsvermenigvuldiging is noemen we dit de *reguliere representatie*.

Opmerking 9.7. De volgende berekening laat zien dat $\rho(g)(\delta_a) = \delta_{\alpha(g,a)}$ wat betekent dat $\rho(g)$ de basiselementen δ_a van $\mathbf{C}X$ precies behandelt zoals α de elementen van X behandelt.

$$\begin{aligned} (\rho(g)\delta_a)(x) &= \delta_a(\alpha(g^{-1}, x)) = \begin{cases} 1 & \text{als } \alpha(g^{-1}, x) = a \text{ dus als } x = \alpha(g, a) \\ 0 & \text{als } \alpha(g^{-1}, x) \neq a \text{ dus als } x \neq \alpha(g, a) \end{cases} \\ &= \delta_{\alpha(g,a)}(x) \end{aligned}$$

Definitie 9.8. Zij ρ een representatie van G op V . Een lineaire deelruimte U van V heet een *invariante lineaire deelruimte* als

$$\rho(a)u \in U \text{ voor alle } a \in G, u \in U$$

In dat geval krijgen we door beperking tot U een representatie $\rho_U: G \rightarrow \text{GL}(U)$. De representatie ρ_U heet een *deelrepresentatie* van ρ .

Voorbeeld 9.9. Zij ρ een representatie van G op V . We noteren V^G voor $\{v \in V ; \rho(g)v = v \text{ alle } g \in G\}$. Dit is een invariante lineaire deelruimte van V .

Voorbeeld 9.10. Zij X en ρ als in Voorbeeld 9.6. We beschrijven twee complementaire lineaire deelruimten van $\mathbf{C}X$ die invariant zijn onder $\text{Sym}(X)$.

- Zij $h = \sum_{a \in X} \delta_a$. Dan is $\rho(g)h = \sum_{a \in X} \rho(g)\delta_a = \sum_{a \in X} \delta_{\alpha(g,a)} = \sum_{b \in X} \delta_b = h$. Dus het lineaire opspansel $L = \langle h \rangle$ is een invariante deelruimte.
- Zij $\eta: \mathbf{C}X \rightarrow \mathbf{C}$ gedefinieerd door $\eta(f) = \sum_{x \in X} f(x)$. Dan is $\eta(\delta_a) = \sum_{x \in X} \delta_a(x) = 1$ voor $a \in X$. Verder is

$$\begin{aligned} \eta(\rho(g)f) &= \eta(\rho(g) \sum_{x \in X} f(x)\delta_x) = \eta(\sum_{x \in X} f(x)\rho(g)\delta_x) \\ &= \eta(\sum_{x \in X} f(x)\delta_{\alpha(g,x)}) = \sum_{x \in X} f(x)\eta(\delta_{\alpha(g,x)}) = \sum_{x \in X} f(x) = \eta(f) \end{aligned}$$

Daaruit volgt dat $M = \ker(\eta)$ een invariante lineaire deelruimte is.

Ga zelf na voor elke $p \in X$ geldt dat M het lineaire opspansel is van de $\delta_a - \delta_p$ met $a \in X$, en dat $\mathbf{C}X = L \oplus M$.

Definitie 9.11. De representatie ρ op V heet *reducibel* als er een invariante lineaire deelruimte U is met $U \neq 0$ en $U \neq V$. De representatie ρ op V heet *irreducibel* als $V \neq 0$ en V niet reducibel is.

Voorbeeld 9.12. Zij $\phi: H \rightarrow G$ een *surjectief* homomorfisme van groepen, en zij ρ een irreducibele representatie van G op V . Dan is de representatie $\rho \circ \phi$ van H op V irreducibel. Als er immers een invariante deelruimte U is voor $\rho \circ \phi$, dan is dat ook een invariante deelruimte voor ρ .

Voorbeeld 9.13. Elke representatie op een vectorruimte van dimensie 1 is irreducibel. In het bijzonder geldt dat voor de representatie uit Voorbeeld 9.3.

We willen nu bewijzen dat elke representatie is op te splitsen in irreducibele representaties (kortweg irreps). Daarvoor is de volgende truc nuttig:

Propositie 9.14. Zij ρ een representatie van een eindige groep G op V . Dan is er een Hermiets inproduct H op V waarvoor ρ unitair in de zin dat

$$H(\rho(g)v, \rho(g)w) = H(v, w) \text{ voor alle } g \in G \text{ en } v, w \in V$$

Bewijs. Kies een willekeurig Hermiets inproduct F op V . Definieer een nieuw Hermiets inproduct H op V door uitmiddelen over G :

$$H(v, w) = \frac{1}{\#G} \sum_{a \in G} F(\rho(a)v, \rho(a)w) \text{ voor } v, w \in V$$

Het is gemakkelijk na te rekenen dat H weer een Hermiets inproduct is. Bovendien is

$$\begin{aligned} H(\rho(g)v, \rho(g)w) &= \frac{1}{\#G} \sum_{a \in G} F(\rho(a)\rho(g)v, \rho(a)\rho(g)w) \\ &= \frac{1}{\#G} \sum_{a \in G} F(\rho(ag)v, \rho(ag)w) = \frac{1}{\#G} \sum_{b \in G} F(\rho(b)v, \rho(b)w) = H(v, w) \end{aligned}$$

Daaruit blijkt dat ρ unitair is voor H . •

Propositie 9.15. *Zij V een complexe vectorruimte met Hermiets inproduct H , en zij ρ een unitaire representatie van een groep G op V en zij U een invariante deelruimte. Dan is het orthoplement*

$$U^\perp = \{v \in V ; H(u, v) = 0 \text{ voor alle } u \in U\}$$

ook een invariante deelruimte.

Bewijs. Stel maar $v \in U^\perp$ dus $H(u, v) = 0$ voor alle $u \in U$. Dan is $H(u, \rho(a)v) = H(\rho(a^{-1})u, v) = 0$ voor alle $u \in U$ en alle $a \in G$ zodat $\rho(a)v \in U^\perp$ voor alle $a \in G$. We krijgen dus

$$V = U \oplus U^\perp, \quad \rho = \rho_U \oplus \rho_{U^\perp}$$

een directe som van twee invariante deelruimten. •

Stelling 9.16. *Zij ρ een representatie van een eindige groep G op een complexe vectorruimte V van eindige dimensie. Dan kunnen we V opsplitsen als een directe som $V = U_1 \oplus U_2 \oplus \dots \oplus U_k$ waarbij de deelruimtes U_i allen invariant zijn, en de deelrepresentaties $\rho_i = \rho_{U_i}$ irreducibel zijn.*

We noteren $\rho = \rho_1 \oplus \rho_2 \oplus \dots \oplus \rho_k$

Bewijs. Kies een Hermiets inproduct op V waarvoor ρ unitair is. Als U een niet-triviale invariante deelruimte van V dan is U^\perp dat ook, en ρ is directe som van twee echte deelrepresentaties. Als U en U^\perp niet beide irreducibel zijn dan herhalen we bovenstaande constructie. Omdat $\dim(U) < \dim(V)$ en $\dim(U^\perp) < \dim(V)$ moet dit proces na eindig veel stappen stoppen, en op dat moment hebben we $V = U_1 \oplus \dots \oplus U_k$ met louter irreducibele factoren. •

Voorbeeld 9.17. Bekijk de standaardrepresentatie ρ van C_n op \mathbf{C}^2 :

$$\rho(r^j) = \begin{pmatrix} \cos(2\pi j/n) & -\sin(2\pi j/n) \\ \sin(2\pi j/n) & \cos(2\pi j/n) \end{pmatrix}$$

Schrijven we e_1, e_2 voor de standaard basisvectoren dan is

$$\begin{aligned} \rho(r^j)(e_1 + ie_2) &= \rho(r^j)e_1 + i\rho(r^j)e_2 \\ &= (\cos(2\pi j/n)e_1 + \sin(2\pi j/n)e_2) + i(-\sin(2\pi j/n)e_1 + \cos(2\pi j/n)e_2) \\ &= (\cos(2\pi j/n) - i\sin(2\pi j/n))(e_1 + ie_2) = e^{-2\pi ji/n}(e_1 + ie_2) \end{aligned}$$

en evenzo $\rho(r^j)(e_1 - ie_2) = e^{2\pi ji/n}(e_1 - ie_2)$. Dit betekent dat $\langle e_1 + ie_2 \rangle$ en $\langle e_1 - ie_2 \rangle$ invariante deelruimten zijn.

Omgekeerd als U een 1-dimensionale deelruimte is dan is er een $v \in \mathbf{C}^2$ zo dat $U = \langle v \rangle$. Als U bovendien invariant is dan moet $\rho(r)v$ een veelvoud zijn van v wat betekent dat v een eigenvector is van $\rho(r)$. Voor $n > 2$ zijn de twee eigenwaarden $e^{2\pi i/n}$ en $e^{-2\pi i/n}$ verschillend en moet v dus een veelvoud zijn van $e_1 + ie_2$ of $e_1 - ie_2$. De splitsing in irreducibele delen is in dat geval uniek. Voor $n = 1, 2$ is $\rho(r)$ een scalairvermenigvuldiging en is elke lineaire deelruimte invariant. De splitsing in irreducibele delen is in dat geval niet uniek.

Voorbeeld 9.18. Bekijk de standaardrepresentatie ρ van D_n op \mathbf{C}^2 :

$$\rho(r^j) = \begin{pmatrix} \cos(2\pi j/n) & -\sin(2\pi j/n) \\ \sin(2\pi j/n) & \cos(2\pi j/n) \end{pmatrix}$$

$$\rho(tr^j) = \begin{pmatrix} \cos(2\pi j/n) & -\sin(2\pi j/n) \\ -\sin(2\pi j/n) & -\cos(2\pi j/n) \end{pmatrix}$$

Als U een lineaire deelruimte is van \mathbf{C}^2 en $U \neq \{0\}, \mathbf{C}^2$ dan is een $v \in \mathbf{C}^2$ zo dat $U = \langle v \rangle$. Als U bovendien invariant is dan moet v een eigenvector zijn van $\rho(r)$. Voor $n > 2$ betekent dit dat v een veelvoud is van $e_1 + ie_2$ of $e_1 - ie_2$. Maar $\rho(t)$ voert $e_1 + ie_2$ in $e_1 - ie_2$ over en omgekeerd. Dus als U invariant is moeten ze allebei tot U behoren, zodat $U = \mathbf{C}^2$. De conclusie is dat ρ voor $n > 2$ irreducibel is.

Voorbeeld 9.19. We beschrijven wat 1-dimensionale representaties van D_n .

- Voor elke n is er de triviale representatie met $\rho(r^j) = 1$ en $\rho(tr^j) = 1$. We noemen deze A_1 .
- Voor elke n is er een representatie $\rho(r^j) = 1$ en $\rho(tr^j) = -1$. We noemen deze A_2 .
- Voor even n is er een representatie $\rho(r^j) = (-1)^j$ en $\rho(tr^j) = (-1)^j$. We noemen deze B_1 .
- Voor even n is er een representatie $\rho(r^j) = (-1)^j$ en $\rho(tr^j) = (-1)^{j+1}$. We noemen deze B_2 .

Het is eenvoudig na te rekenen dat dit alle mogelijkheden zijn. Zie ook Propositie 9.35 verderop.

Voorbeeld 9.20. Zoals we gezien hebben in Voorbeeld 9.18 gaat de standaard representatie van D_n door een basis-transformatie over in de representatie σ welke gegeven wordt door

$$\sigma(r^j) = \begin{pmatrix} e^{2\pi ji/n} & 0 \\ 0 & e^{-2\pi ji/n} \end{pmatrix}$$

$$\sigma(tr^j) = \begin{pmatrix} 0 & e^{-2\pi ji/n} \\ e^{2\pi ji/n} & 0 \end{pmatrix}$$

In het bijzonder is σ irreducibel voor $n > 2$.

Voor $k = 1, 2, \dots, n$ definiëren we een homomorfisme $\phi_k: D_n \rightarrow D_n$ door $\phi_k(r^j) = r^{jk}$ en $\phi_k(tr^j) = tr^{jk}$. Dan is het beeld van ϕ_k precies $D_{n/d}$ waar $d = \text{ggd}(n, k)$.

Volgens Voorbeeld 9.12 is $\sigma_k = \sigma \circ \phi_k$ irreducibel tenzij $\frac{n}{d} = 1$ of 2 . Welnu:

- Als $d = n$ dan is $k = n$. In dit geval zijn $\langle e_1 + e_2 \rangle$ en $\langle e_1 - e_2 \rangle$ invariant. Op die twee deelruimtes ziet σ_k er uit als de eerste twee representaties uit het vorige Voorbeeld.
- Als $d = \frac{n}{2}$ dan is $k = \frac{n}{2}$. Ook in dit geval zijn $\langle e_1 + e_2 \rangle$ en $\langle e_1 - e_2 \rangle$ invariant. Op die twee deelruimtes ziet σ_k er uit als de laatste twee representaties uit het vorige Voorbeeld.

Voor $1 \leq k < \frac{n}{2}$ is σ_k dus een irreducibele representatie. De traditionale notatie voor deze representatie in de Molecuulfysica is E_k . We zullen verderop zien dat we hiermee in wezen alle irreducibele representaties van D_n te pakken hebben.

Als je een natuurlijke manier kent om nieuwe vectorruimtes te construeren uit oude, dan kun je dat gebruiken om nieuwe representaties te construeren uit oude. Een eerste dergelijke constructie is de constructie van de duale ruimte V^* van een vectorruimte V . Zie Aanhangsel 12.4 voor de belangrijkste feiten over deze constructie.

Er is dan de complicatie dat voor lineaire afbeeldingen A en B geldt dat $(A \circ B)^* = B^* \circ A^*$ en niet $A^* \circ B^*$. Deze moeilijkheid kan worden ondervangen door gebruik te maken van het feit dat inverteren van groeps-elementen een soortgelijke eigenschap heeft:

Definitie 9.21. Zij ρ een representatie van G op V . Dan wordt de *duale* representatie van G op V^* gegeven door

$$\rho^*(a) = \rho(a^{-1})^* \text{ voor } a \in G$$

Men gaat gemakkelijk na dat $\rho^*(ab) = \rho^*(a)\rho^*(b)$ voor alle $a, b \in G$ zodat ρ^* inderdaad een representatie is. Dit zou verkeerd zijn gegaan als we het inverteren in bovenstaande formule hadden nagelaten.

Voorbeeld 9.22. Als $\rho: G \rightarrow U(n)$ een *unitaire representatie* is van G op \mathbf{C}^n dan geldt $\rho^*(a) = (\rho(a)^{-1})^T = \overline{\rho(a)}$ voor $a \in G$. In het bijzonder is een orthogonale representatie $\rho: G \rightarrow O(n)$ van G op \mathbf{R}^n steeds *gelijk* aan zijn duale. Zeer in het bijzonder geldt dat voor de representaties genoemd in Voorbeeld 9.5.

We bekijken nu een tweede natuurlijke constructie met vectorruimtes. In het Aanhangsel is uitgelegd hoe uit twee vectorruimtes V en W op natuurlijke wijze een nieuwe vectorruimte $V \otimes W$ geconstrueerd kan worden, het zogenaamde tensorproduct van V en W . Als V en W van eindige dimensie zijn dan is $V \otimes W$ dat ook, en $\dim(V \otimes W) = \dim(V) \dim(W)$.

Als $f: V_1 \rightarrow W_1$ en $g: V_2 \rightarrow W_2$ lineaire afbeeldingen zijn levert deze constructie bovendien een lineaire afbeelding $f \otimes g$ op van $V_1 \otimes V_2$ naar $W_1 \otimes W_2$. Tenslotte is $f \otimes g$ inverteerbaar als f en g het zijn.

Definitie 9.23. Zij ρ een representatie van G op V en zij σ een representatie van G op W . Dan is $\rho \otimes \sigma$ de afbeelding $G \rightarrow \text{GL}(V \otimes W)$ gedefinieerd door

$$(\rho \otimes \sigma)(a) = \rho(a) \otimes \sigma(a) \quad \text{voor } a \in G$$

Men gaat eenvoudig na dat $\rho \otimes \sigma$ een representatie is op $V \otimes W$. Deze heet het tensorproduct van ρ en σ .

Voorbeeld 9.24. Bekijk het bijzonder geval dat $V = \mathbf{C}$ is: het tensorproduct $\mathbf{C} \otimes W$ is te identificeren met W zelf door uitvermenigvuldigen: $c \otimes w \mapsto cw$. Voor de representatie $\tau = \rho \otimes \sigma$ geldt dat

$$\tau(a) = \rho(a)\sigma(a) \quad \text{voor } a \in G$$

Voorbeeld 9.25. Bekijk het bijzondere geval dat $W = V$ en $\sigma = \rho$ is: het tensorproduct $V \otimes V$ is te splitsen in een symmetrisch deel $S^2(V)$ en een antisymmetrische deel $A^2(V)$. Beide deelruimtes zijn invariant onder $\rho \otimes \rho$. We krijgen zo representaties $S^2(\rho)$ en $A^2(\rho)$.

We bekijken nu een derde natuurlijke constructie met vectorruimtes. Zij gegeven twee vectorruimtes V en W . Dan noteren we $\text{Hom}(V, W)$ voor de verzameling van alle lineaire afbeeldingen $g: V \rightarrow W$, voorzien van een structuur van vectorruimte door

$$(g_1 + g_2)(v) = g_1(v) + g_2(v), \quad (cg)(v) = cg(v)$$

Als V en W van eindige dimensie zijn dan is $\text{Hom}(V, W)$ dat ook, en $\dim(\text{Hom}(V, W)) = \dim(V) \dim(W)$.

