Algebraïsche structuren – leerplan Wiskunde B+S’’ (derde graad D-finaliteit)

2024-09-01

1 Inleiding

In het leerplan Wiskunde B+S’’ van de 3de graad D-finaliteit staat een leerplandoel over algebraïsche structuren.

LPD 43 De leerlingen analyseren verzamelingen voorzien van één of meerdere bewerkingen aan de hand van een algebraïsche structuur.

Dit document heeft als doel inhoudelijke duiding te geven bij deze leerplandoelstelling. Dit document is niet bedoeld als leermateriaal voor leerlingen.

2 Algebraïsche structuren

Het leerplandoel geeft niet aan welke algebraïsche structuur gebruikt moet worden. Je kan dus de algebraïsche structuur (of structuren) die je wil behandelen zelf kiezen. Voorbeelden zijn groepen, ringen, velden en vectorruimten. In dit document focussen we op groepen en vectorruimtes. Voor beide structuren geven we de definities, tal van voorbeelden en enkele aanverwante begrippen.

De voorbeelden (en tegenvoorbeelden) kunnen gebruikt worden om het leerplandoel te evalueren: je kan laten nagaan of gegeven verzamelingen met bijhorende bewerking(en) voldoen aan de definitie. Veel van de voorbeelden leggen een link met andere leerinhouden.

De aanverwante begrippen worden niet verplicht door het leerplandoel en staan in oplopende moeilijkheidsgraad. Ze kunnen bijvoorbeeld dienen als suggesties voor het complementair gedeelte. Interessant zijn de gelijkenissen tussen de begrippen ‘*deelgroep*’ (3.3.2) en ‘*lineaire deelruimte*’ (4.3.3) en tussen de begrippen ‘*groepsmorfisme*’ (3.3.3) en ‘*lineaire afbeelding*’ (4.3.4). Voor elke algebraïsche structuur is er een goede notie van deelstructuur en van afbeelding. Kennis van één algebraïsche structuur helpt bij het aanleren van een andere algebraïsche structuur.

3 Groepen

3.1 Wat is een groep?

Een **groep** $G,*$ bestaat uit een niet-lege verzameling G en een bewerking $*$ die voldoen aan de volgende voorwaarden:

1) de bewerking $*$ is gesloten: $x * y \in G$ voor alle $x, y \in G$ (m.a.w. de bewerking kan beschouwd worden als een afbeelding $*: G \times G \to G: (x,y) \mapsto x * y$);
2) de bewerking $*$ is associatief: $x * (y * z) = (x * y) * z$ voor alle $x, y, z \in G$;
3) bestaan van een neutraal element: er bestaat een element $e \in G$ zodat $x * e = x = e * x$ voor alle $x \in G$;

4) bestaan van inverse elementen: voor elk element $x \in G$ bestaat er een element $y \in G$ zodat $x * y = e = y * x$.

Een groep $G,*$ wordt **commutatief** (of **Abels**) genoemd indien $x * y = y * x$ voor alle $x, y \in G$.

Het **neutraal element** van de groep is uniek: stel immers dat er twee zo'n elementen e en e' zijn, dan is $e = e * e' = e'$ (de eerste gelijkheid gebruikt dat e' een neutraal element is; de tweede dat e een neutraal element is).
Bovendien is er maar één **invers element** van een element $x \in G$: stel dat zowel y als z voldoen aan de vierde voorwaarde, dan is $y = y * (x * z) = (y * x) * z = z$. We noteren het invers element van $x \in G$ door x^{-1}.
In groepen kan je rekenen. Bij niet-commutatieve groepen is de volgorde van de elementen van belang, maar mag je wel 'schrappen': als $x * y = x * z$, dan is $y = x^{-1} * (x * y) = x^{-1} * (x * z) = z$.

Voor eindige groepen $G,*$ kan je een tabel maken waarbij zowel de rijen als de kolommen overeenkomen met de elementen van G en waarbij het element in de rij bij $x \in G$ en in de kolom bij $y \in G$ gelijk is aan $x * y$. Zo'n tabel wordt de **Cayley-tabel** van de eindige groep genoemd. In deel 3.2 vind je hiervan enkele voorbeelden terug.

$*$	...	y	...
...	...	...	...
x	...	$x * y$	...
...	...	...	...

3.2 Voorbeelden

- *Getallenverzamelingen met optelling*: $\mathbb{Z},+;\ \mathbb{Q},+;\ \mathbb{R},+;\ \mathbb{C},+$
  Opmerking: het invers element wordt bij een groep met een optelling als bewerking genoteerd door $-x$ in plaats van x^{-1}.
  (tegenvoorbeeld: $\mathbb{N},+$)
- *Getallenverzameling met vermenigvuldiging*: $\mathbb{Q}_0,\cdot\ ; \mathbb{R}_0,\cdot\ ; \mathbb{C}_0,\cdot$
  (tegenvoorbeelden: $\mathbb{Z},\cdot\ ;\ \mathbb{Q},\cdot\ ;\ \mathbb{R},\cdot\ ;\ \mathbb{C},\cdot$)
- *n-tallen met optelling*: $\mathbb{R}^n,+$
- *Matrices met optelling*: $\mathbb{R}^{n\times m},+$
- *Inverteerbare vierkante matrices met vermenigvuldiging*
  (tegenvoorbeeld: vierkante matrices met vermenigvuldiging)
- *Gehele getallen modulo n met optelling*: $\mathbb{Z}_n,+$
  Uitleg: de verzameling $\mathbb{Z}_n$ bestaat uit n elementen $0,1,\dots,n-1$. Twee elementen $x, y \in \mathbb{Z}_n$ worden opgeteld door ze op te tellen als gehele getallen en dan de rest bij deling door n te nemen.
  Concreet voorbeeld: voor $n = 4$ wordt de Cayley-tabel gegeven door

