Fundamenten

Lerarenprogramma Mastermath, versie 2015/12/02

Theo van den Bogaart

Bas Edixhoven

Inhoudsopgave

Voorwoord

Dit is het dictaat van het vak “Fundamenten”, een van de zeven vakken voor leraren in Mastermath. Dit pakket van vakken is ontstaan uit een initiatief van Mastermath (het samenwerkingsverband van de Nederlandse universitaire wiskundeopleidingen dat een nationaal aanbod van mastervakken verzorgt) en de Nederlandse vakdidactici in de wiskunde om actie te ondernemen tegen het tekort aan eerstegraads docenten. Academici met een mastertitel in een bètarichting anders dan wiskunde kunnen door het volgen van een aantal van deze vakken voldoen aan de vakinhoudelijke toelatingseisen van de universitaire lerarenopleidingen. Ook voor de hbo-opleiding tot eerstegraads wiskundedocent is de tekst bruikbaar. Meer informatie over dit programma is te vinden op `http://www.mastermath.nl`.

Dit vak “Fundamenten” heeft als doel het leggen van een stevige fundering voor de overige zes vakken, en tegelijkertijd uit te leggen hoe de hedendaagse wiskunde is opgebouwd. Het gaat dus niet over het leren van rekenvaardigheden, maar meer over het begrijpen van de theorie daarachter, in het bijzonder het leren omgaan met definities, stellingen en bewijzen. Na enige voorbereidingen over verzamelingen, afbeeldingen en logica, worden de getalssystemen van natuurlijke, gehele, rationale, reële en complexe getallen axiomatisch ingevoerd, en dus exact beschreven. Vervolgens worden reële functies en rijen, continuïteit en limieten bestudeerd. Dan volgen een axiomatische behandeling van de complexe getallen en een constructie ervan. Tot slot wordt een deel van de lineaire algebra behandeld vanuit een wiskundig, structureel perspectief.

We volgen een logische opbouw vanuit verzamelingenleer en natuurlijke getallen, waarbij we in de appendices zelfs verder teruggaan tot de ZFC-axioma’s. Ten behoeve van de didactiek doen we echter ook geregeld concessies aan deze logische opbouw, met name door in de voorbeelden al vanaf het begin veel ‘overbekende’ voorbeelden de revue te laten passeren.

Tegelijk met dit alles proberen we zowel de schoonheid als het belang van zuivere wiskunde over te brengen, alsook wat historisch besef. We proberen voorbeelden te geven van spannende onderwerpen voor in de klas en bruggetjes te slaan tussen de wiskunde in deze tekst en wiskunde in het voortgezet onderwijs.

Het dictaat eindigt met een index. Daarvoor staan er antwoorden en uitwerkingen van sommige opgaven (dit wordt aangegeven met het symbool ✍). De uitwerkingen zijn soms beperkt tot een aantal aanwijzingen.

Alle commentaar, maar liefst wel constructief, is welkom (liefst per e-mail aan één van de docenten).

Actuele informatie over dit college zal te vinden zijn op het websysteem van Mastermath.

Theo van den Bogaart
Bas Edixhoven

Verantwoording bronmateriaal

Veel van het materiaal in dit dictaat is afkomstig van het dictaat gebruikt bij het Delfts-Leidse college “Wiskundige Structuren”, geschreven door Eva Coplakova, Bas Edixhoven, Lenny Taelman en Mark Veraar. Ook zijn delen afkomstig uit het Leidse college “Caleidoscoop” van Hans Finkelnberg. Het probleem van de honderd smurfen en Lights out is deel van de wiskunde-folklore, we hebben het niet zelf bedacht. Van het hoofdstuk over lineaire algebra komt een deel van het materiaal

over rij-operaties en het oplossen van lineaire vergelijkingen uit het Leidse college “Lineaire algebra I” van Ronald van Luijk.

I VERZAMELINGEN EN AFBEELDINGEN

Het begrip verzameling kennen we uit het dagelijks leven: een bibliotheek bevat een verzameling van boeken, een museum een verzameling van kunstvoorwerpen. We kennen verzamelingen ook uit de wiskunde: de verzameling van alle getallen, de verzameling van alle punten in het platte vlak, de verzameling van alle oplossingen van een vergelijking; het blijkt dat je heel de wiskunde kunt formuleren in termen van verzamelingenleer. Verzamelingen en hun eigenschappen zijn onderwerp van een breed wiskundig gebied — de verzamelingenleer.

Ongeveer honderd jaar geleden begonnen wiskundigen met een groot enthousiasme verzamelingen overal te gebruiken: het was heel handig elementen die een bepaalde eigenschap hadden als een geheel te beschouwen: een verzameling. Maar heel snel ontstonden problemen: sommige eigenschappen leidden tot tegenspraken wanneer de elementen die aan die eigenschap voldoen in een verzameling worden gevat. Men stuitte op paradoxen. Blijkbaar kunnen niet alle eigenschappen gebruikt worden om verzamelingen te vormen.

Paradoxen

We zullen twee van die tegenspraken bekijken.

I.0.1 Voorbeeld. Paradox van Russell In een dorp woont kapper Hans die alléén die mannen uit het dorp scheert die zichzelf niet scheren. Bekijk nu de verzameling A van alle mannen die door kapper Hans worden geschoren. Dit lijkt een goed gedefinieerde verzameling, maar er bestaan problemen zodra je gaat onderzoeken of kapper Hans zelf, immers ook een man, in verzameling A zit.