Zij nu ρ een representatie van G op V en zij σ een representatie van G op W . Dan kunnen we een representatie τ van G op $\text{Hom}(V, W)$ definiëren door de formule

$$\tau(a)g = \sigma(a) \circ g \circ \rho(a^{-1})$$

We noteren deze representatie voortaan als $\text{Hom}(\rho, \sigma)$. In het bijzondere geval dat σ de triviale representatie is wordt dit precies de duale representatie van ρ .

In bovenstaande situatie is een element van $\text{Hom}(\rho, \sigma)^G$ niets anders dan een lineaire afbeelding $g: V \rightarrow W$ zo dat

$$g \circ \rho(a) = \sigma(a) \circ g \text{ voor alle } a \in G$$

Definitie 9.26. Een dergelijke afbeelding g noemt men wel een *twijnafbbeelding* (Engels: intertwiner). Als g bovendien bijtief is dan hebben we $\sigma(a) = g \circ \rho(a) \circ g^{-1}$ voor alle $a \in G$. In dit geval is de matrix van $\rho(a)$ ten opzichte van een basis e_1, \dots, e_n van V steeds hetzelfde als de matrix van $\sigma(a)$ ten opzichte van de basis $g(e_1), \dots, g(e_n)$ van W . We noemen σ en ρ dan *equivalente* representaties, en noteren dit als $\rho \simeq \sigma$. Als $\rho \simeq \rho^*$ dan heet ρ *zelfdual*.

Voorbeeld 9.27. Zij ρ een representatie van een groep G op $V = \mathbf{C}^3$. In Propositie 12.12 wordt een isomorfisme $A^2(V) \rightarrow V^*$ beschreven, alsmede een formule die zegt dat ϕ een twijnafbbeelding tussen $A^2(\rho)$ en $\det(\rho) \otimes \rho^*$ is. Dus $A^2(\rho)$ is equivalent met $\det(\rho) \otimes \rho^*$.

Merk op dat $\rho^* = \rho$ in het bijzondere geval dat ρ de standaardrepresentatie is van een ondergroep van $O(3)$.

Opmerking 9.28. Zij ρ een irreducibele representatie van G op V en zij σ een irreducibele representatie van G op W , en zij $f: V \rightarrow W$ een twijnafbbeelding. Als f niet de nulafbeelding is dan is f een isomorfisme en dus een equivalentie. Ten eerste is immers $\text{Ker}(f)$ een invariante deelruimte van V en $\text{ker}(f) \neq V$ zodat $\text{Ker}(f) = \{0\}$. Ten tweede is bovendien $\text{Im}(f)$ een invariante deelruimte van W en $\text{Im}(f) \neq \{0\}$ zodat $\text{Im}(f) = W$.

Stelling 9.29. (Lemma van Schur) *Zij ρ een irreducibele representatie is van G op V . Als $A: V \rightarrow V$ een twijnafbbeelding is dan is A een scalair: er is $\lambda \in \mathbf{C}$ zodat $A = \lambda I$.*

Bewijs. Zij $\lambda \in \mathbf{C}$ een nulpunt van de karakteristieke veelterm van A ; dit betekent dat $\det(A - \lambda I) = 0$. Dan is $A - \lambda I$ geen isomorfisme, en dus noodzakelijk de nulafbeelding. •

Gevolg 9.30. *Zij ρ een irreducibele representatie van G op V en zij σ een irreducibele representatie van G op W . Dan is de ruimte van twijnafbbeeldingen van V naar W van dimensie 1 of 0 al naar gelang $\sigma \simeq \rho$ respectievelijk $\sigma \not\simeq \rho$.*

Bewijs. Als $\sigma \not\simeq \rho$ dan is een twijnafbbeelding geen isomorfisme en dus de nulafbeelding. Als $\sigma \simeq \rho$ dan kiezen we een vaste nietnulle twijnafbbeelding $g: V \rightarrow W$; dat is dan een isomorfisme. Als nu $f: V \rightarrow W$ ook een twijnafbbeelding is dan is $g^{-1} \circ f$ een twijnafbbeelding $V \rightarrow V$ en dus een scalair λ . Dit betekent dat $f = \lambda g$. De ruimte van twijnafbbeeldingen bestaat dus uit de veelvouden van g . •

Gevolg 9.31. Als ρ een irreducibele representatie van een abelse groep G op V is dan is $\dim V = 1$.

Bewijs. Als $\dim(V) > 1$ dan kunnen we een lineaire deelruimte U van V kiezen verschillend van $\{0\}$ en van V .

Zij $a \in G$. Nu volgt uit het abels zijn van G dat $\rho(a): V \rightarrow V$ een twijnafbeelding is. Het Lemma van Schur zegt nu dat er een $\lambda(a) \in \mathbf{C}^*$ is met $\rho(a) = \lambda(a)I$. Dit geldt voor elke $a \in G$, dus U is invariant. Dit is in tegenspraak met de irreducibiliteit van ρ . •

Voorbeeld 9.32. Elke irreducibele representaties van C_n is equivalent met een van de representaties ρ_k genoemd in Voorbeeld 9.3. Als immers ρ een irreducibele representatie is, dan heeft hij dimensie 1, en ligt volledig vast door het beeld $\rho(r) \in \mathbf{C}^* = \text{GL}_1(\mathbf{C})$ voor te schrijven. Vanwege $r^n = e$ volgt $\rho(r)^n = 1$ zodat $\rho(r)$ van de vorm $\exp(2k\pi i/n)$ is voor zekere k . In dat geval is $\rho = \rho_k$.

We kunnen bovenstaand voorbeeld op een nuttige manier generalizeren:

Voorbeeld 9.33. Zij G inwendig direct product van een ondergroep A en een cyclische ondergroep B , voortgebracht door een element b van orde m . Zij ρ een irreducibele representatie van G op V . Dan is $\rho(b)$ een twijnafbeelding en dus volgens Schur een scalarvermenigvuldiging met zekere λ . Dan is $\lambda^m = 1$, en de beperking σ van ρ tot A is irreducibel; immers elke deelruimte van V welke invariant is onder σ is het ook onder ρ .

Omgekeerd levert elke irreducibele representatie σ van A tesamen met een scalar λ met $\lambda^m = 1$ een irreducibele representatie ρ van G door het voorschrift $\rho(ab^j) = \lambda^j \sigma(a)$ voor $a \in A$.

Voorbeeld 9.34. In het bijzonder levert elke irreducibele representatie van een ondergroep A van $\text{SO}(3)$ twee irreducibele representaties van $G(A) \subset \text{O}(3)$ al naar gelang $\lambda = +1$ of -1 . Deze worden in de molecuulfysica genoteerd door de naam van de representatie van A te voorzien van een subscript g of u ('gerade' respectievelijk 'ungerade').

Propositie 9.35. Zij G een eindige groep en zij $\pi: G \rightarrow G_{ab} = G/[G, G]$ de afbeelding gedefinieerd door $\pi(a) = a[G, G]$, zoals besproken in Voorbeeld 6.7 en Opmerking 6.8. Dan induceert π op de manier van Voorbeeld 9.4 een bijectie tussen

- Irreducibele representaties van G van dimensie 1.
- Irreducibele representaties van G_{ab} .

Bewijs. Elke irreducibele representatie van G_{ab} is van dimensie 1 en levert door samenstellen met π een irreducibele representatie van G , uiteraard ook van dimensie 1.

Omgekeerd is een 1-dimensionale representatie van G een homomorfisme ρ van G naar de abelse groep $\mathrm{GL}(\mathbf{C}, 1) = \mathbf{C}^*$. Volgens Opmerking 6.8 is er dan een unieke $\psi: G_{ab} \rightarrow \mathbf{C}^*$ zo dat $\psi \circ \pi = \rho$. •

Opmerking 9.36. We zullen aan het eind van het volgende Hoofdstuk zien dat het aantal equivalentie-classes van irreducibele representaties van een eindige abelse groep A gelijk is aan de orde van die groep. In het bijzonder is het aantal 1-dimensionale irreducibele representaties van een eindige groep G dus gelijk aan de orde van G_{ab} .

In het volgende Hoofdstuk gaan we een calculus ontwikkelen om de irreducibele representaties van niet-abelse groepen mee te classificeren.

9.1 Varia.

In het volgende verdiepen we ons nog wat meer in Voorbeeld 9.6.

Lemma 9.37. *Als X en Y eindige verzamelingen zijn dan is er een natuurlijk isomorfisme tussen $\mathbf{C}(X \times Y)$ en $\mathrm{Hom}(\mathbf{C}Y, \mathbf{C}X)$.*

Bewijs. We definiëren een afbeelding $T: \mathbf{C}(X \times Y) \rightarrow \mathrm{Hom}(\mathbf{C}Y, \mathbf{C}X)$. door de formule

$$(T(K)g)(x) = \sum_{y \in Y} K(x, y) \cdot g(y)$$

voor $x \in X$ en $g \in \mathbf{C}Y$ zodat $T(K)g \in \mathbf{C}X$. Het rechterlid is lineair in g zodat de afbeelding T inderdaad in $\mathrm{Hom}(\mathbf{C}Y, \mathbf{C}X)$ terchtkomt. Bovendien is het rechterlid lineair in K wat betekent dat T een lineaire afbeelding is.

Als $T(K) = 0$ dan geldt voor willekeurige $a \in Y$ dat $T(K)\delta_a = 0$ en dus dat $0 = (T(K)\delta_a)(x) = \sum_{y \in Y} K(x, y) \cdot \delta_a(y) = K(x, a)$ voor alle $x \in X$, zodat $K = 0$. Dit laat zien dat T injectief is. Omdat $\dim \mathbf{C}(X \times Y) = \#(X \times Y) = \#(X) \cdot \#(Y) = \dim(\mathbf{C}Y) \cdot \dim(\mathbf{C}X) = \dim \mathrm{Hom}(\mathbf{C}Y, \mathbf{C}X)$ volgt hieruit dat T zelfs bijectief is. •

Veronderstel nu dat de verzamelingen X en Y voorzien zijn van linkswerkingen van een eindige groep G . Dan kunnen we ook $X \times Y$ voorzien van een linkswerking door het voorschrift $g(x, y) = (gx, gy)$. Op de manier van Voorbeeld 9.6 krijgen we nu representaties van G op $\mathbf{C}X$, $\mathbf{C}Y$ en $\mathbf{C}(X \times Y)$ die we gemakshalve als ρ^X , ρ^Y en $\rho^{X \times Y}$ noteren.

Propositie 9.38. *De afbeelding T is een twijnaafbeelding van $\rho^{X \times Y}$ naar $\sigma = \mathrm{Hom}(\rho^Y, \rho^X)$, en dus een equivalentie.*

Bewijs. Dit is natuurlijk slechts een kwestie van nauwgezet de definities nalopen. We moeten narekenen dat $\sigma(a)T = T\rho^{X \times Y}(a)$ voor $a \in G$. Om zo'n gelijkheid van afbeeldingen te bewijzen moeten we laten zien dat beide

leden op een willekeurig element dezelfde waarde hebben. Uiteindelijk komt het er dus op neer dat we moeten narekenen dat

$$(\sigma(a)T(K)f)(z) = (T(\rho^{X \times Y}(a)K)f)(z)$$

voor willekeurige $K \in \mathbf{C}(X \times Y)$, $f \in \mathbf{C}Y$, $z \in X$.

We werken eerst het rechterlid uit. Daartoe schrijven we eerst de definitie van $(T(L)f)(z)$ uit voor het geval $L = \rho^{X \times Y}(a)K$, vervolgens vullen we in hoe $\rho^{X \times Y}$ volgens Voorbeeld 9.6 is gefabriceerd uit de werking op $X \times Y$, en tenslotte gebruiken we hoe de werking op $X \times Y$ is opgebouwd uit de werkingen op X en Y . Dit levert

$$\begin{aligned} (T(\rho^{X \times Y}(a)K)f)(z) &= \sum_{y \in Y} (\rho^{X \times Y}(a)K)(z, y) \cdot f(y) \\ &= \sum_{y \in Y} (K(a^{-1}(z, y))) \cdot f(y) = \sum_{y \in Y} K(a^{-1}z, a^{-1}y) \cdot f(y) \end{aligned}$$

Nu werken we het linkerlid uit. Daartoe vullen we eerst de definitie van $\sigma = \text{Hom}(\rho^Y, \rho^X)$ in, vervolgens vullen we in hoe ρ^X is gefabriceerd uit de werking op X , daarna schrijven we de definitie van $(T(K)g)(\xi)$ uit voor het geval $g = \rho^Y(a^{-1})f$ en $\xi = a^{-1}z$, en tenslotte vullen we in hoe ρ^Y is gefabriceerd uit de werking op Y . We vinden zo

$$\begin{aligned} (\sigma(a)T(K)f)(z) &= (\rho^X(a)T(K)\rho^Y(a^{-1})f)(z) = (T(K)\rho^Y(a^{-1})f)(a^{-1}z) \\ &= \sum_{\eta \in Y} K(a^{-1}z, \eta) \cdot (\rho^Y(a^{-1})f)(\eta) = \sum_{\eta \in Y} K(a^{-1}z, \eta) \cdot f(a\eta) \end{aligned}$$

Door de sommatie over η te vervangen door een ober $y = a\eta$ zien we dat dit hetzelfde oplevert als het rechterlid. •

Door T te beperken vinden we zo:

Gevolg 9.39. *De ruimte van twijnaafbeeldingen $\mathbf{C}Y \rightarrow \mathbf{C}X$ is isomorf met $\mathbf{C}(X \times Y)^G$. In het bijzonder is de dimensie gelijk aan het aantal banen die de werking van G op $X \times Y$ heeft.*

Voorbeeld 9.40. Als in Voorbeeld 9.10 bekijken we de representatie van de groep $\text{Sym}(X)$ op $\mathbf{C}X$. De ruimte van twijnaafbeeldingen van deze representatie naar zichzelf heeft dimensie 2. De werking van $\text{Sym}(X)$ op $X \times X$ heeft namelijk twee banen, te weten $\{(x_1, x_2) \in X \times X ; x_1 = x_2\}$ en $\{(x_1, x_2) \in X \times X ; x_1 \neq x_2\}$.

We kunnen echter direct twee onafhankelijke twijnaafbeeldingen opschrijven, namelijk ten eerste de afbeelding P_L die de identiteit is op L en nul op M , en ten tweede de afbeelding P_M die de identiteit is op M en nul op L . Als M een directe som was van niet-nulle invariante deelruimtes dan zouden we op deze manier nog meer onafhankelijke twijnaafbeeldingen vinden.

Klaarblijkelijk is dat niet het geval en is M irreducibel; de theorie van het volgende Hoofdstuk zal dat nog verder verduidelijken. De representatie op M heet de *spiegelingsrepresentatie* van $\text{Sym}(X)$.

Voorbeeld 9.41. Zijn $n = 2m$ en bekijk de representatie ρ behorende bij de werking van D_n op X_n . Voor elke $\lambda \in \mathbf{C}$ met $\lambda^n = 1$ vinden we een invariante deelruimte opgespannen door $v = \sum_j \lambda^j P_{n,j}$ en $w = \sum_j \lambda^{-j} p_{n,j}$. Als $\lambda^2 \neq 1$ zijn deze twee vectoren onafhankelijk en vinden we zo een 2-dimensionale irreducibele deelrepresentatie. Als $\lambda^2 = 1$ dan zijn ze afhankelijk en vinden we een 1-dimensionale irreducibele deelrepresentatie. We vinden zo

$$\rho \simeq E_1 \oplus E_2 \oplus \cdots \oplus E_{m-1} \oplus A_1 \oplus B_1$$

Op de wijze van het vorige Voorbeeld levert dit $m + 1$ onafhankelijke twijnafbeeldingen van ρ naar zichzelf.

Anderzijds wordt de baan van een element $(p_{n,k}, p_{n,m}) \in X_n \times X_n$ volledig bepaald door de lengte $\|p_{n,k} - p_{n,m}\|$ van de bijbehorende diagonaal van de regelmatige n -hoek. Er zijn $m + 1$ dergelijk diagonalen en dus $m + 1$ banen.

De volgende stelling kan ook helpen irreducibele representaties te vinden.

Propositie 9.42. *Zij ρ een representatie van G op de vectorruimte V en zij a een element van G . Schrijf V als een directe som van eigenruimten V_i bij eigenwaarden λ_i van $\rho(a)$. Als U een invariante deelruimte van V is van ρ , dan is U de (directe) som van de deelruimten $U \cap V_i$.*

Daarmee is niet gezegd dat de $U \cap V_i$ invariant zijn, maar wel dat het aantal mogelijkheden voor U beperkt is. Bijvoorbeeld als alle V_i van dimensie 1 zijn dan zijn er maar 2^n mogelijkheden voor U , waar $n = \dim(V)$. Immers elke $U \cap V_i$ moet hetzij V_i hetzij $\{0\}$ zijn.