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

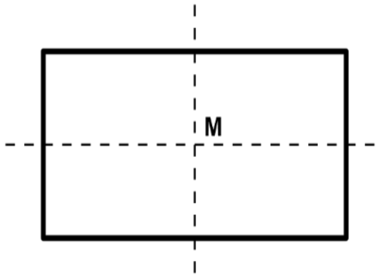
- *Viergroep van Klein*: $\{e, a, b, c\},*$ met Cayley-tabel gegeven door

$*$	e	a	b	c

e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

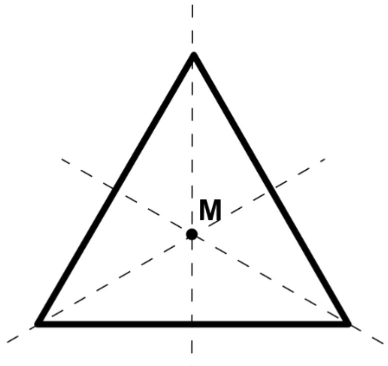
- *Permutaties met samenstelling*: $S_n, \circ$
  Uitleg: de verzameling S_n bestaat uit alle permutaties $\sigma: \{1, \dots n\} \to \{1, \dots, n\}$. De samenstelling van twee permutaties is terug een permutatie.
- *Symmetriegroepen*: voor een gegeven meetkundige figuur in het vlak kan je alle afstandbewarende transformaties (isometrieën) bekijken die de figuur invariant laten. Die transformaties geven aanleiding tot symmetrieën van de figuur en vormen een groep voor de samenstelling.

  Voorbeeld: rechthoek

  Zij S de spiegeling om de horizontale rechte door M, zij S' de spiegeling om de verticale rechte door M en zij S_M de puntspiegeling met centrum M. Dan wordt de symmetriegroep van de rechthoek gegeven door $\{Id, S, S', S_M\}$, waarbij Id de identieke transformatie is.

  Voorbeeld: gelijkzijdige driehoek

  Zij S de spiegeling om de verticale rechte door M en zij R de rotatie over 120° in wijzerzin rond M.
  De symmetriegroep van de gelijkzijdige driehoek bevat 6 elementen en wordt gegeven door $\{Id, R, R^2, S, SR, SR^2\}$, waarbij Id de identieke transformatie is en bv. R^2 de transformatie $R \circ \mathrm{R}$ is (m.a.w. de rotatie over 240°).
  Oefening: met welke van deze 6 elementen komt de transformatie RS overeen?

  Meer algemeen telt de symmetriegroep van een regelmatige n-hoek $2n$ elementen. Zo'n groep wordt een diëdergroep genoemd.

3.3 Aanverwante begrippen

3.3.1 *Orde van een element en van een groep*

Stel dat $G,*$ een groep is en $x \in G$ een element.

- We noteren $x^n = x * x * \dots * x$ waarbij in het rechterlid n keer het element x voorkomt.
  Als de groepsbewerking een optelling is, dan wordt de notatie $nx = x + \cdots + x$ gebruikt.
- De **orde** van x is gelijk aan het kleinste natuurlijke getal $n > 0$ zodat $x^n = x * x * \dots * x = e$.
  Indien zo'n getal n niet bestaat, dan zeggen we dat de orde van x gelijk is aan oneindig.
- De **orde** van de groep G is het aantal elementen van G.
- Indien een eindige groep een element bevat waarvan de orde gelijk is aan de orde van de groep, dan noemen we zo'n groep **cyclisch**.

Voorbeelden:

- De orde van $S_n,\circ$ is n faculteit.
- De orde van elk geheel getal verschillend van nul in $\mathbb{Z},+$ is oneindig; de orde van 0 zelf is 1.
- De orde van 0 in $\mathbb{Z}_4,+$ is 1; de orde van 1 en 3 in $\mathbb{Z}_4$ is 4; de orde van 2 in $\mathbb{Z}_4$ is 2.
- De orde van het element 1 in $\mathbb{Z}_n,+$ is n. De groep $\mathbb{Z}_n,+$ is dus cyclisch.
- De orde van e in de Viergroep van Klein is 1; de orde van de andere elementen is 2.

Oefeningen:

- Beschouw de permutatie p van $\{1,2,3,4,5\}$ met $p(1)=2, p(2)=1, p(3)=4, p(4)=5, p(5)=3$. Wat is de orde van $p \in S_5$?
- Geef voor $n>2$ een formule voor de orde van 2 in de groep $\mathbb{Z}_n,+$ in termen van n.
- Bepaal de ordes van alle elementen in $\mathbb{Z}_{10},+$.

3.3.2 Deelgroep

Beschouw een groep $G,*$ en $H \subset G$ niet-leeg.

- H is een **deelgroep** als H zelf een groep is voor de bewerking $*$.

In eerste instantie zou je dus moeten nagaan dat H voldoet aan de definitie met de vier voorwaarden uit deel 3.1. Het volstaat echter om na te gaan dat:

5) $x*y \in H$ voor alle $x,y \in H$;
6) $x^{-1} \in H$ voor alle $x \in H$.