Het is duidelijk dat er twee mogelijkheden zijn: kapper Hans scheert zichzelf of hij scheert zichzelf niet. Als hij zichzelf scheert dan scheert de kapper hem niet, maar hij zelf is de kapper, dus hij kan zichzelf niet scheren. Aan de andere kant, als hij zichzelf niet scheert dan moet hij, de kapper, zichzelf toch scheren. We zien dat geen van de mogelijkheden mogelijk is, we krijgen een paradox. ∎

I.0.2 Voorbeeld. Paradox van Berry Een van de basiseigenschappen van natuurlijke getallen is dat elke niet-lege verzameling natuurlijke getallen een kleinste element bevat. Beschouw nu alle natuurlijke getallen die beschreven kunnen worden in het Nederlands met behulp van ten hoogste honderd letters. Het Nederlandse alfabet heeft 26 letters, dus met behulp van honderd letters of minder kunnen we ten hoogste $26 + 26^2 + 26^3 + \cdots + 26^{100}$ getallen beschrijven (dit is een heel ruime bovengrens: niet elke lettercombinatie is zinvol, en ook niet elke zinvolle combinatie van letters beschrijft een natuurlijk getal). Er zijn oneindig veel natuurlijke getallen, dus de verzameling getallen die niet met honderd letters of minder te beschrijven zijn is ook oneindig en dus zeker niet leeg. Deze verzameling bevat dus een kleinste element. Zij n het kleinste natuurlijke getal dat niet met

honderd letters of minder te beschrijven is. Maar we hebben n net met minder dan honderd letters beschreven! ∎

Om paradoxen te vermijden moeten we voorzichtig zijn met wat we verzameling zullen noemen: niet elke collectie mag een verzameling zijn.

Er zijn vaste axioma's (grondregels) ingevoerd die het bestaan van sommige verzamelingen garanderen en beschrijven hoe we nieuwe verzamelingen uit oude kunnen maken, welke operaties met verzamelingen zijn toegestaan en welke eigenschappen ze hebben. Uitgaande van de axioma's en met behulp van logica kunnen we verdere eigenschappen van verzamelingen bewijzen. We zullen nu niet diep in de axioma's duiken, want we zullen ons concentreren op het werken met verzamelingen. We zullen operaties met verzamelingen definiëren en de belangrijkste eigenschappen afleiden. Een volledige lijst van axioma's voor de verzamelingenleer is te vinden in Appendix VIII.2. Na hoofdstuk II zullen we voldoende gevorderd zijn om te begrijpen wat daar staat.

I.1 Notatie

Verzamelingen bevatten elementen; als A een verzameling is en x een element van A dan schrijven we[1]

$$x \in A.$$

Om aan te geven dat y *geen* element van A is schrijven we

$$y \notin A.$$

We gebruiken de notatie $\{1\}$ voor de verzameling die alleen het getal 1 bevat, $\{1,2\}$ is een verzameling die precies twee elementen bevat, namelijk de getallen 1 en 2. De verzameling $\{a,b,c,d,e\}$ heeft minstens één en hoogstens vijf elementen: het hangt ervan af hoeveel gelijkheden er gelden tussen de niet gespecificeerde elementen a,b,c,d,e. De verzameling die geen elementen bevat heet de *lege verzameling* en wordt genoteerd als $\varnothing$.

Elementen van een verzameling kunnen ook verzamelingen zijn, bijvoorbeeld $A = \{3,\{2\},\{4,5\}\}$ heeft elementen 3, $\{2\}$ en $\{4,5\}$. Er geldt dus $3 \in A$ maar $2 \notin A$; er geldt echter $\{2\} \in A$.

In de wiskunde zijn verzamelingen die getallen als elementen bevatten van groot belang. We gebruiken de letter $\mathbb{N}$ voor de verzameling van alle natuurlijke getallen: $\mathbb{N} = \{0,1,2,3,\ldots\}$,[2] $\mathbb{Z} = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$ voor de verzameling van alle gehele getallen, $\mathbb{Q}$ voor de verzameling van alle breuken p/q met $p,q \in \mathbb{Z}$ en $q \neq 0$, $\mathbb{R}$ voor de verzameling van alle reële getallen en $\mathbb{C}$ voor de verzameling van alle complexe getallen. Uiteindelijk zullen we deze getalsystemen exact beschrijven door middel van gegevens en eigenschappen, en, uitgaande van $\mathbb{N}$, constructies geven van $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$. Tot het zover is gaan we op een informele manier met deze getalsystemen om.

Als A een verzameling is dan wordt de verzameling van alle elementen uit A die een eigenschap E hebben als volgt genoteerd: $\{x \in A : E(x)\}$.

I.1.1 Voorbeeld.

[1] Verzamelingen worden vaak, maar niet altijd, met behulp van hoofdletters genoteerd en hun elementen met behulp van kleine letters. We zullen ook verzamelingen tegenkomen waarvan de elementen weer verzamelingen zijn.

[2] Pas op, er zijn auteurs die $\mathbb{N}$ anders definiëren, namelijk $\{1,2,3,\ldots\}$. Een goede alternatieve notatie voor $\mathbb{N}$ is $\mathbb{Z}_{\geq 0}$; deze maakt meteen duidelijk dat $0 \in \mathbb{N}$.

(i) De verzameling $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$ is de verzameling van alle positieve reële getallen. Deze verzameling is niet leeg want $5 \in \mathbb{R}_{>0}$. Daarentegen is $\{x \in \mathbb{R} : x > 5 \text{ en } x < 2\}$ leeg, want er bestaat geen reëel getal dat tegelijk groter dan 5 en kleiner dan 2 is.

(ii) De verzameling van alle reële oplossingen van de vergelijking $\sin(\pi x) = 0$ kunnen we kort als volgt schrijven: $A = \{x \in \mathbb{R} : \sin(\pi x) = 0\}$. Analoog, de verzameling $B = \{x \in \mathbb{R} : \cos(\pi x/2) = 0\}$ is de verzameling van alle oplossingen van de vergelijking $\cos(\pi x/2) = 0$.

I.1.2 Axioma. Twee verzamelingen zijn *aan elkaar gelijk* als ze dezelfde elementen hebben, dat wil zeggen, $A = B$ als ieder element van A element van B is, en ieder element van B element van A.

I.1.3 Definitie. Als elk element van A element van B is zeggen we dat A een *deelverzameling* van B is.
Notatie:[3] $A \subseteq B$.

Hieruit volgt dat $A = B$ equivalent is met:[4] $A \subseteq B$ én $B \subseteq A$.

I.1.4 Voorbeeld.

(i) De verzamelingen $A = \{1,2,3\}$ en $B = \{3,3,3,2,2,1\}$ hebben dezelfde elementen en zijn dus aan elkaar gelijk. We kunnen schrijven: $A = B$.