Bewijs. Het is duidelijk dat de som van de deelruimtes $U \cap V_i$ bevat is in V ; het gaat dus om de omgekeerde inclusie. Zij $x \in U$, en schrijf $x = \sum_{i=1}^n x_i$ met $x_i \in V_i$. Dan bevat U voor elke j ook

$$w_j := \prod_{k \neq j} (\rho(a) - \lambda_k I)x = \sum_{i=1}^n \prod_{k \neq j} (\rho(a) - \lambda_k I)x_i = \sum_{i=1}^n \prod_{k \neq j} (\lambda_i - \lambda_k)x_i$$

maar $\prod_{k \neq j} (\lambda_i - \lambda_k)$ is nul voor $i \neq j$, dus

$$w_j = \left(\prod_{k \neq j} (\lambda_j - \lambda_k) \right) x_j$$

We zien dus dat $x_j \in U$, zoals beweerd. •

Voorbeeld 9.43. We kijken nog eens naar de natuurlijke representatie van $G = S_n$ op $V = \mathbf{C}^n$. Zij a de n -cykel $(1\ 2\ 3\ \dots\ n)$. Dan is $\rho(a)e_k = e_{k+1}$ voor elke k , waarbij we deze indices k modulo n tellen. Dus als $\sum_{k=1}^n \alpha_k e_k$ een eigenvector is van $\rho(a)$ dan is $\alpha_k = \lambda \alpha_{k+1}$ voor elke k . In het bijzonder moet gelden $\lambda^n = 1$. We zien dat de eigenwaarden zijn $\lambda_k = \omega^k$, waarbij $\omega = e^{2\pi i/n}$. De bijbehorende eigenruimte V_k is 1-dimensionaal en wordt opgespannen door $v_k := \sum_{\ell=1}^n \omega^{-k\ell} e_\ell$. Er is dus aan de voorwaarden van de Propositie voldaan, wat betekent dat er voor een eventuele invariante deelruimte U maar 2^n mogelijkheden zijn.

Stel je nu voor dat $U \cap V_k \neq \{0\}$ voor zekere $k \neq n$. Kies dan r en $s \in \{1, 2, \dots, n\}$ willekeurig maar verschillend en schrijf t voor de 2-cykel $(r\ s)$. Nu is

$$(\omega^{-kr} - \omega^{-ks})(e_s - e_r) = \rho(t)v_k - v_k \in U$$

hoewel $\omega^{-kr} - \omega^{-ks} \neq 0$. Dus $e_s - e_r \in U$ voor willekeurige r en s . Dit betekent dat $M := \bigoplus_{k=1}^{n-1} V_k = \{\sum_k \xi_k e_k \mid \sum_k \xi_k = 0\}$ in U bevat is. Dus zijn V_n en M de enige invariante deelruimtes.

10 Karakters.

In dit Hoofdstuk is G steeds een eindige groep en zijn de vectorruimtes steeds van eindige dimensie.

Definitie 10.1. Zij ρ een representatie van G op V . Het *karakter* van ρ is de functie $\chi_\rho: G \rightarrow \mathbf{C}$ gedefinieerd door

$$\chi_\rho(a) = \text{tr}(\rho(a)) \text{ voor } a \in G$$

Propositie 10.2. Als ρ een representatie is van G op V en σ een representatie is van G op W dan is

1. Als $\rho \simeq \sigma$ dan $\chi_\rho = \chi_\sigma$.
2. $\chi_\rho(bab^{-1}) = \chi_\rho(a)$ voor alle $a, b \in G$ dus het karakter is constant op conjugatieklassen.
3. $\chi_\rho(e) = \dim V$.
4. $\chi_{\rho^*}(a) = \chi_\rho(a^{-1})$ voor alle $a \in G$.
5. $\chi_{\rho \oplus \sigma}(a) = \chi_\rho(a) + \chi_\sigma(a)$ voor alle $a \in G$.
6. $\chi_{\rho \otimes \sigma}(a) = \chi_\rho(a)\chi_\sigma(a)$ voor alle $a \in G$.
7. $\chi_{\text{Hom}(\rho, \sigma)}(a) = \chi_\rho(a^{-1})\chi_\sigma(a)$ voor alle $a \in G$.
8. $\chi_\rho(a^{-1}) = \overline{\chi_\rho(a)}$.

Bewijs. Het meeste volgt direct uit de eigenschappen van de spoorfunctie. Het voorlaatste item volgt bijvoorbeeld uit een opgave die zegt dat het spoor van de afbeelding $X \mapsto B \circ X \circ A$ gelijk is aan $\text{tr}(B)\text{tr}(A)$.

Voor het laatste item merken we op dat we een Hermiets inproduct op V kunnen kiezen waarvoor $\rho(a)$ unitair is, en dat we het spoor van $\rho(a)$ kunnen bepalen op een basis die orthonormaal is voor dat inproduct. •

In de loop van deze paragraaf zullen we inzien dat de omkering van (1) ook geldt, dus $\rho \simeq \sigma$ dan en slechts dan als $\chi_\rho = \chi_\sigma$. Het karakter karakteriseert dus de representatie op equivalentie na, vandaar de naam.

Definitie 10.3. Zij $L(G)$ de lineaire ruimte van complexwaardige functies op G . Een functie $\phi \in L(G)$ heet *klassefunctie* als $\phi(ab) = \phi(ba)$ voor alle $a, b \in G$. Noteer $C(G)$ voor de lineaire deelruimte van $L(G)$ van klassefuncties.

Dan is $\dim C(G)$ gelijk aan het aantal conjugatieklassen van G . Karakters zijn klassefuncties volgens Propositie 10.2.2.

Definitie 10.4. Voor $\phi, \psi \in L(G)$ stellen we

$$(\phi | \psi) = \frac{1}{\#G} \sum_{x \in G} \phi(x) \overline{\psi(x)}.$$

Men gaat gemakkelijk na dat dit een Hermiets inproduct is op $L(G)$.

Lemma 10.5. *Zij ρ een representatie van G op V . Dan is $(\chi_\rho | 1) = \dim V^G$.*

Bewijs. Definieer een lineaire afbeelding $P: V \rightarrow V$ door

$$Pv = \frac{1}{\#G} \sum_{x \in G} \rho(x)v \text{ voor } v \in V$$

Dan is $\rho(a)P = P$ voor alle $a \in G$ en dus ook $P^2 = P$. De operator P is dus een projectieoperator met als beeld $\text{Im}(P) = V^G$. We vinden dus

$$\begin{aligned} (\chi_\rho | 1) &= \frac{1}{\#G} \sum_{x \in G} \chi_\rho(x) = \frac{1}{\#G} \sum_{x \in G} \text{tr}(\rho(x)) \\ &= \text{tr}(P) = \dim(\text{Im}(P)) = \dim(V^G) \end{aligned}$$

met behulp van Lemma 12.1. •

Stelling 10.6. (Schur orthogonaliteitsrelaties) *Als ρ een irreducibele representatie is van G op V en σ een irreducibele representatie is van G op W dan is*

$$(\chi_\sigma | \chi_\rho) = \begin{cases} 1 & \text{als } \rho \simeq \sigma \\ 0 & \text{als } \rho \not\simeq \sigma \end{cases}$$

Bewijs. Met behulp van Gevolg 9.30 volgt

$$\dim \text{Hom}(V, W)^G = \begin{cases} 1 & \text{als } \rho \simeq \sigma \\ 0 & \text{als } \rho \not\simeq \sigma \end{cases}$$

Anderzijds vinden we door toepassen van Lemma 10.5 op de representatie $\tau = \text{Hom}(\rho, \sigma)$ dat

$$\dim \text{Hom}(V, W)^G = (\chi_\tau | 1) = (\overline{\chi_\rho} \chi_\sigma | 1) = (\chi_\sigma | \chi_\rho)$$

Dit bewijst de stelling. •

Gevolg 10.7. *Zij ρ een representatie van G op V . Zij $V = U_1 \oplus \dots \oplus U_k$ en $\rho = \rho_1 \oplus \dots \oplus \rho_k$ een opsplitsing van (ρ, V) in irreducibele factoren, volgens Stelling 9.16. Zij σ een irreducibele representatie van G op W . Dan is het aantal i waarvoor $\rho_i \simeq \sigma$ gelijk aan $(\chi_\sigma | \chi_\rho)$, en dus onafhankelijk van de gekozen opsplitsing. Het getal $(\chi_\sigma | \chi_\rho) \in \mathbf{N}$ heet de multipliciteit waarmee σ in ρ voorkomt.*

Bewijs. Aangezien $\chi_\rho = \chi_{\rho_1} + \dots + \chi_{\rho_k}$ volgt de bewering uit de orthogonaliteitsrelatie van Schur. •

Gevolg 10.8. *Twee representaties van G met hetzelfde karakter zijn equivalent.*

Bewijs. Dit is duidelijk uit het vorige gevolg. •

Uit de orthogonaliteitsrelaties en het feit dat karakters klassefuncties zijn volgt dat er niet meer onderling inequivalente irreducibele representaties van G kunnen zijn dan $\dim C(G)$, anders gezegd het aantal conjugatieklassen van G .

Notatie 10.9. In algemene situaties nemen we aan dat het volgende gedaan is. Kies in elke equivalentieklasse één irreducibele representatie ρ_i van G op een vectorruimte V_i van dimensie n_i , en schrijf χ_i voor het karakter van ρ_i . We nummeren die keuzes $i = 1, \dots, s$.

Voor concrete groepen G kunnen de representaties natuurlijk specifieke namen krijgen.

Stelling 10.10. *Een representatie ρ van G op V is irreducibel dan en slechts dan als $(\chi_\rho | \chi_\rho) = 1$.*

Bewijs. Schrijf $\rho \simeq m_1\rho_1 \oplus m_2\rho_2 \oplus \dots \oplus m_s\rho_s$ als directe som van de irreducibele representaties van G met multipliciteiten $m_1, \dots, m_s \in \mathbf{N}$. Dan is $(\chi_\rho | \chi_\rho) = \sum_{j=1}^s m_j^2$ gelijk aan 1 alleen als $m_i = 1$ voor zekere i en $m_j = 0$ als $j \neq i$. •

Voorbeeld 10.11. Zij ρ de representatie van S_4 op \mathbf{C}^4 als in Voorbeeld 9.6. Dan is $\chi_\rho(a)$ gelijk aan het aantal enen op de diagonaal van $\rho(a)$ en dus gelijk aan het aantal vaste punten van a . We vinden dus:

$$\chi(e) = 4, \quad \chi((12)) = 2, \quad \chi((123)) = 1, \quad \chi((12)(34)) = \chi((1234)) = 0.$$

Rekening houdend met het aantal elementen per cykel-type vinden we dat $(\chi | \chi) = (4^2 + 6 \cdot 2^2 + 8 \cdot 1^2)/24 = 2$ en $(\chi | 1) = (4 + 6 \cdot 2 + 8 \cdot 1)/24 = 1$. De conclusie is dat ρ de directe som is van de triviale representatie en een irreducibele representatie van dimensie 3.

Stelling 10.12. *Het karakter χ_λ van de reguliere representatie λ van G wordt gegeven door*

$$\chi_\lambda = \#G \cdot \delta_e = \sum_1^s n_j \chi_j.$$

Elke irreducibele representatie komt dus voor in de reguliere, en wel zo vaak als zijn dimensie bedraagt.

Bewijs. Ten opzichte van de basis $\{\delta_x ; x \in G\}$ van $L(G)$ is de matrix van $\lambda(a)$ een permutatiematrix met op de hoofddiagonaal louter nullen als $a \in G$, $a \neq e$ en louter enen als $a = e$. Het is dus duidelijk dat $\chi_\lambda = \#G \cdot \delta_e$.

Schrijf $\lambda \simeq m_1 \rho_1 \oplus \dots \oplus m_s \rho_s$ als directe som van de irreducibele representaties ρ_1, \dots, ρ_s van G met multipliciteiten m_1, \dots, m_s . dan is $\chi_\lambda = \sum m_j \chi_j$ met

$$\begin{aligned} m_j &= (\chi_\lambda | \chi_j) = \frac{1}{\#G} \sum_{a \in G} \chi_\lambda(a) \overline{\chi_j(a)} \\ &= \frac{1}{\#G} \sum_{a \in G} (\#G) \cdot \delta_e(a) \overline{\chi_j(a)} = \overline{\chi_j(e)} = \dim(V_j) \end{aligned}$$

Gevolg 10.13. $\#G = n_1^2 + \dots + n_s^2$.

Bewijs. Evalueer de identiteit $\#G \cdot \delta_e = \sum_1^s n_j \chi_j$ te e .

De volgende Stelling zegt dat s niet alleen kan worden afgeschat met het aantal conjugatieklassen, maar er zelfs aan gelijk is. De karakters van de irreducibele representaties vormen namelijk niet alleen een onafhankelijk stelsel in $C(G)$ maar ook een volledig stelsel.

Stelling 10.14. *De irreducibele karakters χ_1, \dots, χ_s van G zijn een ortho-normale basis van $C(G)$.*

Bewijs. Als ρ een representatie van G op V is en $\phi: G \rightarrow \mathbf{C}$ dan definiëren we $\rho(\phi) \in \text{Hom}(V, V)$ door $\rho(\phi) = \sum_x \phi(x) \rho(x)$.

Als we specialiseren tot het geval dat ϕ een klassefunctie is dan wordt $\rho(\phi) \in \text{Hom}(V, V)^G$ een twijnaafbeelding immers

$$\begin{aligned} \rho(\phi) \rho(y) &= \sum_{x \in G} \phi(x) \rho(xy) = \sum_{z \in G} \phi(zy^{-1}) \rho(z) \\ &= \sum_{z \in G} \phi(y^{-1}z) \rho(z) = \sum_{x \in G} \phi(x) \rho(yx) = \rho(y) \rho(\phi) \end{aligned}$$

Als we nog verder specialiseren tot het geval dat ρ irreducibel is dan volgt uit het Lemma van Schur dat er een $\gamma \in \mathbf{C}$ is met $\rho(\phi) = \gamma I$. De scalair γ berekent men door aan beide zijden het spoor te nemen:

$$\begin{aligned} \gamma \dim(V) &= \gamma \text{tr}(I_V) = \text{tr} \rho(\phi) = \text{tr} \sum_{x \in G} \phi(x) \rho(x) \\ &= \sum_{x \in G} \phi(x) \text{tr} \rho(x) = \sum_{x \in G} \phi(x) \overline{\text{tr} \rho^*(x)} = \sum_{x \in G} \phi(x) \overline{\chi_{\rho^*}(x)} \\ &= \#G \cdot (\phi | \chi_{\rho^*}) \end{aligned}$$

In het bijzonder is $\rho(\phi) = 0$ als $(\phi | \chi_{\rho^*}) = 0$.

Zij $\psi \in C(G)$ en bekijk $\phi = \psi - \sum_j^s (\psi | \chi_j) \chi_j$. Dan is $(\phi | \chi_j) = 0$ voor elke j en dus $\rho_j(\phi) = 0$ voor elke irreducibele representatie ρ_j .

Ook voor een willekeurige representatie ρ van G geldt nu dat $\rho(\phi) = 0$. Dat blijkt door ρ te splitsen in irreducibele delen. Ook voor de reguliere representatie λ geldt dus dat $\lambda(\phi) = 0$.

We hebben nu

$$0 = \lambda(\phi)\delta_e = \sum_{x \in G} \phi(x)\lambda(x)\delta_e = \sum_{x \in G} \phi(x)\delta_x = \phi$$

Maar $\phi = 0$ betekent dat ψ een lineaire combinatie is van de χ_j . •

Gevolg 10.15. *Als G abels is dan is het aantal irreducibele representaties van G gelijk aan zijn orde. Voor algemene G is het aantal 1-dimensionale irreducibele representaties van G gelijk aan de orde van $G/[G, G]$.*

Opmerking 10.16. Men kan ook bewijzen dat n_j steeds een deler is van de orde van G . Daarvoor is theorie nodig die behandeld wordt in de cursus Ringen en Lichamen, met name de theorie van ‘algebraïsch gehele getallen’.

Als afsluiting van dit Hoofdstuk berekenen we enkele karaktertabelen bij wijze van voorbeeld.

Voorbeeld 10.17. We bekijken $G = D_n$ voor n oneven, zeg $n = 2m + 1$. Dan is $[r^{m+1}, t] = r^{2m+2} = r$, waaruit eenvoudig volgt dat $[G, G]$ het opspansel $\langle r \rangle$ van r is, zodat $G/[G, G]$ van orde 2 is. Er zijn dus precies twee 1-dimensionale representaties, die traditioneel A_1 en A_2 heten. Verder zijn er 2-dimensionale irreducibele representaties E_1, E_2, \dots, E_m volgens Voorbeeld 9.20. Omdat $2 \cdot 1^2 + m \cdot 2^2$ gelijk is aan de orde van G , hebben we hiermee alle irreps te pakken. Voor $n = 3$ vinden we zo de volgende tabel:

D_3	E	$2C_3$	$3C_2$
A_1	1	1	1
A_2	1	1	-1
E	2	-1	0

Voorbeeld 10.18. We bekijken nu de groep $G = D_{nh}$. Deze bevat het element

$$\sigma_h = Pr_{2n}^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

de spiegeling om het horizontale vlak. Bij elke irrep X van D_3 zijn er nu twee van D_{nh} die met X' of X'' worden aangeduid al naar gelang ze σ_h in

+1 of -1 afbeelden. Voor $n = 3$ vinden we zo de volgende tabel:

D_{3h}	E	$2C_3$	$3C_2$	σ_h	$2S_3$	$3\sigma_v$
A'_1	1	1	1	1	1	1
A'_2	1	1	-1	1	1	-1
E'	2	-1	0	2	-1	0
A''_1	1	1	1	-1	-1	-1
A''_2	1	1	-1	-1	-1	1
E''	2	-1	0	-2	1	0

Voorbeeld 10.19. We bekijken nu de groep $G = \mathcal{I}$. Deze heeft 5 conjugatieklassen, die we de volgende namen geven:

- E bestaat alleen uit de identieke afbeelding.
- $12C_5$ bestaat uit de 12 rotaties $T_{5,p}$ op pagina 11, dus uit de matrices die daar genoemd worden met $\mu = +1$. Ze hebben spoor $\tau = 1 + 2 \cos(2\pi/5)$.
- $12C'_5$ bestaat uit de 12 rotaties $T_{5,p}^2$ op pagina 11, dus uit de matrices die daar genoemd worden met $\mu = -1$. Ze hebben spoor $1 - \tau = 1 + 2 \cos(4\pi/5)$.
- $20C_3$ bestaat uit de 20 rotaties $T_{3,p}$ op pagina 12. Ze hebben spoor $0 = 1 + 2 \cos(2\pi/3)$.
- $15C_2$ bestaat uit de 15 rotaties $T_{2,p}$ op pagina 12. Ze hebben spoor $-1 = 1 + 2 \cos(2\pi/2)$.