Voorbeelden:

- $\mathbb{Z},+$ is een deelgroep van $\mathbb{Q},+$.
- De x-as is een deelgroep van $\mathbb{R}^2,+$.
- $\{0,2,4\}$ is een deelgroep van $\mathbb{Z}_6,+$.
- $\{1,-1,i,-i\}$ is een deelgroep van de eenheidscirkel $S=\{z \in \mathbb{C}: |z|=1\}$, die op zijn beurt een deelgroep is van de groep $\mathbb{C}_0,\cdot$.
- De vierkante matrices $M \in \mathbb{R}^{n\times n}$ met $det(M)=1$ vormen een deelgroep van de groep van alle inverteerbare vierkante matrices in $\mathbb{R}^{n\times n}$ met de vermenigvuldiging.

Oefeningen:

- Zoek verschillende deelgroepen van $\mathbb{Z},+$. Zou je ze allemaal kunnen geven?
- Bepaal alle deelgroepen van de Viergroep van Klein.
- Bepaal alle deelgroepen van $\mathbb{Z}_6,+$.
- Een belangrijk resultaat over deelgroepen van eindige groepen is de **stelling van Lagrange**: "*de orde van een deelgroep is een deler van de orde van de groep*". Controleer de stelling voor een aantal voorbeelden. Het bewijs van de stelling gebruikt het begrip nevenklasse van een groep en is dus relatief moeilijk.

3.3.3 Groepsmorfisme en isomorfe groepen

Zij $G,*$ en $H,\cdot$ twee groepen.

- Een afbeelding $f: G \to H$ is een **groepsmorfisme** als en slechts als $f(x*y)=f(x)\cdot f(y)$ voor alle $x,y \in G$, m.a.w. de afbeelding gedraagt zich goed t.o.v. de groepsbewerking.

Indien f een groepsmorfisme is, dan geldt ook dat $f(e_G) = e_H$ en $(f(x))^{-1} = f(x^{-1})$ voor alle $x \in G$.

- De twee groepen $G,*$ en $H,\cdot$ zijn **isomorf** als en slechts als er een groepsmorfisme $f: G \to H$ bestaat dat bijectief is.

Opmerking: om het te kunnen hebben over isomorfe groepen is het niet echt nodig om groepsmorfismes in te voeren. Meer informeel kan je stellen dat twee groepen isomorf zijn als ze 'gelijk zijn op naamsverandering van de elementen na'. Bij eindige groepen bijvoorbeeld kan je nagaan of de Cayley-tabellen overeenkomen. Isomorfe groepen hebben dezelfde eigenschappen, bv. ze hebben evenveel elementen van een bepaalde orde.

Voorbeelden:

- De afbeelding $f: \mathbb{Z} \to \mathbb{Z}: x \mapsto 2x$ is een groepsmorfisme, maar $g: \mathbb{Z} \to \mathbb{Z}: x \mapsto 2x + 1$ is dat niet.
- De symmetriegroep van een rechthoek is isomorf met de Viergroep van Klein. Je kan hiervoor bijvoorbeeld de afbeelding $f: \{Id, S, S', S_M\} \to \{e, a, b, c\}$ nemen met $f(Id) = e$, $f(S) = a$, $f(S') = b$ en $f(S_M) = c$.
- De afbeelding $\mathbb{R}^{n\times m} \to \mathbb{R}^{m\times n}: M \mapsto M^T$ die een matrix afbeeldt op zijn getransponeerde is een groepsisomorfisme.

Oefeningen:

- Stel dat $G,*$ een groep is van orde 3. Toon aan dat de groep isomorf is met $\mathbb{Z}_3, +$.
  Hint: stel dat $G = \{e, a, b\}$. Toon (door eliminatie) aan dat $ab = ba = e$, $a^2 = b$ en $b^2 = a$. De Cayley-tabel is dus als volgt:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

- Toon aan dat $\mathbb{Z}_4, +$ en de Viergroep van Klein niet isomorf zijn door de Cayley-tabellen te vergelijken. Dit zijn op isomorfisme na de enige twee groepen van orde 4. Met welke van deze twee groepen is de groep $\{1, -1, i, -i\},\cdot$ isomorf?

4 Vectorruimten

4.1 Wat is een vectorruimte?

Een **reële vectorruimte** $\mathbb{R}, V, +$ bestaat uit een niet-lege verzameling V, een optelling $+$ en een scalaire vermenigvuldiging $\cdot$ met reële getallen die voldoen aan de volgende voorwaarden :

1) $V, +$ is een commutatieve groep (zie deel 3.1, i.h.b. $v + w \in V$ voor alle $v, w \in V$);
2) $r \cdot v \in V$ voor alle $r \in \mathbb{R}$ en $v \in V$;
3) $r \cdot (s \cdot v) = (rs) \cdot v$ voor alle $r, s \in \mathbb{R}$ en $v \in V$;
4) $1 \cdot v = v \cdot 1 = v$ voor alle $v \in V$;
5) $r \cdot (v + w) = r \cdot v + r \cdot w$ voor alle $r \in \mathbb{R}$ en $v, w \in V$;
6) $(r + s) \cdot v = r \cdot v + s \cdot v$ voor alle $r, s \in \mathbb{R}$ en $v \in V$.