(ii) Beschouw de verzamelingen A en B uit Voorbeeld I.1.1 (ii). Als x een geheel getal is dan is $\sin(\pi x) = 0$; dit betekent dat $\mathbb{Z} \subseteq A$. Aan de andere kant, als $\sin(\pi x) = 0$ dan moet x een geheel getal zijn; dit betekent dat $A \subseteq \mathbb{Z}$. We hebben bewezen $A = \mathbb{Z}$: de verzameling van alle oplossingen van de vergelijking $\sin(\pi x) = 0$ is de verzameling van alle gehele getallen.

(iii) Analoog kunnen we bewijzen dat alle oplossingen van $\cos(\pi x/2) = 0$ de verzameling van alle oneven gehele getallen is: $B = \{2k+1 : k \in \mathbb{Z}\}$.[5]

(iv) De verzamelingen $A = \{0,\{1,2,3\},4\}$ en $B = \{0,1,\{2,3\},4\}$ zijn niet aan elkaar gelijk. Immers $1 \notin A$ en $1 \in B$.

Intervallen

I.1.5 Voorbeeld. Belangrijke deelverzamelingen van de reële rechte (de verzameling van alle reële getallen) zijn intervallen. We onderscheiden begrensde en onbegrensde intervallen.

(i) **Begrensde intervallen:** Voor $a, b \in \mathbb{R}$ is $(a,b) = \{x \in \mathbb{R} : a < x < b\}$ een *open interval*[6], $[a,b] = \{x \in \mathbb{R} : a \leqslant x \leqslant b\}$ een *gesloten interval*, en $[a,b) = \{x \in \mathbb{R} : a \leqslant x < b\}$ en $(a,b] = \{x \in \mathbb{R} : a < x \leqslant b\}$ zijn *halfopen (of halfgesloten) intervallen*. Als nodig, dan kunnen we $(a,b]$ links-open en rechts-gesloten noemen, enzovoorts. De termen 'open' en 'gesloten' kan men als volgt onthouden: 'open' betekent dat het randpunt niet in het interval zit, en 'gesloten' dat het er wel in zit.

[3] Voor strikte inclusie wordt vaak '$\subsetneq$' gebruikt, en '$\subset$' is ook een gebruikelijke notatie voor 'deelverzameling'.

[4] Vaak wordt de uitdrukking 'dan en slechts dan als' gebruikt, maar 'als en slechts als' is correcter. Je kunt ook zeggen 'precies dan als'.

[5] Strikt genomen is deze notatie niet toegelaten in het door ons gebruikte systeem van axioma's voor verzamelingstheorie, maar de betekenis is duidelijk. Een correcte notatie zou zijn: $\{x \in \mathbb{Z} : \text{er is een } k \in \mathbb{Z} \text{ zodat } x = 2k+1\}$.

[6] In de schoolwiskunde wordt in plaats van (a,b) meestal de notatie $\langle a,b\rangle$ gebruikt.

(ii) **Onbegrensde intervallen:** Zij $a \in \mathbb{R}$, dan zijn $(a,\infty) = \{x \in \mathbb{R} : x > a\}$ en ook $(-\infty,a) = \{x \in \mathbb{R} : x < a\}$ open intervallen, en $[a,\infty) = \{x \in \mathbb{R} : x \geqslant a\}$ en ook $(-\infty,a] = \{x \in \mathbb{R} : x \leqslant a\}$ gesloten intervallen[7]. Ook de hele reële rechte kan beschouwd worden als een onbegrensd interval: $\mathbb{R} = (-\infty,\infty)$, dat zowel open als gesloten is.

■

I.1.6 Voorbeeld.

(i) Er geldt $(0,1) \subseteq (0,1]$ want elk element van $(0,1)$ is ook een element van $(0,1]$, maar $(0,1] \not\subseteq (0,1)$ omdat 1 een element van $(0,1]$ is maar niet van $(0,1)$.

(ii) $\varnothing$ is een deelverzameling van elke verzameling, want voor iedere $x \in \varnothing$ geldt $x \in A$ (immers, er is geen $x \in \varnothing$, dus er is niets te controleren; zie ook de waarheidstabel in Figuur 2.4 voor de waarheid van de implicatie $(x \in \varnothing) \Rightarrow (x \in A)$).

(iii) Het open interval $(0,-1)$ is leeg, en gelijk aan het gesloten interval $[0,-1]$.

■

Cartesisch product

Het volgende begrip wordt vaak gebruikt.

I.1.7 Definitie. Het *cartesisch product* van twee verzamelingen A en B is de verzameling geordende paren

$$A \times B = \{(a,b) : a \in A \text{ en } b \in B\}.^{8}$$

De volgorde van elementen van een geordend paar is belangrijk: als $a \neq b$ dan $(a,b) \neq (b,a)$. Twee geordende paren (a,b) en (a',b') zijn aan elkaar gelijk als en slechts als $a = a'$ en $b = b'$.

I.1.8 Voorbeeld.

(i) Zij $A = \{0,1,2\}$ en $B = \{0,3\}$. Het cartesisch product van A en B is de volgende verzameling

$$A \times B = \{(0,0),(0,3),(1,0),(1,3),(2,0),(2,3)\}.$$

(ii) Zij $\mathbb{R}$ de reële rechte. Dan is $\mathbb{R} \times \mathbb{R}$ de verzameling van alle punten in het platte vlak[9].

■

Opgaven

1. Zij $V = \{-3,-2,-1,0,1,2,3\}$. Formuleer bij ieder van de volgende verzamelingen steeds een eigenschap $P(x)$ zó dat de verzameling gelijk is aan $\{x \in V : P(x)\}$ en bewijs de gelijkheid ook.

(a) $A = \{1,2,3\}$;

(b) $B = \{0,1,2,3\}$;

(c) $C = \{-2,-1\}$;

(d) $D = \{-2,0,2\}$;

(e) $E = \varnothing$.

✍ **2.** Wat is het aantal elementen van de volgende verzamelingen:

(a) $A = \{0, 2, 4, \ldots, 22\}$;

(b) $B = \{1, \{2\}, \{\{2\}\}\}$;

(c) $C = \{\{\{1\}\}\}$;

(d) $D = \{\varnothing\}$;

(e) $E = \{1, \{1, 2, 3, 4, 5\}\}$.