We kunnen meteen twee irreducibele representaties opschrijven. De triviale representatie noemen we A . De standaard-representatie noemen we T_1 . Een derde representatie vergt een klein beetje meer werk:

Om te controleren dat deze lijst van 60 matrices gesloten is onder vermenigvuldiging maken we niet gebruik van het feit dat $\tau = 1.618\dots$ maar alleen van het feit dat τ een oplossing is van de vergelijking $x^2 = x + 1$. Maar $1 - \tau$ is ook een oplossing van deze vergelijking. Als we dus in elk van deze matrices en op elke plek systematisch τ door $1 - \tau$ vervangen dan blijven dezelfde relaties tussen de matrices bewaard. Anders gezegd: we krijgen zo een homomorfisme naar $O(3)$, oftewel een representatie. Op deze manier vinden we een irreducibele 3-dimensionale representatie T_2 van \mathcal{O} .

We kunnen nu alvast een stukje van de karaktertabel opschrijven:

	E	$12C_5$	$12C'_5$	$20C_3$	$15C_2$
A	1	1	1	1	1
T_1	3	τ	$1 - \tau$	0	-1
T_2	3	$1 - \tau$	τ	0	-1

Beschouw nu de 9-dimensionale representatie $T_1 \otimes T_1$ met karakter $(\chi_{T_1})^2$. We kunnen deze representatie splitsen in irreducibele stukken in de hoop iets nieuws tegen te komen. Het aantal irreducibele stukken equivalent met A respectievelijk met T_1 respectievelijk met T_2 bedraagt

$$\begin{aligned} (\chi_{T_1 \otimes T_1} \mid \chi_A) &= \frac{1}{60}(1 \cdot (3)^2 \cdot 1 + 12 \cdot \tau^2 \cdot 1 + 12 \cdot (1 - \tau)^2 \cdot 1 \\ &\quad + 20 \cdot 0^2 \cdot 1 + 15 \cdot (-1)^2 \cdot 1) = 1 \\ (\chi_{T_1 \otimes T_1} \mid \chi_{T_1}) &= \frac{1}{60}(1 \cdot (3)^2 \cdot 3 + 12 \cdot \tau^2 \cdot \tau + 12 \cdot (1 - \tau)^2 \cdot (1 - \tau) \\ &\quad + 20 \cdot 0^2 \cdot 0 + 15 \cdot (-1)^2 \cdot (-1)) = 1 \\ (\chi_{T_1 \otimes T_1} \mid \chi_{T_2}) &= \frac{1}{60}(1 \cdot (3)^2 \cdot 3 + 12 \cdot \tau^2 \cdot (1 - \tau) + 12 \cdot (1 - \tau)^2 \cdot \tau \\ &\quad + 20 \cdot 0^2 \cdot 0 + 15 \cdot (-1)^2 \cdot (-1)) = 0 \end{aligned}$$

Uit de eerste twee uitkomsten volgt al dat

$$T_1 \otimes T_1 = A \oplus T_1 \oplus H$$

voor zekere 5-dimensionale representatie H . Het karakter van H is $\chi_{T_1}^2 - \chi_A - \chi_{T_1}$, dus de rij $(5, 0, 0, -1, 1)$. Dat levert

$$\begin{aligned} (\chi_H \mid \chi_H) &= \frac{1}{60}(1 \cdot 5 \cdot 5 + 12 \cdot 0 \cdot 0 + 12 \cdot 0 \cdot 0 \\ &\quad + 20 \cdot (-1) \cdot (-1) + 15 \cdot 1 \cdot 1) = 1 \end{aligned}$$

en daaruit blijkt dat de representatie H irreducibel is.

Beschouw nu de 9-dimensionale representatie $T_1 \otimes T_2$ waarvan het karakter $\chi_{T_1} \chi_{T_2}$ is. Het aantal irreducibele stukken equivalent met A respectievelijk met T_1 respectievelijk met T_2 respectievelijk met H bedraagt

$$\begin{aligned} (\chi_{T_1 \otimes T_2} \mid \chi_A) &= \frac{1}{60}(1 \cdot 3 \cdot 3 \cdot 1 + 12 \cdot \tau \cdot (1 - \tau) \cdot 1 + 12 \cdot (1 - \tau) \cdot \tau \cdot 1 \\ &\quad + 20 \cdot 0 \cdot 0 \cdot 1 + 15 \cdot (-1) \cdot (-1) \cdot 1) = 0 \\ (\chi_{T_1 \otimes T_2} \mid \chi_{T_1}) &= \frac{1}{60}(1 \cdot 3 \cdot 3 \cdot 3 + 12 \cdot \tau \cdot (1 - \tau) \cdot \tau + 12 \cdot (1 - \tau) \cdot \tau \cdot (1 - \tau) \\ &\quad + 20 \cdot 0 \cdot 0 \cdot 0 + 15 \cdot (-1) \cdot (-1) \cdot (-1)) = 0 \\ (\chi_{T_1 \otimes T_2} \mid \chi_{T_2}) &= \frac{1}{60}(1 \cdot 3 \cdot 3 \cdot 3 + 12 \cdot \tau \cdot (1 - \tau) \cdot (1 - \tau) + 12 \cdot (1 - \tau) \cdot \tau \cdot \tau \\ &\quad + 20 \cdot 0 \cdot 0 \cdot 0 + 15 \cdot (-1) \cdot (-1) \cdot (-1)) = 0 \\ (\chi_{T_1 \otimes T_2} \mid \chi_H) &= \frac{1}{60}(1 \cdot 3 \cdot 3 \cdot 5 + 12 \cdot \tau \cdot (1 - \tau) \cdot 0 + 12 \cdot (1 - \tau) \cdot \tau \cdot 0 \\ &\quad + 20 \cdot 0 \cdot 0 \cdot (-1) + 15 \cdot (-1) \cdot (-1) \cdot 1) = 1 \end{aligned}$$

Uit de laatste uitkomst volgt al dat

$$T_1 \otimes T_2 = H \oplus F$$

voor zekere 4-dimensionale representatie F . Het karakter van F is $\chi_{T_1}\chi_{T_2} - \chi_H$, dus de rij $(4, -1, -1, 1, 0)$. Dat levert

$$(\chi_F | \chi_F) = \frac{1}{60}(1 \cdot 4 \cdot 4 + 12 \cdot (-1) \cdot (-1) + 12 \cdot (-1) \cdot (-1) + 20 \cdot 1 \cdot 1 + 15 \cdot 0 \cdot 0) = 1$$

en daaruit blijkt dat de representatie F irreducibel is.

We kunnen nu de karaktertabel helemaal opschrijven:

	E	$12C_5$	$12C'_5$	$20C_3$	$15C_2$
A	1	1	1	1	1
T_1	3	τ	$1 - \tau$	0	-1
T_2	3	$1 - \tau$	τ	0	-1
F	4	-1	-1	1	0
H	5	0	0	-1	1

Voorbeeld 10.20. We bekijken tenslotte de groep $G = \mathcal{I}_h$. Volgens Voorbeeld 9.34 is de karaktertabel:

\mathcal{I}_h	E	$12C_5$	$12C_5^2$	$20C_3$	$15C_2$	i	$12S_{10}$	$12S_{10}^3$	$20S_6$	15σ
A_g	1	1	1	1	1	1	1	1	1	1
T_{1g}	3	τ	$1 - \tau$	0	-1	3	$1 - \tau$	τ	0	-1
T_{2g}	3	$1 - \tau$	τ	0	-1	3	τ	$1 - \tau$	0	-1
F_g	4	-1	-1	1	0	4	-1	-1	1	0
H_g	5	0	0	-1	1	5	0	0	-1	1
A_u	1	1	1	1	1	-1	-1	-1	-1	-1
T_{1u}	3	τ	$1 - \tau$	0	-1	-3	$-1 + \tau$	$-\tau$	0	1
T_{2u}	3	$1 - \tau$	τ	0	-1	-3	$-\tau$	$-1 + \tau$	0	1
F_u	4	-1	-1	1	0	-4	1	1	-1	0
H_u	5	0	0	-1	1	-5	0	0	1	-1

11 Moleculaire trillingen.

De toestand van een molecuul bestaande uit n deeltjes wordt beschreven door de posities $x_i \in \mathbf{R}^3$ van de deeltjes samen te vatten tot één vector $(x_1, x_2, \dots, x_m) \in \mathbf{R}^m$, waar $m = 3n$. De potentiële energie van het molecuul wordt beschreven door een functie W op \mathbf{R}^m , die we glad (voldoende vaak differentieerbaar) veronderstellen. Neem aan dat W stationair is te $q = (q_1, q_2, \dots, q_m)$, en noteer

$$V(x_1, x_2, \dots, x_m) = W(q_1 + x_1, q_2 + x_2, \dots, q_m + x_m) - W(q_1, q_2, \dots, q_m)$$

Volgens Taylor is

$$V(x_1, x_2, \dots, x_n) = \left(\sum_{i=1}^n \sum_{j=1}^n h_{ij} x_i x_j \right) + \epsilon(x)$$

waar de $h_{ij} = \frac{1}{2} \frac{\partial^2 V}{\partial x_i \partial x_j}(0)$ een symmetrische matrix vormen en waar ϵ de eigenschap heeft dat $\lim_{x \rightarrow 0} \frac{\epsilon(x)}{\|x\|^2} = 0$. We schrijven $\langle x, Hx \rangle$ voor de dubbele som.

Het is redelijk om aan te nemen dat W niet verandert onder translaties van het *gehele* molecuul. Introduceren we nu de *translatiedeelruimte* $T = \{(v, v, \dots, v) \in \mathbf{R}^m ; v \in \mathbf{R}^3\}$ van \mathbf{R}^m dan kunnen we dat formuleren als $W(y+t) = W(y)$ als $y \in \mathbf{R}^m$ en $t \in T$. Er volgt dan dat

$$V(ax+bt) - V(ax) = 0 \text{ voor } t \in T \text{ en } a, b \in \mathbf{R}$$

Berekenen we de partiële afgeleide van het linkerlid naar a in $a = 0$ dan vinden we met behulp van de kettingregel

$$x_i \frac{\partial V}{\partial x_i}(bt) - x_i \frac{\partial V}{\partial x_i}(0)$$

Berekenen we vervolgens de partiële afgeleide naar b in $b = 0$ dan vinden we

$$x_i t_j \frac{\partial^2 V}{\partial x_j \partial x_i}(0) \quad \text{ofwel} \quad 2\langle x, Ht \rangle$$

Dit moet dus verdwijnen voor elke $x \in \mathbf{R}^m$ en elke $t \in T$. Hieruit volgt dat $Ht = 0$ voor elke $t \in T$.

Als $u \in \mathbf{R}^3$ een vector van lengte 1 is en $\alpha \in \mathbf{R}$, dan wordt de rotatie in \mathbf{R}^3 om u over hoek α beschreven door de afbeelding $D_{u,\alpha}: \mathbf{R}^3 \rightarrow \mathbf{R}^3$ gegeven door

$$D_{u,\alpha}(y) = \cos(\alpha) y + \sin(\alpha) u \times y + (1 - \cos(\alpha)) \langle y, u \rangle u$$

De rotatie van het *gehele* molecuul wordt dus beschreven door de afbeelding $E_{u,\alpha}: \mathbf{R}^m \rightarrow \mathbf{R}^m$ gegeven door

$$E_{u,\alpha}(y_1, y_2, \dots, y_n) = (D_{u,\alpha}(y_1), D_{u,\alpha}(y_2), \dots, D_{u,\alpha}(y_n))$$

Merk op dat de afgeleide hiervan naar α in $\alpha = 0$ gelijk is aan de afbeelding $U: \mathbf{R}^m \rightarrow \mathbf{R}^m$ gegeven door $U(y_1, \dots, y_n) = (u \times y_1, \dots, u \times y_n)$.

Het is redelijk om aan te nemen dat W invariant is onder rotaties van het hele molecuul. Dit levert $W(E_{u,\alpha}(y)) = W(y)$ voor elke $y \in \mathbf{R}^3$, elke $\alpha \in \mathbf{R}$ en elke $u \in \mathbf{R}^3$ met $\|u\| = 1$. In termen van V wordt dat

$$V(sE_{u,\alpha}(x) + E_{u,\alpha}(q) - q) - V(sx) = 0$$

voor elke $s \in \mathbf{R}$, elke $x \in \mathbf{R}^3$, elke $\alpha \in \mathbf{R}$ en elke $u \in \mathbf{R}^3$ met $\|u\| = 1$. Differentieren we het linkerlid naar s in $s = 0$ dan vinden we

$$\sum_i E_{u,\alpha}(x)_i \frac{\partial V}{\partial x_i}(E_{u,\alpha}(q) - q) - x_i \frac{\partial V}{\partial x_i}(0)$$

Differentieren we vervolgens naar α in $\alpha = 0$ dan vinden we

$$\sum_{i,j} x_i \frac{\partial (E_{u,\alpha}(q) - q)_j}{\partial \alpha}(0) = 2 \sum_{i,j} h_{i,j} x_i U(q)_j = 2 \langle x, H(U(q)) \rangle$$

Dit moet dus verdwijnen voor elke $x \in \mathbf{R}^m$. Dit betekent dat H verdwijnt op het lineaire opspansel van $U(q)$ namelijk

$$R = \{(u \times q_1, u \times q_2, \dots, u \times q_n); u \in \mathbf{R}^3\}$$

de zogenaamde *rotatiedeelruimte* van \mathbf{R}^m .

We gaan er verder van uit dat q_1, q_2, \dots, q_n niet allemaal op een lijn liggen. Ga zelf na dat in dat geval $T \cap R = \{0\}$. De ruimte $T + R$ waarop H moet verdwijnen is dan van dimensie 6. We nemen tenslotte aan dat q een stabiele evenwichtspositie is. Dat betekent dat H definitief positief is op de quotiëntruimte van \mathbf{R}^m naar $T + R$. Met andere woorden H is definitief positief op een willekeurige lineaire deelruimte van \mathbf{R}^m van dimensie $m - 6$ die complementair is aan $T + R$, bijvoorbeeld de loodruimte $V = (T + R)^\perp$.

Voor algemene V luidt de bewegingsvergelijking

$$\ddot{x}_k + \frac{\partial V}{\partial x_k} = 0, \quad \text{voor } k = 1, \dots, m$$

Dit is een gekoppeld stelsel van niet-lienaire differentiaalvergelijkingen, waarover moeilijk correcte algemene uitspraken zijn te doen. Wanneer de rest-term $\epsilon(x)$ van $V(x)$ zou verdwijnen, zodat $V(x) = \langle x, Hx \rangle$ dan vereenvoudigt

dit systeem van differentiaalvergelijkingen tot het systeem van lineaire differentiaalvergelijkingen $\ddot{x} + Hx = 0$ dat we veel beter aankunnen. Of en in welke mate oplossingen van dit vereenvoudigde systeem goede benaderingen zijn van oplossingen van het echte systeem is een moeilijke en diepzinnige kwestie in de Analyse, waarop we hier niet verder kunnen ingaan. We werken nu verder met het vereenvoudigde systeem.

Omdat H een symmetrische operator is zijn zijn eigenwaarden reëel, en staan de eigenruimtes bij verschillende eigenwaarden loodrecht op elkaar. Door in elk van de eigenruimtes een orthonormale basis te kiezen vinden we een orthonormale basis f_1, \dots, f_m van \mathbf{R}^m bestaande uit eigenvectoren, zodat $H(f_j) = k_j f_j$ voor elke j . We mogen aannemen dat f_{m-5}, \dots, f_m een basis vormen van $T + R$, wat inhoudt dat $k_{m-5} = \dots = k_m = 0$. De aanname van stabiliteit betekent dat $k_j > 0$ voor $j = 1, \dots, m - 6$.