4.2 Voorbeelden

- *n-tallen*: $\mathbb{R}, \mathbb{R}^n, +$
- *Complexe getallen*: $\mathbb{R}, \mathbb{C}, +$
  Uitleg: de optelling in de vectorruimte is de optelling van complexe getallen; de scalaire vermenigvuldiging in de vectorruimte is de vermenigvuldiging van reële getallen met complexe getallen (wat complexe getallen oplevert).
- *Veeltermen*: $\mathbb{R}, \mathbb{R}[x], +$
- *Veeltermen van maximaal graad* n: $\mathbb{R}, \mathbb{R}[x]_{\leq n}, +$
- *Matrices*: $\mathbb{R}, \mathbb{R}^{n\times m}, +$
- *Oneindige rijen*: $\mathbb{R}, \mathbb{R}^\infty, +$ met $\mathbb{R}^\infty = \{(a_1, a_2, a_3, \dots) | a_i \in \mathbb{R}\}$
  Uitleg: zowel de optelling als de scalaire vermenigvuldiging gebeurt componentsgewijs:
  $(a_1, a_2, a_3, \dots) + (b_1, b_2, b_3, \dots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \dots)$ en
  $r \cdot (a_1, a_2, a_3, \dots) = (ra_1, ra_2, ra_3, \dots)$.
- *Reële functies*: $\mathbb{R}, \mathbb{R}^\mathbb{R}, +$ met $\mathbb{R}^\mathbb{R} = \{f | f: \mathbb{R} \to \mathbb{R} \text{ functie}\}$
  Uitleg: zowel de optelling $f + g$ als de scalaire vermenigvuldiging $r \cdot f$ is puntsgewijs:
  $(f + g)(x) = f(x) + g(x)$ en $(r \cdot f)(x) = r \cdot f(x)$ voor alle $x \in \mathbb{R}$.

4.3 Aanverwante begrippen

4.3.1 Lineaire combinatie, lineair (on)afhankelijk en voortbrengend

Gegeven is een vectorruimte $\mathbb{R}, \mathrm{V}, +$ en vectoren $v_1, \dots, v_n$.

- Een **lineaire combinatie** van de vectoren $v_1, \dots, v_n$ is een vector $v = r_1 \cdot v_1 + \dots + r_n \cdot v_n$ met $r_1, \dots, r_n$ reële getallen.
- De vectoren $v_1, \dots, v_n$ zijn **lineair onafhankelijk** als en slechts als voor elke lineaire combinatie $v = r_1 \cdot v_1 + \dots + r_n \cdot v_n$ geldt dat $v = 0$ impliceert dat $r_1 = \dots = r_n = 0$.
- De vectoren $v_1, \dots, v_n$ zijn **lineair afhankelijk** indien er reële getallen $r_1, \dots, r_n$ bestaan zodat $r_1 \cdot v_1 + \dots + r_n \cdot v_n = 0$ en zodat $r_1, \dots, r_n$ niet allen nul zijn.
- De vectoren $v_1, \dots, v_n$ zijn **voortbrengend** indien elke vector $v \in V$ kan geschreven worden als een lineaire combinatie $v = r_1 \cdot v_1 + \dots + r_n \cdot v_n$.

Voorbeelden:

- In een vectorruimte $\mathbb{R}, \mathrm{V}, +$ zijn een vector v en een veelvoud $v' = \mathrm{r} \cdot \mathrm{v}$ ervan lineair afhankelijk want $r \cdot v + (-1). v' = 0$.
- In $\mathbb{R}, \mathbb{R}^n, +$ zijn de vectoren $e_1 = (1,0, \dots,0), e_2 = (0,1, \dots,0), \dots, e_n = (0,0, \dots,1)$ zowel lineair onafhankelijk als voortbrengend. Een vector $v = (a_1, \dots, a_n)$ kan geschreven worden als de lineaire combinatie $v = a_1 \cdot e_1 + \dots + a_n \cdot e_n$.
- In $\mathbb{R}, \mathbb{R}^3, +$ zijn de vectoren $v_1 = (1,0,0), v_2 = (1,1,0), v_3 = (1,1,1)$ zowel lineair onafhankelijk als voortbrengend. De twee vectoren v_1 en v_2 zijn lineair onafhankelijk maar niet voortbrengend: de vector v_3 kan bijvoorbeeld niet geschreven worden als een lineaire combinatie van v_1 en v_2.
- De vectoren $1, i$ zijn zowel lineair onafhankelijk als voortbrengend voor $\mathbb{R}, \mathbb{C}, +$.

Oefeningen:

- Zijn de vectoren $(0,1), (1,2), (2,3)$ lineair onafhankelijk in de vectorruimte $\mathbb{R}, \mathbb{R}^2, +$? Zijn ze voortbrengend?

- Toon aan dat de veeltermen $1, x, x^2, \dots, x^n$ lineair onafhankelijk zijn in $\mathbb{R}, \mathbb{R}[x], +$, maar niet voortbrengend.

4.3.2 Basis en dimensie

Gegeven is een vectorruimte $\mathbb{R}, \mathrm{V}, +$ en $v_1, \dots, v_n \in V$.

- De verzameling $\{v_1, \dots, v_n\}$ is een basis van V als en slechts als ze lineair onafhankelijk en voortbrengend zijn. In dat geval zeggen we dat $v_1, \dots, v_n$ een basis vormen.
- Stel dat de vectorruimte $\mathbb{R}, \mathrm{V}, +$ een (eindige) basis $\{v_1, \dots, v_n\}$ heeft. Men kan aantonen dat elke andere basis dan ook n elementen heeft. Het getal n wordt de **dimensie** van de vectorruimte genoemd. Indien $\mathbb{R}, \mathrm{V}, +$ geen eindige basis heeft, dan zeggen we dat ze **dimensie oneindig** heeft.
- Als de vectoren $v_1, \dots, v_n$ een basis vormen en $v \in V$, dan kunnen we de vector v schrijven als een unieke lineaire combinatie $v = r_1 \cdot v_1 + \cdots + r_n \cdot v_n$. We noemen $(r_1, \dots, r_n) \in \mathbb{R}^n$ de **coördinaatsvector** en de getallen $r_1, \dots, r_n$ de **coördinaten** van v. Deze hangen af van de gekozen basis.