✍ **3.**

(a) Vind alle deelverzamelingen van $\{0, 1\}$.

(b) Vind alle deelverzamelingen van $\{0, 1, 2\}$.

(c) Vind alle deelverzamelingen van $\{0, 1, 2, 3\}$.

★ (d) Zij A een *eindige* verzameling, d.w.z., een verzameling die maar eindig veel elementen bevat.[10] Vind een verband tussen het aantal elementen van A en het aantal deelverzamelingen van A, en bewijs je vermoeden.

✍ **4.** Laat A de verzameling van alle even natuurlijke getallen, B de verzameling van alle natuurlijke getallen die deelbaar door 3 zijn en C de verzameling van alle natuurlijke getallen die deelbaar door 6 zijn. Bewijs of weerleg:

(a) $A \subseteq B$;

(b) $A \subseteq C$;

(c) $B \subseteq C$;

(d) $B \subseteq A$;

(e) $C \subseteq A$;

(f) $C \subseteq B$.

✍ **5.** Bewijs: voor elke verzameling A geldt dat $\varnothing \subseteq A$ en $A \subseteq A$.

6. Welke van de volgende verzamelingen zijn aan elkaar gelijk? Bewijs je bewering of geef een tegenvoorbeeld.

(a) $A = \{n \in \mathbb{Z} : |n| < 2\}$;

(b) $B = \{n \in \mathbb{Z} : n^3 = n\}$;

(c) $C = \{n \in \mathbb{Z} : n^2 \leqslant n\}$;

(d) $E = \{-1, 0, 1\}$.

✍ **7.** Als $A = B$, dan geldt natuurlijk $A \times B = B \times A$. Dat is echter geen noodzakelijk voorwaarde! Geef de precieze voorwaarden op de verzamelingen A en B opdat $A \times B = B \times A$.

✍ **8.** Voor elke verzameling A zij $\mathscr{P}(A)$ de verzameling van alle deelverzamelingen van A (deze heet de *machtsverzameling* van A). Geef de lijst van elementen van $\mathscr{P}(A) \times \mathscr{P}(B)$, waarbij $A = \{0, 1\}$ en $B = \{\varnothing\}$.

I.2 Operaties op verzamelingen

De basisoperaties op verzamelingen zijn als volgt gedefinieerd.

[7] Het hier gebruikte symbool ∞ is *geen* element van $\mathbb{R}$, maar het is slechts onderdeel van een notatie.

[8] Helaas zijn onze notaties voor een geordend paar (a, b) van reële getallen en het open interval (a, b) gelijk. De lezer zal iedere keer de juiste keuze moeten maken op grond van de context.

[9] In plaats van $\mathbb{R} \times \mathbb{R}$ schrijven we vaak $\mathbb{R}^2$.

[10] Voor de duidelijkheid: het reële interval $(0, 1)$ heet dan misschien wel eens een eindig interval, maar het is géén eindige verzameling.

I.2.1 Definitie. Zij Ω een verzameling. Voor deelverzamelingen A en B van Ω definiëren we

(i) het *complement* van A in Ω door

$$\Omega \setminus A = \{x \in \Omega : x \notin A\}$$

(we schrijven vaak A^c als duidelijk is wat de verzameling Ω is);

(ii) de *vereniging* van A en B door

$$A \cup B = \{x \in \Omega : x \in A \text{ of } x \in B\};$$

(iii) de *doorsnede* van A en B door

$$A \cap B = \{x \in \Omega : x \in A \text{ en } x \in B\}.$$

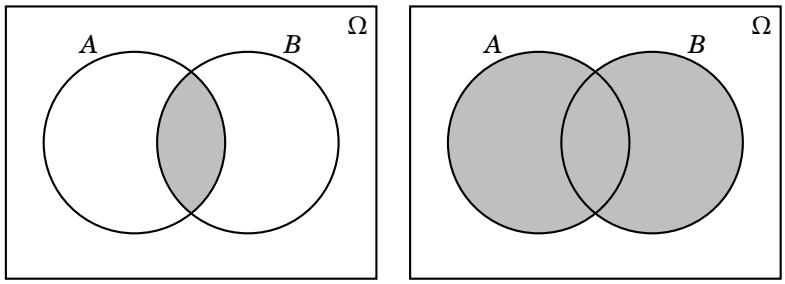
(iv) het *verschil* van A en B door

$$A \setminus B = \{x \in \Omega : x \in A \text{ en } x \notin B\}.$$

I.2.2 Opmerking. In de bovenstaande definitie hangen $A \cup B$, $A \cap B$ en $A \setminus B$ niet af van de verzameling Ω waarin dit alles gebeurt. We zullen dan ook in deze gevallen deze Ω niet meer altijd noemen.

I.2.3 Voorbeeld. Beschouw weer de verzamelingen A en B uit Voorbeeld I.1.1(ii). Dan is $A \cap B$ de verzameling van alle getallen die oplossingen zijn van beide vergelijkingen $\sin(\pi x) = 0$ en $\cos(\pi x/2) = 0$, en $A \cup B$ is de verzameling van alle getallen die oplossingen zijn van tenminste één van die twee vergelijkingen. Omdat $A = \mathbb{Z}$ en $B = \{2k+1 : k \in \mathbb{Z}\}$ is het niet moeilijk in te zien dat $A \cap B = B$ en $A \cup B = A$. ∎

Om doorsnede en vereniging van A en B te illustreren kunnen we venndiagrammen tekenen. In Figuur 1.1 zijn de doorsnede $A \cap B$ en de vereniging $A \cup B$ getekend. De venndiagrammen zijn ook handig om allerlei eigenschappen van de basisoperaties te vinden; zie bijvoorbeeld Opgaven I.2.1 en I.2.2.



Figuur 1.1 – Doorsnede en vereniging van A en B

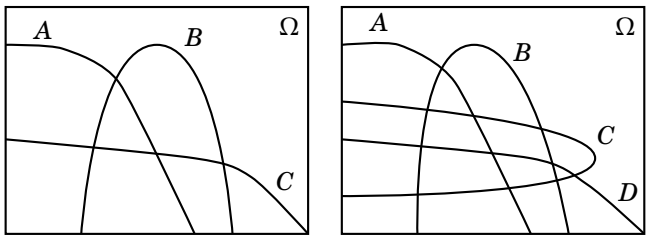
I.2.4 Definitie. Twee verzamelingen A en B heten *disjunct* als $A \cap B = \varnothing$.