De bewegingen waarbij het molecuul als geheel niet verschuift of draait zijn dus superposities van $(3n - 6)$ harmonische eigentrillingen met frequenties $\nu_j = \sqrt{k_j}$ voor $j = 1, \dots, 3n - 6$. Voor een kwantitatieve bepaling van deze frequenties moet men de symmetrische operator $H: \mathbf{R}^{3n} \rightarrow \mathbf{R}^{3n}$ expliciet kennen. Heeft het molecuul in positie q een voldoende rijke symmetrie, dan stelt kennis van deze symmetriegroep G ons in staat een aantal opmerkelijke kwalitatieve conclusies te trekken. Veronderstel dat het i^{de} atoom en het j^{de} atoom alleen dan gelijke massa hebben als ze identiek zijn. Nemen we het zwaartepunt $\sum_1^n m_j q_j / \sum_1^n m_j$ van het molecuul als oorsprong van \mathbf{R}^3 dan wordt de symmetriegroep G gegeven door

$$G = \{a \in O(3) ; \forall i \exists j \text{ met } m_i = m_j \text{ en } a q_i = q_j\}$$

Deze groep komt voorzien van een aantal bijzondere representaties:

- Als ondergroep van $O(3)$ heeft G een *standaardrepresentatie* π op \mathbf{R}^3 met karakter χ_π .
- De determinant levert een 1-dimensionale representatie van $O(3)$ en dus door samenstellen met π een 1-dimensionale representatie ‘det’ van G .
- Elke element $a \in G$ geeft een permutatie $\sigma_a \in S_n$ door $\sigma_a(i) = j$ als $a(q_i) = q_j$. In combinatie met de standaardrepresentatie van S_n op \mathbf{R}^n levert dat een representatie ρ van G op \mathbf{R}^n . We hebben:

$$\rho(a)(y_1, \dots, y_n) = (y_{\sigma_a^{-1}(1)}, \dots, y_{\sigma_a^{-1}(n)}) \text{ waar } (y_1, \dots, y_n) \in \mathbf{R}^n$$

en het karakter wordt gegeven door $\chi_\rho(a) = \#\{i ; \sigma_a(i) = i\}$.

- We definiëren de *natuurlijke* representatie Π van G op \mathbf{R}^{3n} als $\pi \otimes \rho$. Voor $a \in G$ hebben we dus

$$\Pi(a)(x_1, \dots, x_n) = \left(a x_{\sigma_a^{-1}(1)}, \dots, a x_{\sigma_a^{-1}(n)} \right) \text{ waar } (x_1, \dots, x_n) \in \mathbf{R}^{3n}$$

Als speciaal geval van de algemene formule voor het karakter van een tensor-product krijgen we dus:

Stelling 11.1. (Regel van Wigner). *Het karakter χ_Π van de natuurlijke representatie Π van G op \mathbf{R}^{3n} wordt gegeven door*

$$\chi_\Pi(a) = \#\{i; \sigma_a(i) = i\} \cdot \chi_\pi(a)$$

We hebben echter gezien dat we uit \mathbf{R}^{3n} de 3-dimensionale deelruimtes T en R moeten vewijderen om het relevante deel te krijgen:

- De translatiedeelruimte T van \mathbf{R}^{3n} is een invariante deelruimte want

$$\Pi(a)(v, \dots, v) = (av, \dots, av) \in T$$

voor $a \in G$ en $v \in \mathbf{R}^3$. Uit deze formule blijkt ook dat de afbeelding $\mathbf{R}^3 \rightarrow T$ die v in (v, v, \dots, v) overvoert een equivalentie is. Het karakter χ_T van deze deelrepresentatie is dus gelijk aan χ_π .

- De rotatiedeelruimte R van \mathbf{R}^3 is ook invariant want

$$\begin{aligned} \Pi(a)(u \times q_1, \dots, u \times q_n) &= \left(a \left(u \times q_{\sigma_a^{-1}(1)} \right), \dots, a \left(u \times q_{\sigma_a^{-1}(n)} \right) \right) = \\ &= \left(\left(\det(a) \cdot (a(u) \times a q_{\sigma_a^{-1}(1)}), \dots, \det(a) \cdot (a(u) \times a q_{\sigma_a^{-1}(n)}) \right) \right) = \\ &= \left((\det(a) \cdot (a(u) \times q_1), \dots, \det(a) \cdot (a(u) \times q_n)) \right) = \\ &= \det(a) \cdot (a(u) \times q_1, \dots, a(u) \times q_n) \end{aligned}$$

Hier hebben we gebruikt dat $a q_{\sigma_a^{-1}(j)} = q_j$ per definitie van σ_a , en dat $a(u \times v) = \det(a) \cdot (a(u) \times a(v))$ voor $a \in O(3)$ en $u, v \in \mathbf{R}^3$. Uit deze formule blijkt ook dat de afbeelding $\mathbf{R}^3 \rightarrow R$ die u in $(u \times q_1, \dots, u \times q_n)$ overvoert een equivalentie is op de factor $\det(a)$ na. De beperking van Π tot R is dus equivalent met $(\det) \otimes \pi$, en het karakter χ_R van deze deelrepresentatie is dus gelijk aan $\det \cdot \chi_\pi$.

We krijgen dus een orthogonale opsplitsing in invariante deelruimten

$$\mathbf{R}^{3n} = V \oplus T \oplus R$$

met V het opspannel van f_1, \dots, f_{3n-6} . Het karakter χ_V van de beperking van Π tot V is dus

$$\chi_V = \chi_\Pi - \chi_T - \chi_R = \chi_\Pi - \chi_\pi - \det \cdot \chi_\pi$$

en kan berekend worden met behulp van de regel van Wigner.

Aangezien de symmetriegroep G de bewegingsvergelijking behoudt krijgen we

$$\Pi(a)H = H\Pi(a) \quad \text{voor alle } a \in G$$

De eigenruimte $V_\nu = \{v \in H ; Hv = \nu^2 v\}$ is dus invariant, en de eigenruimte-opsplitsing van H op de *vibratiedeelruimte* V

$$V = \bigoplus_{\nu > 0} V_\nu$$

is een opsplitsing van V in invariante deelruimten. We noteren Π_ν voor de beperking van de representatie Π tot V_ν , en χ_ν voor zijn karakter.

Definitie 11.2. Als de deelrepresentatie Π_ν van G op V_ν irreducibel is voor alle $\nu > 0$ met $V_\nu \neq 0$ dan zegt men dat de operator H op V *natuurlijke ontaarding* heeft voor G . Zo niet dan spreekt men van *toevallige ontaarding*.

In de regel hebben we natuurlijke ontaarding. Een toevallige ontaarding kan worden opgeheven door een kleine nog steeds met G commuterende verstoring H' van H . Toevallige ontaarding kan er ook op wijzen dat G nog niet de volledige symmetriegroep voor het gestelde probleem is. We nemen in de rest van deze paragraaf aan dat H op V natuurlijke ontaarding voor G heeft.

Conclusie 11.3. Het *vibratiespectrum* van M is $\{\nu ; V_\nu \neq 0\}$ en dus de wortel uit het eigenwaardenspectrum van H op V . Het aantal frequenties in het vibratiespectrum van M is dus (hoogstens) gelijk aan het aantal irreducibele factoren van de representatie $\Pi_V : G \rightarrow \text{GL}(V)$. Dit kan belangrijk kleiner zijn dan $3n - 6$.

De frequenties in het vibratiespectrum van M kan men experimenteel vaststellen op een aantal manieren. Bij elke vorm van experiment meet men slechts bepaalde frequenties in het vibratiespectrum gegeven door een zogenaamde *selectieregel*. Het meest gebruikelijke experiment is door licht te schijnen op M en aan het verstrooide licht het infraroodspectrum te meten. De selectieregel voor infraroodspectroscopie zegt:

De frequentie $\nu > 0$ komt voor in het infraroodspectrum van M \iff de irreducibele representatie Π_ν van G op V_ν komt voor in de standaardrepresentatie $\pi : G \rightarrow \text{O}(\mathbf{R}^3)$.

Met karaktertheorie vertaalt deze selectieregel zich in $(\chi_\pi | \chi_\nu) \geq 1$.

Een alternatieve vorm van spectroscopie werd ontdekt door Raman in 1928. De selectieregel voor Ramanspectroscopie luidt:

De frequentie ν komt voor in het Ramanspectrum van M \iff de irreducibele representatie Π_ν van G op V_ν komt voor in de tweede symmetrische macht $S^2(\pi)$ van de standaardrepresentatie $\pi : G \rightarrow \text{O}(\mathbf{R}^3)$.

Met karaktertheorie vertaalt deze selectieregel zich in $(\chi_{S^2\pi} | \chi_\nu) \geq 1$.

Propositie 11.4. *Er geldt $\chi_{S^2(\pi)} = \chi_\pi^2 - \det \cdot \chi_\pi$.*

Bewijs. We gaan uit van de formule

$$\pi \otimes \pi \cong S^2(\pi) \oplus A^2(\pi)$$

Hieruit volgt dat $\chi_\pi^2 = \chi_{S^2(\pi)} + \chi_{A^2(\pi)}$. Volgens Voorbeeld 9.27 is $A^2(\pi)$ equivalent met $\det \cdot \pi$. •

Het volledige vibratiespectrum van M kan worden bepaald met behulp van neutronenverstrooiing.

Conclusie 11.5. Zij $\nu > 0$ een frequentie in het vibratiespectrum van M . Selectieregel voor ν in infraroodspectrum: $(\chi_\pi | \chi_\nu) \geq 1$. Selectieregel voor ν in Ramanspectrum: $(\chi_\pi^2 - \det \cdot \chi_\pi | \chi_\nu) \geq 1$.

Voorbeeld 11.6. Een molecuul XY_3 met het X -aatom in de oorsprong van \mathbf{R}^3 en de drie Y -atomen op de plaatsen $(2, 0, 0)$, $(-1, \sqrt{3}, 0)$, $(-1, -\sqrt{3}, 0)$. De symmetriegroep G is de groep D_{3h} . In Voorbeeld 10.18 vonden we de volgende tabel voor de irreducibele karakters:

D_{3h}	E	$2C_3$	$3C_2$	σ_h	$2S_3$	$3\sigma_v$
A'_1	1	1	1	1	1	1
A'_2	1	1	-1	1	1	-1
E'	2	-1	0	2	-1	0
A''_1	1	1	1	-1	-1	-1
A''_2	1	1	-1	-1	-1	1
E''	2	-1	0	-2	1	0

In het bijzonder is $\det = \chi_{A''_2}$. Daaruit vinden we de volgende waarden voor de karakters van de in dit Hoofdstuk genoemde representaties:

	E	$2C_3$	$3C_2$	σ_h	$2S_3$	$3\sigma_v$
$\chi_T = \chi_\pi$	3	0	1	1	-2	-1
$\chi_R = \det \cdot \chi_\pi$	3	0	-1	-1	2	-1
χ_ρ	4	1	2	4	1	2
$\chi_\Pi = \chi_\pi \chi_\rho$	12	0	2	4	-2	-2
$\chi_V = \chi_\Pi - \chi_T - \chi_R$	6	0	2	4	-2	0
$\chi_{S^2(\pi)} = \chi_\pi^2 - \det \cdot \chi_\pi$	6	0	2	2	2	2

Men controleert eenvoudig dat

$$\chi_V = \chi_{A'_1} + 2\chi_{E'} + \chi_{A''_1}$$

$$\chi_\pi = \chi_{E'} + \chi_{A''_1},$$

$$\chi_{S^2(\pi)} = \chi_\pi^2 - \det \cdot \chi_\pi = 2\chi_{A'_1} + \chi_{E'} + \chi_{E''}.$$

Het volledige vibratiespectrum heeft dus 4 frequenties: Hiervan zien we er 3 in het infraroodspectrum, en ook 3 in het Ramanspectrum. Het infraroodspectrum en het Ramanspectrum hebben 2 frequenties gemeen.

Voorbeeld 11.7. Zoals bekend heeft het icosaaëder twaalf hoekpunten, in elk waarvan vijf driehoeken bijeenkomen. Als je het icosaaëder bij die hoekpunten afknot dan worden die hoekpunten vervangen door regelmatige vijfhoeken. De driehoeken veranderen daarbij in zeshoeken, die bij juiste keuze van de mate van afknotting ook regelmatig zijn. We krijgen zo een half-regelmatig veelvlak gevormd door twaalf regelmatige vijfhoeken en twintig regelmatige zeshoeken. Dit is precies de vorm van een voetbal.

Dit veelvlak heeft $12 \times 5 = 60$ hoekpunten. Plaatsen we in die posities koolstof-atomen dan ontstaat het molecuul *buckminsterfullerene* of kortweg de *buckyball*, genoemd naar de uitvinder en architect Buckminster Fuller. De symmetriegroep G is de groep \mathcal{I}_h , net zoals dat het geval was voor het oorspronkelijke icosaaëder. In Voorbeeld 10.20 hebben we de karaktertabel van G bepaald; we gaan dat nu gebruiken om aan het vibratiespectrum van C_{60} te rekenen.

Een essentieel deel van de berekening is de bepaling van χ_ρ . We willen dus voor elke $a \in G$ weten wat de waarde is van $\chi_\rho(a) = \#\{i ; \sigma_a(i) = i\}$ met andere woorden hoeveel atomen er bij de symmetrie $a \in G$ op hun plaats blijven.

- Als $a \in \mathcal{I} \subset \mathcal{I}_h$, dus als a een rotatie is, dan kunnen alleen de punten van het veelvlak op hun plaats blijven die op de draaiings-as liggen.
 - De as van een rotatie van orde 5 ging door een van de hoekpunten van het icosaaëder, dus door het middelpunt van een van de vijfhoeken. Geen van de nieuwe hoekpunten ligt op die as.
 - De as van een rotatie van orde 3 ging door het middelpunt van een van de zijvlakken van het icosaaëder, dus door het middelpunt van een van de zeshoeken. Geen van de nieuwe hoekpunten ligt op die as.
 - De as van een rotatie van orde 2 ging door het midden van een van de ribben van het icosaaëder, wat ook het midden is van een van de ribben van de nieuwe figuur. Geen van de nieuwe hoekpunten ligt op die as.
- Als $a \in \mathcal{I}_h - \mathcal{I}$, dus als a geen rotatie is, dan is a een combinatie $b \circ P$ van een rotatie b als boven beschreven en de spiegeling P om de oorsprong.
 - Een dergelijke afbeelding laat alleen de oorsprong vast tenzij de rotatie b van orde 2 is.

- Als de rotatie b van orde 2 is, dus een spiegeling om een as, dan is $a = b \cdot P$ de spiegeling om het vlak loodrecht op die as. In dat geval blijven de hoekpunten die in dat vlak liggen op hun plaats, en dat zijn er 4.

Samenvattend kunnen we zeggen dat χ_ρ de waarde 60 heeft op de klasse E van het eenheidselement, en de waarde 4 op de klasse 15σ bestaande uit de 15 vlakspiegelingen. Op de andere acht conjugatieklassen is de waarde nul. Verder:

- De standaard-representatie π van $G = \mathcal{I}_h$ op \mathbf{C}^3 is precies T_{1u} en dus irreducibel.
- Het translatie-deel T van de natuurlijke representatie Π is equivalent met π en dus met T_{1u} .
- Het rotatie-deel R van Π is equivalent met $\det \cdot \pi$ en dus met T_{1g} . Dat is eveneens irreducibel.

We komen zo op de volgende tabel:

\mathcal{I}_h	E	$12C_5$	$12C_5^2$	$20C_3$	$15C_2$
$\chi_T = \chi_\pi$	3	τ	$1 - \tau$	0	-1
$\chi_R = \det \cdot \chi_\pi$	3	τ	$1 - \tau$	0	-1
χ_ρ	60	0	0	0	0
$\chi_\Pi = \chi_\pi \chi_\rho$	180	0	0	0	0
$\chi_V = \chi_\Pi - \chi_T - \chi_R$	174	-2τ	$2\tau - 2$	0	2
$\chi_{S^2(\pi)} = \chi_\pi^2 - \det \cdot \chi_\pi$	6	1	1	0	2

\mathcal{I}_h	i	$12S_{10}$	$12S_{10}^3$	$20S_6$	15σ
$\chi_T = \chi_\pi$	-3	$-1 + \tau$	$-\tau$	0	1
$\chi_R = \det \cdot \chi_\pi$	3	$1 - \tau$	τ	0	-1
χ_ρ	0	0	0	0	4
$\chi_\Pi = \chi_\pi \chi_\rho$	0	0	0	0	4
$\chi_V = \chi_\Pi - \chi_T - \chi_R$	0	0	0	0	4
$\chi_{S^2(\pi)} = \chi_\pi^2 - \det \cdot \chi_\pi$	6	1	1	0	2

Combineren we bovenstaande waarde voor het karakter van $S^2(\pi)$ met de waarden van de karakters van de tien irreducibele representaties in tabel 10.20 dan vinden we bijvoorbeeld

$$\begin{aligned} (\chi_{S^2(\pi)} | \chi_{A_g}) &= (1 \cdot 6 \cdot 1 + 12 \cdot 1 \cdot 1 + 12 \cdot 1 \cdot 1 + 20 \cdot 0 \cdot 1 + 15 \cdot 2 \cdot 1 \\ &\quad + 1 \cdot 6 \cdot 1 + 12 \cdot 1 \cdot 1 + 12 \cdot 1 \cdot 1 + 20 \cdot 0 \cdot 1 + 15 \cdot 2 \cdot 1)/120 \\ &= 1 \end{aligned}$$

$$\begin{aligned} (\chi_{S^2(\pi)} | \chi_{H_g}) &= (1 \cdot 6 \cdot 5 + 12 \cdot 1 \cdot 0 + 12 \cdot 1 \cdot 0 + 20 \cdot 0 \cdot (-1) + 15 \cdot 2 \cdot 1 \\ &\quad + 1 \cdot 6 \cdot 5 + 12 \cdot 1 \cdot 0 + 12 \cdot 1 \cdot 0 + 20 \cdot 0 \cdot (-1) + 15 \cdot 2 \cdot 1)/120 \\ &= 1 \end{aligned}$$

De andere scalaire producten zijn nul. Hieruit volgt dat $S^2(\pi)$ equivalent is met $A_g \oplus H_g$. Je had ook kunnen observeren dat de rij behorende bij $S^2(\pi)$ in bovenstaande tabel precies de som is van de rijen bij A_g en bij H_g in tabel 10.20.