Voorbeelden:

- De vectoren $e_1, \dots, e_n$ vormen een basis van $\mathbb{R}, \mathbb{R}^n, +$, dus is de dimensie n. Ten opzichte van deze basis is de coördinaatsvector van $v = (a_1, \dots, a_n) \in \mathbb{R}^n$ gelijk aan $(a_1, \dots, a_n)$. Daarom wordt de basis ook de natuurlijke basis van $\mathbb{R}^n$ genoemd.
- Omdat $1 \cdot (1{,}0) + 2 \cdot (0{,}1) = (1{,}2) = 3 \cdot (1{,}0) + (-2) \cdot (1, -1)$ is de coördinaatsvector van $(1{,}2)$ t.o.v. de natuurlijke basis $\{(1{,}0), (0{,}1)\}$ gelijk aan $(1{,}2)$ en ten opzichte van de basis $\{(1{,}0), (1, -1)\}$ gelijk aan $(3, -2)$. Hoewel de vector $(1{,}0)$ deel uitmaakt van beide basissen zijn beide coördinaten verschillend.
- De vectoren $1, i$ vormen een basis van $\mathbb{R}, \mathbb{C}, +$, dus is de dimensie 2. De coördinaatsvector van $a + bi$ is $(a, b) \in \mathbb{R}^2$.
- De vectoren $1, x, x^2, \dots, x^n$ vormen een basis van $\mathbb{R}, \mathbb{R}[x]_{\leq n}, +$, dus is de dimensie $n + 1$.

Oefeningen:

- Beschouw vectoren $v_1 = (a_{1,1}, \dots, a_{n,1}), \dots, v_n = (a_{1,n}, \dots, a_{n,n}) \in \mathbb{R}^n$. Toon aan dat de vectoren $v_1, \dots, v_n$ een basis vormen van $\mathbb{R}, \mathbb{R}^n, +$ als en slechts als de vierkante matrix $M = (a_{i,j}) \in \mathbb{R}^{n \times n}$ inverteerbaar is (m.a.w. $det(M) \neq 0$).
- Toon aan dat $\mathbb{R}, \mathbb{R}^{n \times m}, +$ dimensie nm heeft.
- Toon (m.b.v. een bewijs uit het ongerijmde) aan dat $\mathbb{R}, \mathbb{R}[x], +$ dimensie oneindig heeft.

4.3.3 Lineaire deelruimte

Gegeven is een vectorruimte $\mathbb{R}, \mathrm{V}, +$ en $W \subset V$ niet-leeg.

- W is een lineaire deelruimte van V als en slechts als $\mathbb{R}, \mathrm{W}, +$ een vectorruimte is.

Om te checken of een deelverzameling W een lineaire deelruimte is, volstaat het om de volgende voorwaarden na te gaan:

7) $w + w' \in W$ voor alle $w, w' \in W$;
8) $r \cdot w \in W$ voor alle $r \in \mathbb{R}$ en $w \in W$.

Voorbeelden:

- Alle rechten door de oorsprong zijn lineaire deelruimtes van $\mathbb{R}, \mathbb{R}^2, +$. Rechten die niet door de oorsprong gaan zijn dat niet.
- De verzameling van alle diagonaalmatrices is een lineaire deelruimte van $\mathbb{R}, \mathbb{R}^{n \times n}, +$.

Oefeningen:

- Stel dat $\mathbb{R}, \mathrm{V}, +$ een vectorruimte is en neem $v_1, \ldots, v_n \in V$. Toon aan dat alle lineaire combinaties van de vectoren $v_1, \ldots, v_n$ een lineaire deelruimte vormen. Deze deelruimte wordt doorgaans genoteerd door $< v_1, \ldots, v_n >$.
- Vormen alle reële functies f met $f(0) = 3$ een deelruimte van $\mathbb{R}, \mathbb{R}^{\mathbb{R}}, +$? Wat met alle reële functies f met $f(3) = 0$?
- *Voor de geïnteresseerden in differentiaalvergelijkingen*: toon aan dat alle oplossingen van een homogene lineaire differentiaalvergelijking een deelruimte vormen van $\mathbb{R}, \mathbb{R}^{\mathbb{R}}, +$.

4.3.4 Lineaire afbeelding

Zij $\mathbb{R}, \mathrm{V}, +$ en $\mathbb{R}, \mathrm{W}, +$ twee reële vectorruimtes.

- Een afbeelding $f: V \to W$ is een **lineaire afbeelding** als en slechts als $f(v + v') = f(v) + f(v')$ voor alle $v, v' \in V$ en $f(r \cdot v) = r \cdot f(v)$ voor alle $v \in V$ en $r \in \mathbb{R}$, m.a.w. de afbeelding gedraagt zich goed t.o.v. de optelling en de scalaire vermenigvuldiging van vectoren.