I.2.5 Voorbeeld.

(i) De verzamelingen $A = \{x \in \mathbb{R} : x > 9\}$ en $B = \{0, 1/2\}$ zijn disjunct: $A \cap B = \varnothing$ want alle elementen van A zijn reële getallen groter dan 9 en geen element van B is groter dan 9.

(ii) De verzamelingen $C = (-3, \pi)$ en $D = (1, 33]$ zijn niet disjunct; immers $2 \in C \cap D$ want $-3 < 2 < \pi$ en $1 < 2 \leqslant 33$. In feite bevat de doorsnede oneindig veel elementen: $C \cap D = (1, \pi)$.

In Figuur 1.2 zijn venndiagrammen voor drie respectievelijk vier deelverzamelingen van Ω getekend. Venn-diagrammen voor meer dan vier verzamelingen zijn lastig: het is niet makkelijk om in een overzichtelijke manier alle mogelijke doorsneden in één plaatje te krijgen.



Figuur 1.2 – Venn-diagrammen voor drie en vier verzamelingen

Vereniging en doorsnede van oneindig veel verzamelingen

In de wiskunde onderzoeken we vaak oneindige objecten: er zijn oneindig veel natuurlijke getallen, oneindig veel breuken, oneindig veel punten in het platte vlak, oneindig veel lijnen, oneindig veel functies. Daarvoor is de taal van de verzamelingenleer ook handig.

We kunnen ook de doorsnede en de vereniging van *willekeurig* veel verzamelingen definiëren:

I.2.6 Definitie. Laat Ω een verzameling zijn. Laat L een verzameling zijn, en voor elke $\lambda \in L$, A_λ een deelverzameling van Ω. Dan:

$$\bigcap_{\lambda\in L} A_\lambda = \{x \in \Omega : \text{voor elke } \lambda \in L \text{ geldt } x \in A_\lambda\}$$

en

$$\bigcup_{\lambda\in L} A_\lambda = \{x \in \Omega : \text{er is een } \lambda \in L \text{ met } x \in A_\lambda\}.$$

I.2.7 Voorbeeld. Beschouw de verzameling $\mathbb{N}$ van alle natuurlijke getallen. Voor elke $n \in \mathbb{N}$ zij $A_n = (0, 1/(n+1)]$. We bewijzen dat $\bigcap_{n\in\mathbb{N}} A_n = \varnothing$. Immers, neem aan dat $\bigcap_{n\in\mathbb{N}} A_n \neq \varnothing$. Dan is er een $x \in \mathbb{R}$ met $x \in \bigcap_{n\in\mathbb{N}} A_n$. Volgens Definitie I.2.6 ligt x in elk interval $(0, 1/(n+1)]$, dat wil zeggen, voor elke $n \in \mathbb{N}$ geldt $0 < x \leqslant 1/(n+1)$. We krijgen een tegenspraak: voor alle $n \in \mathbb{N}$ met $n + 1 > 1/x$ geldt dat $1/(n+1) < x$.

Dit soort bewijs heet *bewijs uit het ongerijmde*. Het werkt hier als volgt: Om een bewering te bewijzen (in ons geval: $\bigcap_{n\in\mathbb{N}} A_n = \varnothing$) kunnen we het tegengestelde veronderstellen ($\bigcap_{n\in\mathbb{N}} A_n \neq \varnothing$) en laten zien dat dit tot een onjuiste bewering, een tegenspraak, leidt (er is een $x \in \mathbb{R}$ en er is een $n \in \mathbb{N}$ zó dat $x \leqslant 1/(n+1)$ én $x > 1/(n+1)$).

Hoofdstuk II bevat een meer gedetailleerde behandeling van bewijzen uit het ongerijmde; zie voorbeeld II.3.4.

I.2.8 Voorbeeld. Beschouw nu voor elke $n \in \mathbb{N}$ de verzameling $B_n = (0, n]$. We bewijzen nu dat $\bigcup_{n\in\mathbb{N}} B_n = (0,\infty)$. Volgens Definitie I.1.2 moeten we laten zien dat $\bigcup_{n\in\mathbb{N}} B_n \subseteq (0,\infty)$ en $(0,\infty) \subseteq \bigcup_{n\in\mathbb{N}} B_n$. We bewijzen nu de eerste inclusie. Laat $x \in \bigcup_{n\in\mathbb{N}} B_n$. Volgens Definitie I.2.6 is er een $n \in \mathbb{N}$ met $x \in (0, n]$. Hieruit volgt dat $x \in (0,\infty)$. Nu de tweede inclusie. Laat $x \in (0,\infty)$. Neem dan een $n \in \mathbb{N}$ met $x < n$, dan $x \in (0, n]$ en bijgevolg $x \in \bigcup_{n\in\mathbb{N}} B_n$.

Opgaven

✍ **1.** (**Wetten van de Morgan**) Zij Ω een verzameling. Bewijs dat voor alle deelverzamelingen A en B van Ω geldt
   (a) $\Omega \setminus (A \cap B) = (\Omega \setminus A) \cup (\Omega \setminus B)$;
   (b) $\Omega \setminus (A \cup B) = (\Omega \setminus A) \cap (\Omega \setminus B)$.

2. Zij Ω een verzameling. Formuleer en bewijs de Wetten van de Morgan
   (a) voor drie deelverzamelingen van Ω;
   (b) voor vier deelverzamelingen van Ω.

3. Bewijs dat voor alle verzamelingen A, B en C geldt
   (a) $B \setminus (B \setminus A) = A \cap B$;
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
   (c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

4. (a) Zij $A = \{1,2,3,4,5,6,7,8,9\}$. Vind $A \cap A$, $A \cup A$ en $A \setminus A$.
   (b) Zij A een willekeurige verzameling. Vind en bewijs een algemene regel voor $A \cap A$, $A \cup A$ en $A \setminus A$.