Op dezelfde manier berekenen we

$$\begin{aligned}(\chi_{\Pi} | \chi_{A_g}) &= (1 \cdot 180 \cdot 1 + 15 \cdot 4 \cdot 1)/120 = 2 \\(\chi_{\Pi} | \chi_{T_{1g}}) &= (1 \cdot 180 \cdot 3 + 15 \cdot 4 \cdot (-1))/120 = 4 \\(\chi_{\Pi} | \chi_{T_{2g}}) &= (1 \cdot 180 \cdot 3 + 15 \cdot 4 \cdot (-1))/120 = 4 \\(\chi_{\Pi} | \chi_{F_g}) &= (1 \cdot 180 \cdot 4 + 15 \cdot 4 \cdot 0)/120 = 6 \\(\chi_{\Pi} | \chi_{H_g}) &= (1 \cdot 180 \cdot 5 + 15 \cdot 4 \cdot 1)/120 = 8 \\(\chi_{\Pi} | \chi_{A_u}) &= (1 \cdot 180 \cdot 1 + 15 \cdot 4 \cdot (-1))/120 = 1 \\(\chi_{\Pi} | \chi_{T_{1u}}) &= (1 \cdot 180 \cdot 3 + 15 \cdot 4 \cdot 1)/120 = 5 \\(\chi_{\Pi} | \chi_{T_{2u}}) &= (1 \cdot 180 \cdot 3 + 15 \cdot 4 \cdot 1)/120 = 5 \\(\chi_{\Pi} | \chi_{F_u}) &= (1 \cdot 180 \cdot 4 + 15 \cdot 4 \cdot 0)/120 = 6 \\(\chi_{\Pi} | \chi_{H_u}) &= (1 \cdot 180 \cdot 5 + 15 \cdot 4 \cdot (-1))/120 = 7\end{aligned}$$

Hieruit volgt dat

$$\Pi \simeq 2A_g \oplus 4T_{1g} \oplus 4T_{2g} \oplus 6F_g \oplus 8H_g \oplus A_u \oplus 5T_{1u} \oplus 5T_{2u} \oplus 6F_u \oplus 7H_u$$

en omdat $\Pi = V \oplus T \oplus R$ terwijl $T \simeq T_{1u}$ en $R \simeq T_{1g}$ volgt daaruit

$$V \simeq 2A_g \oplus 3T_{1g} \oplus 4T_{2g} \oplus 6F_g \oplus 8H_g \oplus A_u \oplus 4T_{1u} \oplus 5T_{2u} \oplus 6F_u \oplus 7H_u$$

in ieder geval een directe som van 46 irreducibele representaties.

Het volledige vibratiespectrum bevat dus hoogstens 46 frequenties; dat is een veel betere schatting dan de 174 waar we zonder symmetrie-overwegingen op zouden uitkomen. In het infraroodspectrum zie je van die 46 alleen die waarvan het type voorkomt in π , namelijk type T_{1u} . Dat zijn er slechts 4. In het Ramanspectrum zie je van die 46 alleen die waarvan het type voorkomt in $S^2(\pi)$, namelijk A_g en H_g . Dat zijn er slechts $2 + 8 = 10$.

Het C_{60} -molecuul met deze rijke icosaedersymmetrie werd pas in 1985 experimenteel gevonden door Kroto, Heath, O'Brien, Curl, Smalley. Voor dit werk hebben Curl, Kroto en Smalley in 1996 de Nobelprijs voor chemie ontvangen. De bovenstaande wiskundige conclusies voor het vibratiespectrum van C_{60} zijn alle experimenteel geverifieerd.

12 Aanhangsel: Lineaire algebra.

12.1 Matrices en basis-transformaties

Zij gegeven een vector-ruimte V over \mathbf{R} .

We zeggen dat een deelverzameling X van V een *basis* vormt van V als voor elke $v \in V$ geldt dat

$$v = \sum_{x \in X} c_x x$$

voor zekere getallen $c_x \in \mathbf{R}$, en deze getallen bovendien uniek vastliggen. We noemen die getallen wel de *componenten* van v met betrekking tot de basis X . Elke basis heeft evenveel elementen. Dat aantal heet de *dimensie* van de vectorruimte V . We zullen ons gewoonlijk beperken tot het geval dat de dimensie eindig is.

Zij gegeven twee vectorruimtes V en W . Een afbeelding $A: V \rightarrow W$ heet *lineair* als geldt

- $A(cv) = cA(v)$ voor alle $v \in V$ en $c \in \mathbf{R}$.
- $A(v_1 + v_2) = A(v_1) + A(v_2)$ voor alle $v_1, v_2 \in V$.

Het standaard voorbeeld van een vectorruimte van dimensie n is de verzameling \mathbf{R}^n van n -tallen reële getallen, met pleksgewijze vectorruimtebewerkingen. De standaard basis daarvan heeft als k -de element de vector die een 1 heeft op plek k en een 0 op alle andere plaatsen. Als V een vectorruimte is met basis e_1, e_2, \dots, e_n dan krijgen we een bijectieve lineaire afbeelding $A: \mathbf{R}^n \rightarrow V$ door te definiëren

$$A(c_1, c_2, \dots, c_n) = c_1 e_1 + c_2 e_2 + \dots + c_n e_n$$

Omgekeerd levert een bijectieve lineaire afbeelding $A: \mathbf{R}^n \rightarrow V$ een basis van V door A los te laten op de standaard basis van \mathbf{R}^n .

Neem nu aan dat V voorzien is van een basis X en W voorzien is van een basis Y . Een lineaire afbeelding $A: V \rightarrow W$ is dan helemaal bekend zodra de $A(x)$ gegeven zijn voor $x \in X$. Bovendien kan $A(x)$ beschreven worden door zijn componenten te geven met betrekking tot de basis Y .

Deze overwegingen leiden tot het begrip matrix van A . We nemen aan dat beide bases genummerd zijn: zeg dat X bestaat uit de elementen e_1, e_2, \dots, e_n van V en dat Y bestaat uit de elementen f_1, f_2, \dots, f_m van W . Dan is de matrix van A met betrekking tot die twee genummerde bases het rechthoekige diagram α dat op plek (ij) bevat de f_i -component van $A(e_j)$:

$$A(e_j) = \sum_i \alpha_{ij} f_i$$

De studie van samenstellingen van lineaire afbeeldingen leidt op de volgende manier tot het begrip matrixproduct. Stel dat er nog een vectorruimte U gegeven is, met een basis Z bestaande uit g_1, g_2, \dots, g_p , en ook nog een lineaire afbeelding $B: U \rightarrow V$. Schrijf β voor de matrix van B met betrekking tot de gegeven bases van U en V , en γ voor de matrix van $A \circ B$ met betrekking tot de gegeven bases van U en W . Dan hebben we:

$$(A \circ B)g_k = \sum_i \gamma_{ik} f_i \text{ maar ook}$$

$$(A \circ B)g_k = A \left(\sum_j \beta_{jk} e_j \right) = \sum_j \beta_{jk} A(e_j) = \sum_j \beta_{jk} \sum_i \alpha_{ij} f_i$$

waaruit volgt dat

$$\gamma_{ik} = \sum_j \alpha_{ij} \beta_{jk}$$

Dat is de formule voor het matrixproduct $\gamma = \alpha\beta$.

Een belangrijk speciaal geval treedt op als $U = V$ en als B de identieke afbeelding is. Dit levert het volgende op. Als we de basis X van V vervangen door een basis Z dan heeft dit tot gevolg dat de matrix α van A wordt vervangen door $\alpha\beta$. Hier is β de matrix die de elementen van de nieuwe basis Z uitdrukt in de elementen van de oude basis X .

Op soortgelijke manier kan men beschrijven wat er gebeurt met de matrix van A als we de basis Y van W vervangen door een andere basis. Nu moet aan de linkerkant worden vermenigvuldigd met de matrix die de oude basis uitdrukt in de nieuwe, dus met de *inverse* van de matrix die de nieuwe basis uitdrukt in de oude.

Een nog belangrijker en specialer geval treedt op als $W = V$ en $Y = X$. Dit levert het volgende op. Zij $A: V \rightarrow V$ een lineaire afbeelding en zij α zijn matrix ten opzichte van een basis e_1, e_2, \dots, e_n ; dezelfde basis aan allebei de kanten. Als we deze basis vervangen door een nieuwe basis g_1, g_2, \dots, g_n dan is het effect op de matrix α dat deze wordt vervangen door $\beta^{-1}\alpha\beta$, waar β de matrix is die de nieuwe basis uitdrukt in de oude.

12.2 Determinanten en sporen

De *determinant* is een hele bijzondere functie van de verzameling van vierkante matrices van reële getallen naar \mathbf{R} . We kunnen in het bestek van dit aanhangsel niet ingaan op de constructie van deze functie, maar volstaan met het opsommen van essentiële eigenschappen.

- $\det(\alpha\beta) = \det(\alpha) \det(\beta)$.

- Als we uit een $n \times n$ matrix α een $(n + 1) \times (n + 1)$ matrix β maken door

$$\beta_{ij} = \begin{cases} \alpha_{ij} & \text{als } i \leq n, j \leq n \\ 1 & \text{als } i = j = n + 1 \\ 0 & \text{anders} \end{cases}$$

dan is $\det(\beta) = \det(\alpha)$.

- $\det(\alpha) = a$ als α de 1×1 matrix is met $\alpha_{11} = a$.

In feite ligt de determinants-functie al helemaal vast door bovenstaande drie eisen, maar we kunnen nog meer belangwekkende eigenschappen opschrijven:

- De determinant verandert niet van waarde als we bij een kolom een veelvoud van een andere kolom optellen. Hetzelfde geldt voor rijen.
- De determinant verandert niet van waarde als we de matrix spiegelen.
- De determinant van een singuliere matrix is nul, die van een inverteerbare matrix is ongelijk nul.

Als V een vectorruimte is van eindige dimensie n en $A: V \rightarrow V$ is een lineaire afbeelding dan kunnen we na keuze van een basis van V praten over de $n \times n$ matrix α van A . Als we de basis door een andere vervangen dan wordt de matrix α vervangen door $\beta^{-1}\alpha\beta$, waar β de matrix is die de nieuwe basis uitdrukt in de oude. De eigenschappen van de determinant hebben tot gevolg dat de determinant daarbij niet verandert. We kunnen dus zinvol spreken over de determinant van A . Deze is ongelijk nul d.e.s.d. als A inverteerbaar is.

Als $v_1, v_2, \dots, v_n \in \mathbf{R}^n$ dan schrijven we $\text{Det}(v_1, v_2, \dots, v_n)$ voor de determinant van de lineaire afbeelding die de standaard basisvector e_i steeds in v_i overvoert. met ander woorden voor de determinant van de matrix met de v_i -tjes als kolommen. Er geldt dan

$$\text{Det}(T(v_1), T(v_2), \dots, T(v_n)) = \det(T) \cdot \text{Det}(v_1, v_2, \dots, v_n)$$

Behalve de determinant is er nog een andere belangrijke functie van reële $n \times n$ matrices naar reële getallen, de *spoor*:

$$\text{tr}(\alpha) = \sum_{i=1}^n \alpha_{ii}$$

Uit de formule voor matrixvermenigvuldiging lezen we af dat voor willekeurige α en β geldt:

$$\begin{aligned} \operatorname{tr}(\alpha\beta) &= \sum_{i=1}^n (\alpha\beta)_{ii} = \sum_{i=1}^n \sum_{j=1}^n \alpha_{ij}\beta_{ji} = \\ &= \sum_{k=1}^n \sum_{m=1}^n \beta_{km}\alpha_{mk} = \sum_{k=1}^n (\beta\alpha)_{kk} = \operatorname{tr}(\beta\alpha) \end{aligned}$$

Als γ willekeurig is maar β inverteerbaar dan levert dit:

$$\operatorname{tr}(\beta^{-1}\gamma\beta) = \operatorname{tr}(\beta\beta^{-1}\gamma) = \operatorname{tr}(\gamma)$$

Dus als V een vectorruimte is van eindige dimensie en $T: V \rightarrow V$ is een lineaire afbeelding dan kunnen we de spoor van T definiëren als de spoor van de matrix van T met betrekking tot een willekeurige basis van V ; het resultaat is immers onafhankelijk van de basiskeuze.

Lemma 12.1. *Zij V een vectorruimte van eindige dimensie en zij $P: V \rightarrow V$ een lineaire afbeelding zo dat $P^2 = P$, een zogenaamde projectie-operator. Dan is $\operatorname{tr}(P) = \dim(\operatorname{Im}(P))$.*

Bewijs. We bewijzen dat $V = \operatorname{Ker}(P) \oplus \operatorname{Im}(P)$. Immers als elke $x \in V$ is te schrijven als de som van $x - P(x) \in \operatorname{Ker}(P)$ en $P(x) \in \operatorname{Im}(P)$. Als $x \in \operatorname{Ker}(P) \cap (\operatorname{Im}(P))$ dan is $x = P(y)$ voor zekere $y \in V$ en we hebben $0 = P(x) = P^2(y) = P(y) = x$.

Kies nu een basis e_1, \dots, e_m van $\operatorname{Im}(P)$ en een basis f_1, \dots, f_k van $\operatorname{Ker}(P)$. Dan is $e_1, \dots, e_m, f_1, \dots, f_k$ een basis van V en op deze basis heeft P als matrix

$$\begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}$$

Hieruit lees je af dat $\operatorname{tr}(P) = m = \dim(\operatorname{Im}(P))$. •

12.3 Tekens van permutaties

Zij X een eindige verzameling. We definiëren $\mathbf{C}X$ als de verzameling van alle afbeeldingen $f: X \rightarrow \mathbf{C}$. Deze verzameling heeft een structuur van \mathbf{C} -vectorruimte door te definiëren

$$\begin{aligned} (f_1 + f_2)(x) &= f_1(x) + f_2(x) \\ (cf)(x) &= cf(x) \end{aligned}$$

voor $f_1, f_2 \in \mathbf{C}X$, $x \in X$, $c \in \mathbf{C}$. Voor elke $a \in X$ kunnen we een element $\delta_a \in \mathbf{C}X$ definiëren door

$$\delta_a(x) = \begin{cases} 1 & \text{als } x = a \\ 0 & \text{als } x \neq a \end{cases}$$

We laten nu zien dat deze elementen een basis vormen van $\mathbf{C}X$.

Stel dat $\sum_{a \in X} c_a \delta_a = 0$. Als we beide leden van deze gelijkheid tussen functies loslaten op een element $x \in X$ dan staat er $c_x = 0$. Omdat x willekeurig was bewijst dit dat de δ_a onafhankelijk zijn. Als $f \in \mathbf{C}X$ een willekeurige functie is dan is $f = \sum_{a \in X} f(a) \delta_a$. Dat deze gelijkheid van functies geldt blijkt door beide leden op een willekeurige $x \in X$ los te laten. Deze formule laat zien dat de δ_a ook een volledig stelsel vormen.

Elke afbeelding $h: X \rightarrow X$ levert een lineaire afbeelding $P_h: \mathbf{C}X \rightarrow \mathbf{C}X$ door $(P_h f)(x) = f(h(x))$. Bovendien is P_h bijjectief als h het is. Er geldt dan $P_{h_1} P_{h_2} = P_{h_2 h_1}$ met andere woorden dit definieert een rechts-werking van $\text{Sym}(X)$ op $\mathbf{C}X$. We kunnen er een linkswerking van maken door te combineren met het nemen van inverses in $\text{Sym}(X)$; dit is wat gebeurt in Voorbeeld 9.6.

Bij elke $\sigma \in S_n$ definiëren we een lineaire afbeelding $P_\sigma: \mathbf{R}^n \rightarrow \mathbf{R}^n$ door de formule

$$P(e_j) = e_{\sigma(j)}$$

Dan is het duidelijk dat $P_{\sigma\tau} = P_\sigma P_\tau$. De matrix van P_σ ten opzichte van de basis e_1, \dots, e_n heet de permutatie-matrix behorende bij σ .

Definieer nu $\varepsilon: S \rightarrow \mathbf{Q}^*$ door $\varepsilon(\sigma) = \det(P_\sigma)$. Dan heeft ε de volgende eigenschappen:

- $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ voor alle $\sigma, \tau \in S_n$.
- $\varepsilon(\sigma) = -1$ als σ een verwisseling is.

We gaan nu een andere constructie geven voor de afbeelding ε .

Definitie 12.2. Als $A \subset \{1, 2, \dots, n\}$ uit twee elementen bestaat dan kunnen we schrijven $A = \{i, j\}$ met $i < j$. Definiëren we nu

$$\ell(\sigma, A) = \begin{cases} 0 & \text{als } \sigma(i) < \sigma(j) \\ 1 & \text{als } \sigma(i) > \sigma(j) \end{cases}$$

$$\ell(\sigma) = \sum_A \ell(\sigma, A)$$

dan telt $\ell(\sigma)$ het aantal paren A die door σ in de verkeerde volgorde gebracht worden. We noemen $\ell(\sigma)$ de *lengte* van σ . Een permutatie heet *even* of *oneven* al naar gelang de lengte van de permutatie even of oneven is.