Voorbeelden:

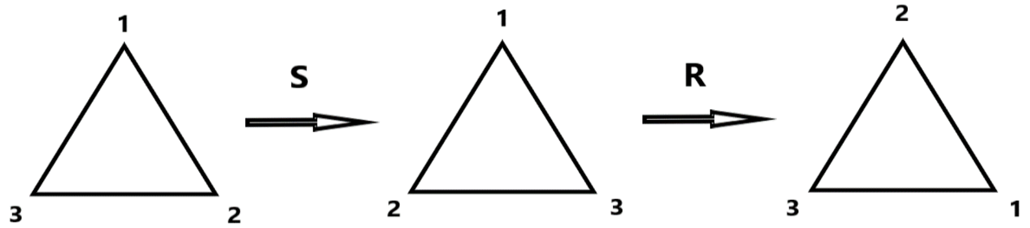
- De afbeelding $f: \mathbb{R}^2 \to \mathbb{R}^2: (x, y) \mapsto (x + 2y, 3x + 4y)$ is een lineaire afbeelding.
- Elke afbeelding van de vorm $f: \mathbb{R}^n \to \mathbb{R}^m: v \mapsto Av$, met $A \in \mathbb{R}^{m \times n}$ en waarbij de vector v als een kolommatrix wordt bekeken, is een lineaire afbeelding. Omgekeerd is elke lineaire afbeelding $f: \mathbb{R}^n \to \mathbb{R}^m$ van deze vorm: in de kolommen van de matrix A staan precies de beelden $f(e_1), \ldots, f(e_n)$.
- De afbeelding $\frac{d}{dx}: \mathbb{R}[x] \to \mathbb{R}[x]$ die een veelterm afbeeldt op zijn afgeleide is lineair.
- De afbeelding $\mathbb{C} \to \mathbb{C}: a + bi \mapsto a - bi$ die een complex getal afbeeldt op zijn complex toegevoegde is een lineaire afbeelding van de reële vectorruimte $\mathbb{R}, \mathbb{C}, +$ naar zichzelf.

Met vragen en bemerkingen over dit document kun je terecht bij jouw vakbegeleider wiskunde.

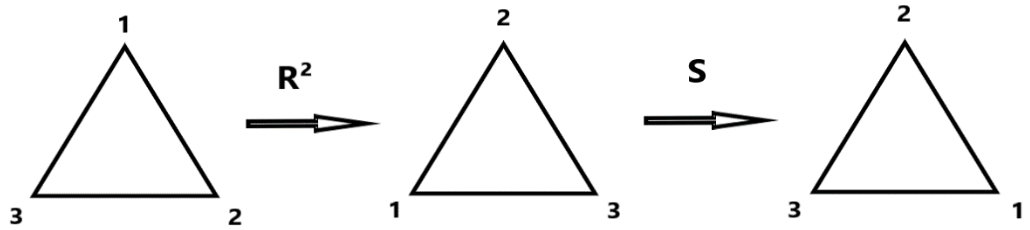
5 Oplossingen oefeningen

5.1 Oefeningen bij deel groepen

- Bij het voorbeeld (deel 3.2) van de symmetriegroep van een gelijkzijdige driehoek: met welke van deze 6 elementen komt de transformatie RS overeen?
Oplossing: om de transformaties visueel te maken is het handig om de hoekpunten van de driehoek te benoemen (bv. met de getallen $1,2,3$). De transformatie $RS = R \circ S$ komt overeen met:



Het hoekpunt 1 wordt door de transformatie RS dus afgebeeld op het hoekpunt 2. We kunnen alle transformaties zo voorstellen, i.h.b. de transformaties Id, R, R^2, S, SR, SR^2. Het blijkt dat RS overeenkomt met SR^2 (de groep is dus niet commutatief):



Extra uitleg: de gelijkheid $RS = SR^2$ kan dan ook gebruikt worden om de Cayley-tabel verder op te stellen. Zo is $SR \circ SR = SRSR = S(RS)S = S(SR^2)R = S^2R^3 = Id \circ Id = Id$.
De Cayley-tabel wordt gegeven door:

$\circ$	Id	R	R^2	S	SR	SR^2
Id	Id	R	R^2	S	SR	SR^2
R	R	R^2	Id	SR^2	S	SR
R^2	R^2	Id	R	SR	SR^2	S
S	S	SR	SR^2	Id	R	R^2
SR	SR	SR^2	S	R^2	Id	R
SR^2	SR^2	S	SR	R	R^2	Id

- Beschouw de permutatie p van $\{1,2,3,4,5\}$ met $p(1) = 2, p(2) = 1, p(3) = 4, p(4) = 5, p(5) = 3$. Wat is de orde van $p \in S_5$?
Oplossing: we bepalen opeenvolgende machten $p^2, p^3, \dots$ van de permutatie p tot we een macht p^n tegenkomen die samenvalt met de identieke afbeelding.
    - $p^2(1) = 1, p^2(2) = 2, p^2(3) = 5, p^2(4) = 3, p^2(5) = 4$
    - $p^3(1) = 2, p^3(2) = 1, p^3(3) = 3, p^3(4) = 4, p^3(5) = 5$
    - $p^4(1) = 1, p^4(2) = 2, p^4(3) = 4, p^4(4) = 5, p^4(5) = 3$
    - $p^5(1) = 2, p^5(2) = 1, p^5(3) = 5, p^5(4) = 3, p^5(5) = 4$
    - $p^6(1) = 1, p^6(2) = 2, p^6(3) = 3, p^6(4) = 4, p^6(5) = 5$

  De orde van $p \in S_5$ is dus 6.
- Geef voor $n > 2$ een formule voor de orde van 2 in de groep $\mathbb{Z}_n, +$ in termen van n.
Oplossing: de orde van 2 in de groep $\mathbb{Z}_n, +$ hangt af van het al dan niet even zijn van n. Als n even is, dan is de orde gelijk aan $n/2$; als n oneven is, dan is de orde gelijk aan n.
- Bepaal de ordes van alle elementen in $\mathbb{Z}_{10}, +$.

Oplossing: de orde van het element 0 is 1; de orde van de elementen $1,3,7,9$ is 10; de orde van de elementen $2,4,6,8$ is 5; de orde van het element 5 is 2.