5. Beschouw de verzamelingen $A = \{x \in \mathbb{N} : x \geqslant 15\}$ en $B = \{x \in \mathbb{N} : x \leqslant 20\}$. Beschrijf nu $\mathbb{N} \setminus A$, $\mathbb{N} \setminus B$, $A \cap B$ en $A \cup B$ met soortgelijke formules.

6. Zij $K = \{1,2,4\}$. Vind $\bigcup_{k \in K} A_k$ en $\bigcap_{k \in K} A_k$ als gegeven is:
   (a) $A_k = \{k^2\}$;
   (b) $A_k = [k-1, k+1]$;
   (c) $A_k = (k, \infty)$.

★✍ **7.** Beschouw voor elke $n \in \mathbb{N}$ de verzameling $A_n = \{x \in \mathbb{R} : 1/2^n \leqslant x < 2 + 1/2^n\}$.
   (a) Vind $\bigcap_{n \in \mathbb{N}} A_n$.
   (b) Vind $\bigcup_{n \in \mathbb{N}} A_n$.

8. Laat A, B en C deelverzamelingen zijn van Ω.
   (a) Wat is het verband tussen $A \cup (B \setminus C)$ en $(A \cup B) \setminus (A \cup C)$?
   (b) Wanneer geldt $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$?

9. Vereenvoudig de volgende uitdrukking met behulp van venndiagrammen:

$$(A \cap B \cap C^c) \cup (A \cap B \cap D^c) \cup (A \cap B \cap C \cap D).$$

I.3 Functies

Je bent het begrip *functie* natuurlijk al tegengekomen; vaak als een voorschrift dat aan elk getal een getal toevoegt, bijvoorbeeld de functie met het voorschrift $f(x) = x^2$ die aan elk getal zijn kwadraat toevoegt. Er zijn echter veel meer mogelijkheden, waarbij we ons niet tot getallen hoeven te beperken: het voorschrift dat aan elke auto zijn kenteken toevoegt, het voorschrift dat aan elke persoon zijn geboortedatum toevoegt, of de kleur van zijn ogen definiëren ook functies. Een

functie kan beschreven worden door een formule (bijvoorbeeld $f(x) = x^2$), maar ook als een grafiek (bijvoorbeeld het verloop van de koers van aandelen in de tijd), of een tabel (bijvoorbeeld tentamencijfers van studenten die aan een tentamen hebben plaatsgenomen).

Om algemene eigenschappen van functies af te leiden en ze te kunnen gebruiken moeten we eerst afspreken welke voorschriften functies definiëren, en ook wat een functie precies is, zodat we bijvoorbeeld over gelijkheid van functies kunnen praten. Informeel gesproken is een functie van A naar B een voorschrift dat aan *elk* element van A *precies één* element van B toevoegt. Maar als we functies als voorschriften zouden definiëren, dan zouden de voorschriften $f(x) = 2x + 2$ en $g(x) = 2(x + 1)$ niet dezelfde functie van $\mathbb{R}$ naar $\mathbb{R}$ zijn. De formele definitie die volgt zegt dat een functie van A naar B niet een *voorschrift* is, maar de *grafiek* van een voorschrift is: de deelverzameling van $A \times B$ bestaande uit alle paren (a, b) die aan het voorschrift voldoen. Informeel gezegd: het doet er alleen maar toe *wat* het voorschrift doet, en niet *hoe*.

I.3.1 Definitie. Een *functie*[11] van een verzameling A naar een verzameling B is een tripel (A, B, f) met f een deelverzameling van $A \times B$ met de volgende eigenschap:

> voor iedere $a \in A$ bestaat er precies één $b \in B$ zodanig dat $(a, b) \in f$; deze b noteren we als $f(a)$.

Notatie: $f : A \to B$, en $a \mapsto f(a)$.

De verzameling A heet het *domein* en B het *codomein*[12] van f. De verzameling f heet de *grafiek* van de functie (A, B, f). In plaats van '$(a, b) \in f$' schrijven we vaak '$f(a) = b$'. Als $(a, b) \in f$ dan noemen we b *het beeld* van a onder f en a *een origineel* van b onder f. Merk op dat volgens deze definitie een functie gegeven wordt door haar domein, haar codomein en haar grafiek. Voor twee afbeeldingen $f : A \to B$ en $g : C \to D$ geldt dus dat $f = g$ precies dan als geldt: $A = C$, en $B = D$, en voor alle $a \in A$ geldt $f(a) = g(a)$.

I.3.2 Voorbeeld. De afbeeldingen $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ en $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto |x|^2$ zijn dus gelijk, ook al zijn ze gegeven door verschillende formules. ∎

I.3.3 Voorbeeld. Laat A de verzameling zijn van alle studenten van een bepaalde nederlandse universiteit. Dan hebben we functies $f : A \to \mathbb{N}$ en $g : A \to \mathbb{R}$ die elk element van A naar hun studienummer sturen. Deze functies zijn niet gelijk, want de codomeinen zijn verschillend. ∎

I.3.4 Opmerking. Volgens de definitie van een functie heeft elk element van het domein precies één beeld. Een element van het codomein kan echter géén origineel hebben, of één of meerdere originelen hebben.

Beschouw bijvoorbeeld $f : \mathbb{R} \to [-1, 1]$ gegeven door $f(x) = \sin(\pi x)$. Voor elke $x \in \mathbb{R}$ is de waarde van x onder f uniek bepaald, maar het getal $0 \in [-1, 1]$ heeft oneindig veel originelen: voor elke $x \in \mathbb{Z}$ geldt $f(x) = 0$.

I.3.5 Definitie. Laat A en B twee verzamelingen zijn en zij $f : A \to B$.

(i) f heet *injectief* als voor alle $a_1 \in A$ en $a_2 \in A$ met $f(a_1) = f(a_2)$ geldt dat $a_1 = a_2$. (Met andere woorden, verschillende elementen van A hebben verschillende beelden. Of, met wéér andere woorden: voor iedere $b \in B$ is er *hoogstens* één $a \in A$ met $f(a) = b$.)

[11] Functies worden vaak ook *afbeeldingen* genoemd.

[12] Voor domein en codomein worden ook wel de namen bron(verzameling) en doel(verzameling) gebruikt.