Schrijven we verder

$$\varepsilon(\sigma, A) = \begin{cases} 1 & \text{als } \sigma(i) < \sigma(j) \\ -1 & \text{als } \sigma(i) > \sigma(j) \end{cases}$$

$$\varepsilon(\sigma) = \prod_A \varepsilon(\sigma, A)$$

dan is duidelijk dat

$$\begin{aligned}\varepsilon(\sigma, A) &= (-1)^{\ell(\sigma, A)} \\ \varepsilon(\sigma) &= (-1)^{\ell(\sigma)}\end{aligned}$$

We noemen $\varepsilon(\sigma)$ het *teken* van σ . Even permutaties hebben teken $+1$ en oneven permutaties hebben teken -1 .

Stelling 12.3. *Het teken $\varepsilon: S_n \rightarrow \{+1, -1\}$ is een homomorfisme.*

Bewijs. • Als f een veelterm is in de veranderlijken x_1, x_2, \dots, x_n met gehele coëfficiënten dan kunnen we schrijven

$$f = \sum_{i_1, \dots, i_n \geq 0} a(i_1, \dots, i_n) x_1^{i_1} \dots x_n^{i_n}$$

met $a(i_1, \dots, i_n) \in \mathbf{Z}$ voor $i_1, \dots, i_n \geq 0$. Als $\sigma \in S_n$ een permutatie is dan definiëren we een nieuwe veelterm $\sigma \star f$ door

$$\begin{aligned}\sigma \star f &= \sum_{i_1, \dots, i_n \geq 0} a(i_1, \dots, i_n) x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n} \\ &= \sum_{j_1, \dots, j_n \geq 0} a(j_{\sigma(1)}, \dots, j_{\sigma(n)}) x_1^{j_1} \dots x_n^{j_n}\end{aligned}$$

waarbij de tweede uitdrukking uit de eerste volgt via de substitutie $i_1 = j_{\sigma(1)}, \dots, i_n = j_{\sigma(n)}$. Het is eenvoudig te controleren dat

$$\begin{aligned}\sigma \star (f + g) &= \sigma \star f + \sigma \star g \\ \sigma \star (f \cdot g) &= (\sigma \star f) \cdot (\sigma \star g) \\ \sigma \star (x_i) &= x_{\sigma(i)}\end{aligned}$$

voor alle f en g en i , en in feite ligt de bewerking \star door deze drie eigenschappen geheel vast.

Men kan verder gemakkelijk nagaan dat

$$\sigma \star (\tau \star f) = (\sigma \circ \tau) \star f$$

voor alle σ, τ en f en dat $e \star f = f$ voor alle f .

Dit betekent dat we een linksactie van S_n op die verzameling van veeltermen hebben.

- Gegeven een $A \subset \{1, 2, \dots, n\}$ die uit twee elementen bestaat dan kunnen we daarbij een eerste-graads veelterm f_A definiëren door

$$f_A = (x_i - x_j) \text{ als } A = \{i, j\} \text{ met } i < j$$

Het is dan duidelijk dat

$$\sigma \star f_A = \varepsilon(\sigma, A) \cdot f_{\sigma(A)}$$

Definiëren we nu de veelterm Δ als het product van de f_A over al dergelijke A dan hebben we

$$\sigma \star \Delta = \varepsilon(\sigma)\Delta$$

- Voor alle permutaties σ en τ hebben we nu

$$\begin{aligned} \varepsilon(\sigma \circ \tau) \cdot \Delta &= (\sigma \circ \tau) \star \Delta = \sigma \star (\tau \star \Delta) = \\ &= \sigma \star (\varepsilon(\tau) \cdot \Delta) = \varepsilon(\tau) \cdot (\sigma \star \Delta) = \varepsilon(\tau) \cdot (\varepsilon(\sigma) \cdot \Delta) \end{aligned}$$

waaruit het gestelde volgt door het schrappen van de factor Δ . •

Ga nu zelf na dat $\varepsilon(\sigma) = (-1)^{k-1}$ als σ een k -cykel is.

12.4 Duale ruimtes en tensorproducten

Zij $\mathbf{F} = \mathbf{Q}, \mathbf{R}$ of \mathbf{C} , en zij V een vectorruimte over \mathbf{F} . We noteren V^* voor de verzameling van alle lineaire functies $g: V \rightarrow \mathbf{F}$, voorzien van een structuur van vectorruimte door

$$(g_1 + g_2)(v) = g_1(v) + g_2(v), \quad (cg)(v) = cg(v)$$

We noemen dit de duale ruimte van V .

Als e_1, e_2, \dots, e_n een basis is van V dan kunnen we voor elke $j \leq n$ een lineaire functie $e_j^*: V \rightarrow \mathbf{F}$ definiëren door de formule

$$e_j^* \left(\sum_{i=1}^n c_i e_i \right) = c_j$$

In het bijzonder is dan $e_j^*(e_i) = 1$ als $i = j$ en 0 anders.

De elementen $e_1^*, e_2^*, \dots, e_n^*$ vormen een basis van V . Om te zien dat ze een volledig stelsel vormen merken we op dat voor elke $g \in V^*$ geldt $g = \sum_{j=1}^n g(e_j) e_j^*$. Dit controleer je gemakkelijk door beide leden op een willekeurige vector los te laten. Om te laten zien dat ze een onafhankelijk stelsel vormen veronderstel je dat $\sum_{i=1}^n c_i e_i^* = 0$ voor zekere coëfficiënten c_j . Invullen van e_i in beide leden levert dan $c_i = 0$. We concluderen dat V^* eindig dimensionaal is als V het is en dat dan $\dim(V^*) = \dim(V)$.

Als $A: V \rightarrow W$ een lineaire afbeelding is dan krijgen we een lineaire afbeelding $A^*: W^* \rightarrow V^*$ door de formule

$$(A^*g)v = g(A(v))$$

Stel nu dat e_1, e_2, \dots, e_n een basis is van V en dat f_1, f_2, \dots, f_m een basis is van W en dat α de matrix is van A met betrekking tot deze basissen, zodat $A(e_i) = \sum_{k=1}^m \alpha_{ki} f_k$. Dan volgt hieruit dat $A^*f_j^* = \sum_{\ell=1}^n \alpha_{j\ell} e_\ell^*$ immers

$$(A^*f_j^*)(e_i) = f_j^*(A(e_i)) = f_j^*\left(\sum_{k=1}^m \alpha_{ki} f_k\right) = \alpha_{ji} = \left(\sum_{\ell=1}^n \alpha_{j\ell} e_\ell^*\right)(e_i)$$

Dit betekent dat de matrix van de lineaire afbeelding A^* met betrekking tot de basissen $f_1^*, f_2^*, \dots, f_m^*$ en $e_1^*, e_2^*, \dots, e_n^*$ gegeven wordt door de gespiegelde matrix α^T , gedefinieerd door $(\alpha^T)_{\ell j} = \alpha_{j\ell}$.

Zij gegeven vectorruimtes V en W en S . Dan noemen we een afbeelding $\phi: V \times W \rightarrow S$ *bilineair* als hij lineair in elk van de twee inputs afzonderlijk, dus

$$\begin{aligned} \phi(\alpha_1 v_1 + \alpha_2 v_2, w) &= \alpha_1 \phi(v_1, w) + \alpha_2 \phi(v_2, w) \\ \phi(v, \beta_1 w_1 + \beta_2 w_2) &= \beta_1 \phi(v, w_1) + \beta_2 \phi(v, w_2) \end{aligned}$$

De verzameling $Bi(V, W; S)$ van al zulke bilineaire afbeeldingen kun je voorzien van een structuur van vectorruimte door

$$(\phi_1 + \phi_2)(v, w) = \phi_1(v, w) + \phi_2(v, w), \quad (c\phi)(v, w) = c\phi(v, w)$$

Lemma 12.4. *Zij gegeven vectorruimtes V en W .*

1. Voor $v \in V$ en $w \in W$ zij h de afbeelding $V^* \times W^* \rightarrow \mathbf{R}$ gegeven door $h(f, g) = f(v) \cdot g(w)$. Dan is h bilineair en levert dus een element van $T(V, W) = Bi(V^*, W^*; \mathbf{R})$.
2. Zij t de afbeelding $V \times W \rightarrow T(V, W)$ die aan v en w bovenstaande h toevoegt. Dan is t bilineair.

Bewijs. Routine:

1. We controleren een helft:

$$\begin{aligned} h(c_1 f_1 + c_2 f_2, g) &= (c_1 f_1 + c_2 f_2)(v) \cdot g(w) = \\ &= (c_1 f_1(v) + c_2 f_2(v)) \cdot g(w) = c_1 f_1(v) \cdot g(w) + c_2 f_2(v) \cdot g(w) = \\ &= c_1 h(f_1, g) + c_2 h(f_2, g) \end{aligned}$$

De andere helft gaat net zo.

2. Om na te gaan dat $t(c_1v_1 + c_2v_2, w)$ en $c_1t(v_1, w) + c_2t(v_2, w)$ als afbeeldingen samenvallen controleren we dat de waarden op willekeurige f en g hetzelfde zijn:

$$\begin{aligned} t(c_1v_1 + c_2v_2, w)(f, g) &= f(c_1v_1 + c_2v_2) \cdot g(w) = \\ &= (c_1 \cdot f(v_1) + c_2 \cdot f(v_2)) \cdot g(w) = c_1 \cdot f(v_1) \cdot g(w) + c_2 \cdot f(v_2) \cdot g(w) = \\ &= c_1 \cdot t(v_1, w)(f, g) + c_2 \cdot t(v_2, w)(f, g) \end{aligned}$$

De andere helft gaat net zo. •

Lemma 12.5. *Zij nu v_1, \dots, v_k een basis van V en zij w_1, \dots, w_m een basis van W . Dan vormen de km vele elementen $t(v_i, w_j)$ een basis van $T(V, W)$.*

Bewijs. We moeten laten zien dat we voor gegeven $h \in T(V, W)$ altijd getallen c_{ij} kunnen vinden zodanig dat

$$h = \sum_{i,j} c_{ij} t(v_i, w_j)$$

Om er achter te komen wat de c -tjes moeten zijn vullen we in deze formule aan beide zijden $v_p^* \in V^*$ en $w_q^* \in W^*$ in, met p en q willekeurig. Dat levert

$$\begin{aligned} h(v_p^*, w_q^*) &= \left(\sum_{i,j} c_{ij} t(v_i, w_j) \right) (v_p^*, w_q^*) = \sum_{i,j} c_{ij} \cdot t(v_i, w_j)(v_p^*, w_q^*) = \\ &= \sum_{i,j} c_{ij} \cdot v_p^*(v_i) \cdot w_q^*(w_j) = \sum_{i,j} c_{ij} \cdot \delta(p, i) \cdot \delta(q, j) = c_{pq} \end{aligned}$$

Klaarblijkelijk hebben we is er maar één keuze mogelijk en moeten we in feite laten zien dat

$$h = \sum_{i,j} c_{ij} t(v_i, w_j) \quad \text{met } c_{ij} = h(v_i^*, w_j^*)$$

Om te laten zien dat de linkerzijde en de rechterzijde dezelfde afbeelding $V^* \times W^* \rightarrow \mathbf{R}$ beschrijven moeten we nagaan dat ze op willekeurige $f \in V^*$ en $g \in W^*$ dezelfde waarde hebben. We doen dat in twee stappen:

- Het klopt voor $f = v_p^*$ en $g = w_q^*$. Dat is precies de berekening die we net uitgevoerd hebben!
- Het klopt als $f = \sum_p a_p v_p^*$ en $g = \sum_q b_q w_q^*$. Immers als we het rechterlid even h' noemen dan hebben we

$$\begin{aligned} h(f, g) &= h \left(\sum_p a_p v_p^*, \sum_q b_q w_q^* \right) = \sum_p \sum_q a_p b_q h(v_p^*, w_q^*) = \\ &= \sum_p \sum_q a_p b_q h'(v_p^*, w_q^*) = h' \left(\sum_p a_p v_p^*, \sum_q b_q w_q^* \right) = h'(f, g) \end{aligned}$$

vanwege de eerste stap en omdat h en h' allebei bilineair zijn.

Dit is voldoende omdat elke f en elke g zo te schrijven is. De v_p^* vormen immers een basis van V^* , en de w_q^* vormen een basis van W^* . •

Gevolg 12.6. *Zij $\phi: V \times W \rightarrow X$ een bilineaire afbeelding. Dan is er een unieke lineaire afbeelding $\psi: T(V, W) \rightarrow X$ zodanig dat $\psi \circ t = \phi$.*

Bewijs. De eis $\psi \circ t = \phi$ houdt in dat ψ op het basis-element $t(v_i, w_j)$ van $T(V, W)$ de waarde $\phi(v_i, w_j)$ moet aannemen. Maar een lineaire afbeelding wordt uniek vastgelegd door zijn waarden op de elementen van een basis voor te schrijven. Het is niet moeilijk om te controleren dat de zo gevonden ψ inderdaad aan de eis voldoet. •

We hebben gaandeweg de volgende stelling bewezen:

Stelling 12.7. *Zij gegeven eindig-dimensionale vectorruimten V en W . Dan is er een vectorruimte T en een bilineaire afbeelding $t: V \times W \rightarrow T$ zodanig dat elke andere bilineaire afbeelding $\phi: T \rightarrow S$ te schrijven is als $\phi = \psi \circ t$ voor zekere unieke lineaire afbeelding $\psi: T \rightarrow S$.*

Opmerking 12.8. Als $t: V \times W \rightarrow T$ en $t': V \times W \rightarrow T'$ allebei de eigenschap hebben die in de Stelling worden genoemd, dan zij T en T' isomorf.

Bewijs. In vier stappen:

- Er is een lineaire afbeelding $\psi: T \rightarrow T'$ zodanig dat $\psi \circ t = t'$.
- Er is een lineaire afbeelding $\psi': T' \rightarrow T$ zodanig dat $\psi' \circ t' = t$.
- Nu zijn $\psi' \circ \psi$ en de identieke afbeelding van T allebei lineaire afbeeldingen $\iota: T \rightarrow T$ met de eigenschap $t \circ \iota = t$. Vanwege uniciteit moet $\psi \circ \psi'$ dus gelijk zijn aan de identieke afbeelding.
- Evenzo is $\psi' \circ \psi$ de identieke afbeelding van T' .

Dus ψ is een isomorfisme met inverse ψ' . •

Klaarblijkelijk zijn de in de Stelling genoemde eigenschappen voldoende om de vectorruimte T vast te leggen. We kunnen dus onze verdere bespiegelingen over de ruimte T funderen op bovenstaande Stelling, en we mogen ‘vergeten’ hoe we die T gevonden/gemaakt hebben. We schrijven voortaan $v \otimes w$ voor $t(v, w)$ en $V \otimes W$ voor $T(V, W)$. De volgende Propositie is een voorbeeld van deze filosofie:

Propositie 12.9. *Zij gegeven lineaire afbeeldingen $A: V \rightarrow V'$ en $B: W \rightarrow W'$. Dan is er een unieke lineaire afbeelding $C: V \otimes W \rightarrow V' \otimes W'$ zodanig dat $C(v \otimes w) = A(v) \otimes B(w)$.*

Bewijs. De afbeelding $V \times W \rightarrow V' \otimes W'$ die (v, w) afbeeldt naar $A(v) \otimes B(w)$ is bilineair en is dus te schrijven als $C \circ t$ voor een unieke lineaire C . •

We schrijven deze lineaire afbeelding C voortaan als $A \otimes B$. Hij wordt dus gekarakteriseerd door $(A \otimes B)(v \otimes w) = A(v) \otimes B(w)$.

Propositie 12.10. *Zij gegeven lineaire afbeeldingen*

$$F: V'' \rightarrow V, \quad A: V \rightarrow V' \quad G: W'' \rightarrow W, \quad B: W \rightarrow W'$$

dan geldt $(A \circ F) \otimes (B \circ G) = (A \otimes B) \circ (F \otimes G)$.

Bewijs. Linker- en rechterlid voeren $v \otimes w$ over in $(A(F(v)) \otimes B(G(w)))$. •

We gaan nu onderzoeken hoe we een matrix vinden voor de lineaire afbeelding $A \otimes B$ uit matrices voor A respectievelijk B .

Zij $\alpha = (a_{ij})$ de matrix van A op een basis v_1, \dots, v_k van V en een basis v'_1, \dots, v'_ℓ van V' . Zij $\beta = (b_{pq})$ de matrix van B op een basis f_1, \dots, f_m van W en een basis f'_1, \dots, f'_n van W' . Hoe de matrix van $A \otimes B$ er uitziet hangt natuurlijk af van de manier waarop we de basiselementen $v_i \otimes w_j$ van $V \otimes W$ aftellen. Er zijn twee voor de hand liggende manieren:

- We tellen ze af als

$$v_1 \otimes w_1, v_1 \otimes w_2, v_1 \otimes w_3 \dots, v_1 \otimes w_m, v_2 \otimes w_1, \dots, v_k \otimes w_m$$

In dat geval wordt de matrix van $A \otimes B$ verkregen door elk element a_{ij} van α te vervangen door de matrix $a_{ij}\beta$.

- We tellen ze af als

$$v_1 \otimes w_1, v_2 \otimes w_1, v_3 \otimes w_1 \dots, v_k \otimes w_1, v_1 \otimes w_2, \dots, v_k \otimes f_m$$

In dat geval wordt de matrix van $A \otimes B$ verkregen door elk element b_{pq} van β te vervangen door de matrix $b_{pq}\alpha$.