- Zoek verschillende deelgroepen van $\mathbb{Z},+$. Zou je ze allemaal kunnen geven?
  Oplossing: voor elk natuurlijk getal $n \in \mathbb{N}$ is $n\mathbb{Z},+$ een deelgroep (voor $n = 0$ en $n = 1$ krijg je de triviale deelgroepen $\{0\},+$ en $\mathbb{Z},+$). We kunnen aantonen dat elke deelgroep $H \subset \mathbb{Z}$ van deze vorm is. Als $H = \{0\}$, dan is $n = 0$. Als $H \neq \{0\}$, neem dan n het kleinste natuurlijk getal verschillend van nul dat behoort tot H. Omdat H een deelgroep is, volgt de inclusie $n\mathbb{Z} \subset H$ direct. Om de andere inclusie $H \subset n\mathbb{Z}$ aan te tonen, neem $m \in H$ willekeurig en zij r de rest bij deling van m door n. Omdat r van de vorm $m - qn$ is voor een geheel getal q, is ook $r \in H$. Bovendien geldt dat $0 \leq r < n$. Dus moet $r = 0$ (anders in tegenspraak met de keuze van n), waaruit volgt dat $m \in n\mathbb{Z}$.
- Bepaal alle deelgroepen van de Viergroep van Klein.
  Oplossing: de deelgroepen zijn $\{e\}, \{e,a\}, \{e,b\}, \{e,c\}, \{e,a,b,c\}$. Er zijn dus geen deelgroepen met drie elementen: als twee van de drie elementen a,b,c tot een deelgroep behoort, dan moet ook het derde element tot de deelgroep behoren.
- Bepaal alle deelgroepen van $\mathbb{Z}_6,+$.
  Oplossing: de deelgroepen zijn $\{0\}, \{0,3\}, \{0,2,4\}, \{0,1,2,3,4,5\}$.
- Een belangrijk resultaat over deelgroepen van eindige groepen is de **stelling van Lagrange**: "*de orde van een deelgroep is een deler van de orde van de groep*". Controleer de stelling voor een aantal voorbeelden. Het bewijs van de stelling gebruikt het begrip nevenklasse van een groep en is dus relatief moeilijk.
  Oplossing: de Viergroep van Klein van orde 4 heeft enkel deelgroepen van orde 1, 2 en 4; de groep $\mathbb{Z}_6,+$ van orde 6 heeft enkel deelgroepen van orde 1, 2, 3 en 6.
- Stel dat $G,*$ een groep is van orde 3. Toon aan dat de groep isomorf is met $\mathbb{Z}_3,+$.
  Hint: stel dat $G = \{e,a,b\}$. Toon (door eliminatie) aan dat $ab = ba = e$, $a^2 = b$ en $b^2 = a$. De Cayley-tabel is dus als volgt:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

  Oplossing: we volgen de hint van hierboven. Als $ab = a$, dan volgt dat $b = e$, een contradictie; als $ab = b$, dan volgt dat $a = e$, een contradictie. Bijgevolg is $ab = e$ en analoog volgt ook $ba = e$. Als $a^2 = e$, dan is $a^2 = ab$ waaruit volgt dat $a = b$, een contradictie; als $a^2 = a$, dan volgt dat $a = e$, een contradictie. Bijgevolg is $a^2 = b$. Analoog kunnen we ook de gelijkheid $b^2 = a$ aantonen. De Cayley-tabel kan nu volledig ingevuld worden. De afbeelding $f: G = \{e,a,b\} \to \mathbb{Z}_3 = \{0,1,2\}$ met $f(e) = 0, f(a) = 1, f(b) = 2$ is een isomorfisme.
- Toon aan dat $\mathbb{Z}_4,+$ en de Viergroep van Klein niet isomorf zijn door de Cayley-tabellen te vergelijken. Dit zijn op isomorfisme na de enige twee groepen van orde 4. Met welke van deze twee groepen is de groep $\{1,-1,i,-i\},\cdot$ isomorf?
  Oplossing: de Cayley-tabellen van $\mathbb{Z}_4,+$ en van de Viergroep van Klein zijn:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Er zijn bij $\mathbb{Z}_4, +$ twee elementen met orde twee (m.a.w. met het neutraal element 0 op de diagonaal); bij de Viergroep van Klein zijn er dat vier. De twee groepen kunnen dus niet isomorf zijn. De Cayley-tabel van $\{1, -1, i, -i\}, \cdot$ wordt gegeven door:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	-1
$-i$	$-i$	i	1	-1

Hier zijn er, net zoals bij de groep $\mathbb{Z}_4, +$, twee elementen met orde twee. De groepen $\{1, -1, i, -i\}, \cdot$ en $\mathbb{Z}_4, +$ zijn ook isomorf: de afbeelding $f: \mathbb{Z}_4 \to \{1, -1, i, -i\}$ met $f(0) = 1, f(1) = i, f(2) = -1, f(3) = -i$ is een isomorfisme.