(ii) f heet *surjectief* als voor elke $b \in B$ er een $a \in A$ bestaat met $f(a) = b$. (Met andere woorden, als de verzameling van beelden de hele verzameling B is. Of, met wéér andere woorden, voor iedere $\in B$ is er *minstens* één $a \in A$ met $f(a) = b$.)

(iii) f heet *bijectief* als f injectief en surjectief is. (Met andere woorden, voor iedere $b \in B$ is er *precies* één $a \in A$ is met $f(a) = b$.)

(iv) Het *beeld* van f is de verzameling van $b \in B$ waarvoor er een $a \in A$ is met $b = f(a)$. Het is een deelverzameling van B. Notaties: $f(A)$ of $\{f(a) : a \in A\}$ of $\{b \in B :$ er bestaat een $a \in A$ met $b = f(a)\}$.

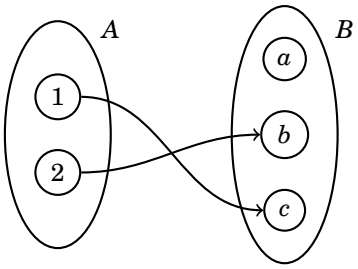
(v) Voor C een deelverzameling van A definiëren we de *beperking* (ook wel *restrictie* genoemd) van f tot C als de functie $f|_C : C \to B$, $x \mapsto f(x)$.

I.3.6 Opmerking. Laat A en B twee verzamelingen zijn en zij $f : A \to B$. Dan geldt dat f surjectief is precies dan als $f(A) = B$.

We krijgen een surjectieve afbeelding door het codomein van f te beperken tot het beeld van f: de afbeelding $g : A \to f(A)$, $x \mapsto f(x)$ is surjectief.

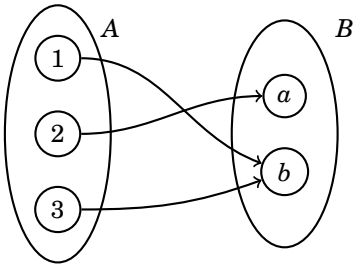
Als A en B eindig zijn dan is het makkelijk functies van A naar B grafisch weer te geven: zie de volgende voorbeelden.

I.3.7 Voorbeeld. Zij $A = \{1, 2\}$ en $B = \{a, b, c\}$ met a, b en c verschillend. De functie $f : A \to B$, gedefinieerd door $f(1) = c$ en $f(2) = b$, is injectief want verschillende elementen van A hebben verschillende beelden, maar niet surjectief omdat $a \in B$ geen beeld is van een element van A (zie Figuur 1.3).



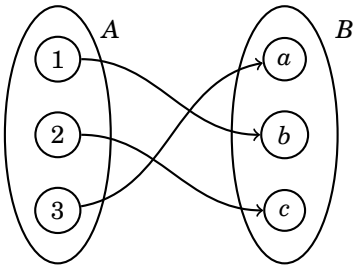
Figuur 1.3 – Een injectieve, niet surjectieve functie $f : A \to B$

I.3.8 Voorbeeld. Zij $A = \{1, 2, 3\}$ en $B = \{a, b\}$ met a en b verschillend. De functie $f : A \to B$, gedefinieerd door $f(1) = b$, $f(2) = a$ en $f(3) = b$, is surjectief want elk element van B is een beeld van een element van A, maar niet injectief omdat de elementen 1 en 3 verschillend zijn en toch hetzelfde beeld hebben (zie Figuur 1.4).



Figuur 1.4 – Een surjectieve, niet injectieve functie $f : A \to B$

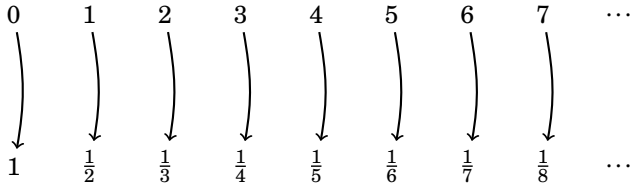
I.3.9 Voorbeeld. Zij $A = \{1,2,3\}$ en $B = \{a,b,c\}$ met a, b en c verschillend. De functie $f : A \to B$, gedefinieerd door $f(1) = b$, $f(2) = c$ en $f(3) = a$, is surjectief en injectief (zie Figuur 1.5).



Figuur 1.5 – Een bijectieve functie $f : A \to B$

Een functie $a : \mathbb{N} \to B$ noemen we soms ook een *rij* in B. We schrijven dan vaak a_n in plaats van $a(n)$; een gebruikelijke notatie is $(a_n)_{n\in\mathbb{N}}$ (merk wel op dat we dan eigenlijk het codomein niet meer noemen, er is dus al enige mate van slordigheid).

I.3.10 Voorbeeld. De functie $f : \mathbb{N} \to \mathbb{R}$ gegeven door $f(n) = 1/(n+1)$ is dan de reële rij $(1/(n+1))_{n\in\mathbb{N}}$. Deze functie is injectief (als $n \neq m$ dan $1/(n+1) \neq 1/(m+1)$), maar niet surjectief omdat (bijvoorbeeld) het getal 0 uit het codomein van f geen origineel heeft (er is geen natuurlijk getal n met $1/(n+1) = 0$).



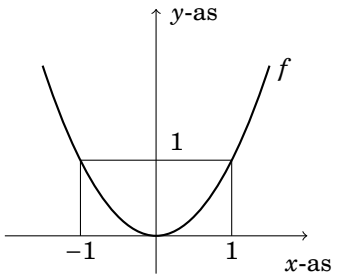
Figuur 1.6 – De rij $(1/(n+1))_{n\in\mathbb{N}}$ als een functie $f : \mathbb{N} \to \mathbb{R}$

Laat $I \subseteq \mathbb{R}$ een interval zijn, en $f : I \to \mathbb{R}$. Om f grafisch weer te geven tekenen we meestal de grafiek als deelverzameling van $I \times \mathbb{R}$: zoals uit de definitie volgt is de grafiek de verzameling van alle punten van de vorm $(x, f(x))$ met $x \in I$.