In beide gevallen zijn de elementen van de resulterende matrix van de vorm $a_{ij}b_{pq}$, maar de volgordes verschillen. Een dergelijk manier om twee matrices in elkaar te schuiven heet wel het *Kronecker product* van die matrices.

Gevolg 12.11. *Als* $A: V \rightarrow V$ *en* $B: W \rightarrow W$ *lineaire afbeeldingen zijn dan geldt*

$$\text{tr}(A \otimes B) = \text{tr}(A) \cdot \text{tr}(B)$$

Zij V een vectorruimte. We kunnen een bilineaire afbeelding $T: V \times V \rightarrow V \otimes V$ definiëren door de formule $T(v_1, v_2) = v_2 \otimes v_1$. Dit geeft aanleiding tot een lineaire afbeelding $T: V \otimes V \rightarrow V \otimes V$ zodanig dat $T(v_1 \otimes v_2) = v_2 \otimes v_1$. Het is niet moeilijk in te zien dat $T \circ T$ de identieke afbeelding is. Dit kunnen we gebruiken om $V \otimes V$ in twee stukken te splitsen.

- De ruimte $S^2(V)$ van *symmetrische tensoren* is $\ker(1 - T)$, wat hetzelfde is als $\text{Im}(1 + T)$.
- De ruimte $A^2(V)$ van *alternerende tensoren* is $\ker(1 + T)$, wat hetzelfde is als $\text{Im}(1 - T)$.

Bij een lineaire afbeelding $F: V \rightarrow V'$ hebben we volgens Propositie 12.9 een lineaire afbeelding $F \otimes F: V \otimes V \rightarrow V' \otimes V'$ en deze voert $A^2(V)$ in $A^2(V')$ over. We noemen deze beperking respectievelijk $A^2(F)$.

Zij $V = \mathbf{R}^3$ en bekijk de afbeelding $D: V \times V \rightarrow V^*$ gegeven door $D(v_1, v_2)(v_3) = \text{Det}(v_1, v_2, v_3)$. Deze D is bilineair en geeft dus aanleiding tot een lineaire afbeelding $D: V \otimes V \rightarrow V^*$. Vanwege de symmetrie-eigenschappen van Det is D nul op $S^2(V)$. We bekijken daarom de beperking ϕ van D tot $A^2(V)$.

Propositie 12.12. *Deze $\phi: A^2(V) \rightarrow V^*$ is een isomorfisme. Als $F: V \rightarrow V'$ een isomorfisme is dan correspondeert $A^2(F)$ onder ϕ met $\det(F) \cdot (F^*)^{-1}$.*

Bewijs. De ruimte $V \otimes V$ wordt opgespannen door de $e_i \otimes e_j$, dus de ruimte $A^2(V)$ wordt opgespannen door de $(1 - T)$ beelden daarvan namelijk de $e_i \otimes e_j - e_j \otimes e_i$. Welnu:

$$\begin{aligned}\phi(e_1 \otimes e_2 - e_2 \otimes e_1) &= 2e_3^*, \\ \phi(e_2 \otimes e_3 - e_3 \otimes e_2) &= 2e_1^*, \\ \phi(e_3 \otimes e_1 - e_1 \otimes e_3) &= 2e_2^*,\end{aligned}$$

en daaruit blijkt dat ϕ een isomorfisme is.

De tweede bewering is dat

$$\phi \circ A^2(F) = (\det(F) \cdot (F^*)^{-1}) \circ \phi$$

zoals aangegeven in het volgende diagram:

$$\begin{array}{ccc} A^2(V) & \xrightarrow{\phi} & V^* \\ \downarrow A^2(F) & & \downarrow \det(F) \cdot (F^*)^{-1} \\ A^2(V) & \xrightarrow{\phi} & V^* \end{array}$$

Welnu, $(\phi \circ A^2(F))(v_1 \otimes v_2 - v_2 \otimes v_1) = \phi(F(v_1) \otimes F(v_2) - F(v_2) \otimes F(v_1))$ is het element van V^* dat v_3 overvoert in

$$2\text{Det}(F(v_1), F(v_2), v_3)$$

Anderzijds is $(\det(F) \cdot (F^*)^{-1}) \circ \phi(v_1 \otimes v_2 - v_2 \otimes v_1)$ het element van V^* dat v_3 overvoert in

$$\begin{aligned} & \det(F) \cdot ((F^*)^{-1})(\phi(v_1 \otimes v_2 - v_2 \otimes v_1))(v_3) \\ &= \det(F) \cdot (\phi(v_1 \otimes v_2 - v_2 \otimes v_1)(F^{-1}v_3)) \\ &= \det(F) \cdot 2 \text{Det}(v_1, v_2, F^{-1}v_3) \end{aligned}$$

Vanwege de eigenschappen van Det is dat hetzelfde. •

De tweede bewering is precies de regel van Cramer voor een 3×3 matrix: $\det(F)$ maal de gespiegelde inverse van de matrix van F is gelijk aan de matrix van determinanten van 2×2 deelmatrices.

12.5 Inproducten.

Zij V een vectorruimte over \mathbf{R} van eindige dimensie.

Definitie 12.13. Een symmetrische vorm op V is een afbeelding $B: V \times V \rightarrow \mathbf{R}$ die voldoet aan de volgende eisen

1. $B(u, v + w) = B(u, v) + B(u, w)$ voor alle $u, v, w \in V$
2. $B(cu, v) = cB(u, v)$ voor alle $u, v \in V$ en $c \in \mathbf{R}$.
3. $B(v, u) = B(u, v)$ voor alle $u, v \in V$.

Als e_1, e_2, \dots, e_n een basis van V is dan wordt een B helemaal vastgelegd door het geven van de symmetrische matrix (β) waar

$$\beta_{ij} = B(e_i, e_j)$$

Definitie 12.14. Een symmetrische vorm B op V heet een scalair product of inproduct als ook nog voldaan is aan de volgende eis:

$$B(u, u) > 0 \text{ als } u \in V \text{ en } u \neq 0.$$

Dit is het geval als de matrix van B ten opzichte van zekere basis precies de eenheids-matrix is. We noemen die basis dan *orthonormaal*.

Zij gegeven een vectorruimte V met scalair product B en een vectorruimte W met scalair product C . Een lineaire afbeelding $A: V \rightarrow W$ heet een *isometrie* als

$$B(x, y) = C(A(x), A(y))$$

voor alle $x, y \in V$. Voor de bijbehorende matrices geldt dan

$$\beta = \alpha^T \gamma \alpha$$

waar γ de matrix van C is, β die van B , en α die van A . In het bijzonder vinden we $I_n = \alpha^T \alpha$ als de basissen van V en W allebei orthonormaal zijn.

Merk op dat een orthogonale afbeelding $A: V \rightarrow W$ altijd injectief is, en als V en W dezelfde eindige dimensie hebben dan is hij dus zelfs bijtief. Een bijtieve isometrie heet een *orthogonale* afbeelding. Een orthogonale afbeelding van een ruimte naar zichzelf noemen we een *orthogonale transformatie* van die ruimte.

Het standaard voorbeeld van een ruimte met scalair product is \mathbf{R}^n met het scalair product B_E dat gegeven wordt door

$$B_E(x, y) = \sum_{i=1}^n x_i y_i$$

en dat ook het *Euclidische* scalair product genoemd wordt. In plaats van $B_E(u, v)$ schrijven we gewoonlijk $\langle u, v \rangle$. De standaard basis van \mathbf{R}^n is een orthonormale basis. Een orthogonale transformatie van \mathbf{R}^n wordt precies beschreven door een $n \times n$ matrix α met $\alpha^T \alpha = I_n$.

Als V een vectorruimte is met orthonormale basis dan is er een unieke orthogonale lineaire afbeelding $A: \mathbf{R}^n \rightarrow V$ die de standaard basis in de gegeven basis overvoert. Omgekeerd levert elke orthogonale lineaire afbeelding een orthonormale basis van V door hem los te laten op de standaard basis van \mathbf{R}^n .

We gaan nu standaard-vormen afleiden voor de matrices van orthogonale transformaties in dimensies 2 en 3.

Lemma 12.15. *Zij V een vectorruimte met scalair product, en met orthonormale basis $\{e_1, e_2\}$. Zij $A: V \rightarrow V$ een orthogonale transformatie van determinant 1. Als $A(e_1) = \xi e_1 + \eta e_2$, dan is $A(e_2) = -\eta e_1 + \xi e_2$.*

Bewijs. Noteer $A(e_2)$ als $\kappa e_1 + \lambda e_2$. Dan is

$$\begin{aligned} & (\kappa + \eta)^2 + (\lambda - \xi)^2 \\ &= (\kappa^2 + \lambda^2) + (\xi^2 + \eta^2) - 2(\lambda\xi - \kappa\eta) \\ &= B(A(e_2), A(e_2)) + B(A(e_1), A(e_1)) - 2\det(A) \\ &= B(e_2, e_2) + B(e_1, e_1) - 2\det(A) = 1 + 1 - 2 = 0 \end{aligned}$$

Daaruit volgt dat $\kappa = -\eta$ en $\lambda = \xi$. •

Omdat $\xi^2 + \eta^2 = 1$ kun je $\phi \in \mathbf{R}$ kiezen (niet uniek) zó dat $\xi = \cos(\phi)$ en $\eta = \sin(\phi)$. We kunnen dan het bovenstaande Lemma als volgt herschrijven.

Propositie 12.16. *Een element van $SO(2)$ heeft altijd de vorm*

$$r(\phi) := \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix}$$

Het element is dan meetkundig te interpreteren als een draaiing over een hoek ϕ in de richting gaande van e_1 naar e_2 (dat is tegen de klok in als je e_1 en e_2 op de gebruikelijke manier tekent).

Lemma 12.17. *Als $A \in \text{SO}(3)$ dan is er $p \in \mathbf{R}^3$ met $p \neq 0$ en $Ap = p$.*

Bewijs. Uit de eigenschappen van de determinant leiden we af:

$$\begin{aligned} \det(A - 1) &= \det(A^t - 1) = \det(A) \det(A^t - 1) \\ &= \det(AA^t - A) = \det(1 - A) = -\det(A - 1) \end{aligned}$$

Dus $A - 1$ is singulier en bezit een niet-nulle vector in de kern. •

In dimensie 3 is de de volgende stelling van Euler nuttig:

Propositie 12.18. *Voor elke $\phi \in \mathbf{R}$ schrijf*

$$M_\phi = \begin{pmatrix} \cos(\phi) & -\sin(\phi) & 0 \\ \sin(\phi) & \cos(\phi) & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad N_\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\phi) & -\sin(\phi) \\ 0 & \sin(\phi) & \cos(\phi) \end{pmatrix}$$

Dan geldt: voor elke $A \in \text{SO}(3)$ zijn er $\alpha, \beta, \gamma \in \mathbf{R}$ met $A = M_\alpha N_\beta M_\gamma$.

Bewijs. Noteer $e = (0, 0, 1) \in \mathbf{R}^3$. Schrijf $v = A(e)$ als $(a, b, c) \in \mathbf{R}^3$. We constateren:

- Noteer $r = \sqrt{a^2 + b^2}$.
Dan is $r^2 + c^2 = 1$. Dus is er $\beta \in \mathbf{R}$ met $r = \sin(\beta)$ en $c = \cos(\beta)$.
- Neem even aan dat $r \neq 0$ en noteer $s = a/r$, $t = b/r$.
Dan is $s^2 + t^2 = 1$. Dus is er $\alpha \in \mathbf{R}$ met $s = \sin(\alpha)$ en $t = -\cos(\alpha)$.

Samengevat hebben we

$$\begin{aligned} v = (a, b, c) &= (sr, tr, c) = \\ &= (\sin(\alpha) \sin(\beta), -\cos(\alpha) \sin(\beta), \cos(\beta)) = M_\alpha N_\beta e \end{aligned}$$

Als $r = 0$ dan kun je $\alpha = 0$ kiezen en geldt deze formule ook.

Nu is $N_\beta^{-1} M_\alpha^{-1} A e = e$. Dus $N_\beta^{-1} M_\alpha^{-1} A$ is van de vorm M_γ voor zekere $\gamma \in \mathbf{R}$, ofwel $A = M_\alpha N_\beta M_\gamma$. •

Je kunt dus elk element van $\text{SO}(3)$ beschrijven met drie reële getallen, de ‘Euler hoeken’. Helaas is die schrijfwijze niet uniek. In de eerste plaats tellen die hoeken natuurlijk alleen maar modulo gehele veelvouden van 2π . In de tweede plaats hangt $M_\alpha N_\beta M_\gamma$ voor $\beta = 0$ alleen van $\alpha + \gamma$ af.

12.6 Hermietse inproducten.

Bijna alles wat in de vorige sectie is gedaan met de reële getallen kan vrij letterlijk worden overgedaan voor de complexe getallen.

Wel zijn er kleine wijzigingen nodig. Zo kunnen we van een symmetrische vorm B niet verwachten dat $B(x, x)$ alleen maar reële waarden aanneemt, laat staan alleen positieve.

We moeten daarom wat morrelen aan de lineariteits-eis en de symmetrie-eis:

Definitie 12.19. Zij V een vectorruimte over \mathbf{C} van eindige dimensie. Een Hermietse vorm op V is een afbeelding $H: V \times V \rightarrow \mathbf{C}$ die voldoet aan de volgende eisen:

1. $H(u, v + w) = H(u, v) + H(u, w)$ voor alle $u, v, w \in V$
2. $H(cu, v) = cH(u, v)$ voor alle $u, v \in V$ en $c \in \mathbf{C}$.
3. $H(v, u) = \overline{H(u, v)}$ voor alle $u, v \in V$.

Uit de combinatie van de tweede en derde eis volgt nu: $H(u, cv) = \bar{c}H(u, v)$ voor $u, v \in V$, $c \in \mathbf{C}$.

Als e_1, e_2, \dots, e_n een basis van V is dan wordt een B helemaal vastgelegd door het geven van de matrix (β) waar

$$\beta_{ij} = B(e_i, e_j)$$

De matrix β is Hermiets in de zin dat $\beta_{ji} = \overline{\beta_{ij}}$.

Definitie 12.20. Een Hermiets vorm H op V heet een Hermiets inproduct als ook nog voldaan is aan de volgende eis:

$$H(u, u) > 0 \text{ als } u \in V \text{ en } u \neq 0.$$

Deze eis heeft zin omdat uit de derde eis blijkt dat $H(u, u)$ reëel is.

Zoals in het reële geval is aan de extra eis voldaan als de matrix van H ten opzichte van zekere basis precies de eenheids-matrix is, en noemen we die basis dan *orthonormaal*.

Zij gegeven een vectorruimte V met Hermiets inproduct H en een vectorruimte W met scalar product K . Een lineaire afbeelding $A: V \rightarrow W$ heet weer *isometrisch* als

$$H(x, y) = K(A(x), A(y))$$

voor alle $x, y \in V$. Voor de bijbehorende matrices geldt dan

$$\beta = \bar{\alpha}^T \gamma \alpha$$

waar γ de matrix van K is, β die van H , en α die van A . In het bijzonder vinden we $I_n = \bar{\alpha}^T \alpha$ als de basissen van V en W allebei orthonormaal zijn.

Merk op dat een isometrie $A: V \rightarrow W$ altijd injectief is, en als V en W dezelfde eindige dimensie hebben dan is hij dus zelfs bijectief. Een bijectieve isometrie heet een *unitaire* afbeelding. Een unitaire afbeelding van een ruimte naar zichzelf noemen we een *unitaire transformatie* van die ruimte.

Het standaard voorbeeld van een ruimte met Hermiets inproduct is \mathbf{C}^n met het Hermiets inproduct dat gegeven wordt door

$$\langle x | y \rangle = \sum_{i=1}^n x_i \bar{y}_i$$

De standaard basis van \mathbf{C}^n is een orthonormale basis. Een unitaire transformatie van \mathbf{C}^n wordt precies beschreven door een $n \times n$ matrix α met $\bar{\alpha}^T \alpha = I_n$.

Analoog aan het reële geval hebben unitaire transformaties in dimensie 2 een standaardvorm:

Propositie 12.21. *Een element van $SU(2)$ heeft altijd de vorm*

$$\begin{pmatrix} \xi & -\bar{\eta} \\ \eta & \bar{\xi} \end{pmatrix}$$

met $\xi \bar{\xi} + \eta \bar{\eta} = 1$.

Voor dimensie drie hebben we niet zoiets: de redenering die ons vertelde dat $\det(A-1) = 0$ als $A \in SO(3)$ vertelt alleen maar dat $\det(A-1)$ imaginair is als $A \in SU(3)$.

Inhoudsopgave

1	Symmetrie en transformatiegroepen	1
2	Eindige voorbeelden in \mathbb{R}^3.	6
3	Groepen en ondergroepen	16
4	Werkingen van groepen.	27
5	Groepen van orthogonale transformaties.	34
6	Normaaldelers en factorgroepen	42
7	Sylow theorie.	51
8	De symmetrische groep.	54
9	Representaties.	63
9.1	Varia.	71
10	Karakters.	75
11	Moleculaire trillingen.	83
12	Aanhangsel: Lineaire algebra.	92
12.1	Matrices en basis-transformaties	92
12.2	Determinanten en sporen	93
12.3	Tekens van permutaties	95
12.4	Duale ruimtes en tensorproducten	98
12.5	Inproducten.	104
12.6	Hermietse inproducten.	107