5.2 Oefeningen bij deel vectorruimten

- Zijn de vectoren $(0,1), (1,2), (2,3)$ lineair onafhankelijk in de vectorruimte $\mathbb{R}, \mathbb{R}^2, +$? Zijn ze voortbrengend?
  Oplossing: de vectoren zijn lineair afhankelijk, want $2 \cdot (1,2) = (2,4) = (0,1) + (2,3)$ en dus $(-1) \cdot (0,1) + 2 \cdot (1,2) + (-1) \cdot (2,3) = (0,0)$. De vectoren zijn wel voortbrengend, want $(x, y) = (y - 2x) \cdot (0,1) + x \cdot (1,2) + 0 \cdot (2,3)$ voor alle $x, y \in \mathbb{R}$.
- Toon aan dat de veeltermen $1, x, x^2, \dots, x^n$ lineair onafhankelijk zijn in $\mathbb{R}, \mathbb{R}[x], +$, maar niet voortbrengend.
  Oplossing: als $a_0 \cdot 1 + a_1 \cdot x + \dots + a_n \cdot x^n = 0$, dan moeten alle coëfficiënten $a_i = 0$. De vectoren zijn dus lineair onafhankelijk. De vectoren zijn niet voortbrengend, want bijvoorbeeld de veelterm x^{n+1} is niet te schrijven als een lineaire combinatie.
- Beschouw vectoren $v_1 = \left(a_{1,1}, \dots, a_{n,1}\right), \dots, v_n = \left(a_{1,n}, \dots, a_{n,n}\right) \in \mathbb{R}^n$. Toon aan dat de vectoren $v_1, \dots, v_n$ een basis vormen van $\mathbb{R}, \mathbb{R}^n, +$ als en slechts als de vierkante matrix $M = \left(a_{i,j}\right) \in \mathbb{R}^{n \times n}$ inverteerbaar is (m.a.w. $det(M) \neq 0$).
  Oplossing: een vector $v = (b_1, \dots, \mathrm{b_n})$ kan geschreven worden als een lineaire combinatie van de vectoren $v_1, \dots, \mathrm{v_n}$ als en slechts als het stelsel $MX = B$ een oplossing heeft, waarbij B de kolommatrix $(b_1 \;\dots\; \mathrm{b_n})^T$ is. Het stelsel $MX = B$ heeft voor elke kolommatrix B een oplossing als en slechts als M inverteerbaar is.
- Toon aan dat $\mathbb{R}, \mathbb{R}^{n \times m}, +$ dimensie nm heeft.
  Oplossing: voor elke $i \in \{1, \dots, n\}$ en $j \in \{1, \dots, m\}$ kan je de matrix $E_{i,j}$ beschouwen met een 1 op de i-de rij en j-de kolom en elders overal nullen. Deze matrices vormen een basis: elke matrix $M = \left(a_{i,j}\right)$ kan geschreven worden als de lineaire combinatie $\sum_{i,j} a_{i,j} \cdot E_{i,j}$.
- Toon (m.b.v. een bewijs uit het ongerijmde) aan dat $\mathbb{R}, \mathbb{R}[x], +$ dimensie oneindig heeft.
  Oplossing: stel dat de vectorruimte eindige dimensie heeft. Neem een (eindige) basis $v_1, \dots, v_n$ en stel m het maximum van de graden van de veeltermen in de basis. De veelterm x^{m+1} kan niet geschreven worden als een lineaire combinatie van de veeltermen $v_1, \dots, v_n$, dus zijn de veeltermen niet voortbrengend.
- Stel dat $\mathbb{R}, \mathrm{V}, +$ een vectorruimte is en neem $v_1, \dots, v_n \in V$. Toon aan dat alle lineaire combinaties van de vectoren $v_1, \dots, v_n$ een lineaire deelruimte vormen. Deze deelruimte wordt doorgaans genoteerd door $< v_1, \dots, v_n >$.
  Oplossing: de som van twee lineaire combinaties $a_1 \cdot v_1 + \dots + a_n \cdot v_n$ en $b_1 \cdot v_1 + \dots + b_n \cdot v_n$ is een lineaire combinatie $(a_1 + b_1) \cdot v_1 + \dots + (a_n + b_n) \cdot v_n$; het scalair product van een lineaire combinatie $a_1 \cdot v_1 + \dots + a_n \cdot v_n$ met een reëel getal r is een lineaire combinatie $(ra_1) \cdot v_1 + \dots + (ra_n) \cdot v_n$. De twee voorwaarden zijn dus voldaan.

- Vormen alle reële functies f met $f(0) = 3$ een deelruimte van $\mathbb{R}, \mathbb{R}^{\mathbb{R}}, +$? Wat met alle reële functies f met $f(3) = 0$?
  Oplossing: als f en g reële functies zijn met $f(0) = g(0) = 3$, dan is $(f+g)(0) = f(0) + g(0) = 6$. De reële functies f met $f(0) = 3$ vormen dus geen deelruimte. De reële functies f met $f(3) = 0$ vormen wel een lineaire deelruimte: indien $f(3) = g(3) = 0$, dan is $(f+g)(3) = f(3) + g(3) = 0$ en $(r \cdot f)(3) = rf(3) = 0$.
- Voor de geïnteresseerden in differentiaalvergelijkingen: toon aan dat alle oplossingen van een homogene lineaire differentiaalvergelijking een deelruimte vormen van $\mathbb{R}, \mathbb{R}^{\mathbb{R}}, +$.
  Oplossing: een homogene lineaire differentiaalvergelijking is van de vorm $c_n(x)y^{(n)} + \cdots + c_1(x)y^{(1)} + c_0(x)y = 0$, waarbij de c_i veeltermen zijn in x en $y^{(i)}$ de i-de afgeleide is van de functie y. Indien y_1 en y_2 oplossingen zijn, dan is ook $y_1 + y_2$ een oplossing:
  $c_n(x)(y_1 + y_2)^{(n)} + \cdots + c_1(x)(y_1 + y_2)^{(1)} + c_0(x)(y_1 + y_2) = (c_n(x){y_1}^{(n)} + \cdots + c_1(x){y_1}^{(1)} + c_0(x)y\_1) + (c_n(x){y_2}^{(n)} + \cdots + c_1(x){y_2}^{(1)} + c_0(x)y\_2) = 0 + 0 = 0.$
  Analoog is ook ry een oplossing indien y een oplossing is. De oplossingen vormen dus een deelruimte.