I.3.11 Voorbeeld. De functie $f : \mathbb{R} \to [0,\infty)$ gegeven door $f(x) = x^2$ is niet injectief: -1 en 1 horen tot het domein van f, er geldt $-1 \neq 1$ maar $f(-1) = (-1)^2 = 1^2 = f(1)$ (zie Figuur 1.7). Zij is wel surjectief: voor elke $y \in [0,\infty)$ is er een $x \in \mathbb{R}$ met $f(x) = y$; neem bijvoorbeeld $x = \sqrt{y}$.

Door het domein van een functie te veranderen, krijgen we een *nieuwe* functie die geheel andere eigenschappen kan hebben. Bijvoorbeeld, $g : \mathbb{R} \to \mathbb{R}$ gegeven door $g(x) = x^2$ is niet injectief, maar de beperking van g tot $[0,\infty)$, $g|_{[0,\infty)} : [0,\infty) \to \mathbb{R}$, is injectief.

I.3.12 Voorbeeld. Er bestaat geen functie van $\{0,1,2,3\}$ naar $\mathbb{N}$ die surjectief is. Immers, zij $f : \{0,1,2,3\} \to \mathbb{N}$ een afbeelding. De verzameling $\mathbb{N}$ is oneindig en dus is $X = \mathbb{N} \setminus \{f(0), f(1), f(2), f(3)\}$ niet leeg (X is zelfs oneindig). Kies een $b \in X$, dan heeft b geen origineel onder f.



Figuur 1.7 – Grafiek van de functie $f(x) = x^2$

Samenstelling van functies

Een van de mooie eigenschappen van bijectieve functies is dat ze een inverse hebben. We zullen later zien dat als f bepaalde 'mooie' eigenschappen heeft (bijvoorbeeld continu is) deze eigenschappen door de inverse van f geërfd worden. Het volgende begrip is essentieel voor het definiëren van inverse functies, maar zeker nog belangrijker op zichzelf.

I.3.13 Definitie. Laat $f : A \to B$ en $g : B \to C$ twee functies zijn. De *samenstelling* van f en g is de functie $g \circ f : A \to C$ gedefinieerd door

$$(g \circ f)(a) = g\big(f(a)\big).$$

We lezen $g \circ f$ als 'g na f'.

I.3.14 Voorbeeld. De functie $f : \mathbb{R} \to [-1,1]$ is gegeven door $f(x) = \sin x$, en de functie $g : [-1,1] \to \mathbb{R}$ door $g(x) = x^2$. Dan is $f \circ g : [-1,1] \to [-1,1]$ de functie gedefinieerd door $(f \circ g)(x) = \sin(x^2)$, en $g \circ f : \mathbb{R} \to \mathbb{R}$ is gedefinieerd door $(g \circ f)(x) = (\sin x)^2$.

Als $f : A \to B$ en $g : B \to A$ functies zijn dan geldt niet altijd dat $f \circ g = g \circ f$. Als $A \neq B$ dan kan $f \circ g$ al zeker niet gelijk zijn aan $g \circ f$, want de domeinen verschillen. ■

I.3.15 Stelling. De samenstelling van functies is associatief, dat wil zeggen,

$$h \circ (g \circ f) = (h \circ g) \circ f$$

voor alle $f : A \to B$, $g : B \to C$ en $h : C \to D$.

Bewijs. Neem aan $f : A \to B$, $g : B \to C$ en $h : C \to D$ drie willekeurige functies zijn. De identiteit volgt uit het feit dat voor elke $a \in A$ geldt

$$\big(h \circ (g \circ f)\big)(a) = h\big((g \circ f)(a)\big) = h\big(g(f(a))\big)$$

en

$$\big((h \circ g) \circ f\big)(a) = (h \circ g)\big(f(a)\big) = h\big(g(f(a))\big).$$

■

I.3.16 Definitie. Voor A een verzameling definiëren we de functie $\mathrm{id}_A : A \to A$, gegeven door $a \mapsto a$. Deze functie heet de *identieke functie* van A. Ook de benamingen *identiteitsfunctie* en *identiteit* zijn gebruikelijk.

I.3.17 Opmerking. Als A en B verzamelingen zijn, en $f : A \to B$, dan geldt

$$f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f.$$

Inverse functies

Zij $f : A \to B$ een bijectie. We definiëren in $B \times A$ de volgende deelverzameling

$$g = \{(b,a) \in B \times A : (a,b) \in f\}.$$

Merk op dat g een functie is van B naar A. Immers: omdat f surjectief is, is er voor iedere $b \in B$ een $a \in A$ zodat $(b,a) \in g$, en omdat f injectief is, is deze a uniek.

I.3.18 Definitie. Zij $f : A \to B$ een bijectie. De *inverse* van f is de functie $g : B \to A$ met $g = \{(b,a) \in B \times A : (a,b) \in f\}$.

De inverse functie $f : A \to B$ is de unieke functie $g : B \to A$ zodat voor alle $a \in A$ en $b \in B$ geldt

$$g(b) = a \qquad \text{als en slechts als} \qquad f(a) = b.$$

We gebruiken als notatie: $g = f^{-1}$. Zie Opgave I.3.14 voor een karakterisering van inverse functies in termen van samenstelling.

I.3.19 Lemma. Zij $f : A \to B$ een bijectie. De inverse f^{-1} is ook een bijectie en er geldt: $(f^{-1})^{-1} = f$.

Bewijs. Opgave I.3.15. ∎

I.3.20 Voorbeeld. De functie $f : \mathbb{R} \to \mathbb{R}$ gedefinieerd door $f(x) = 2 - 3x$ is bijectief (ga zelf na dat f injectief en surjectief is). Om haar inverse te vinden beschouw een willekeurige $y \in \mathbb{R}$. Er geldt, voor alle $x \in \mathbb{R}$,

$$2 - 3x = y \qquad \text{als en slechts als} \qquad x = \frac{2-y}{3}.$$

De inverse $f^{-1} : \mathbb{R} \to \mathbb{R}$ is dus gegeven door het voorschrift[13] $f^{-1}(x) = (2-x)/3$. Opgave I.3.21 ∎

I.3.21 Definitie. Laat $f : A \to B$ een afbeelding zijn, en C een deelverzameling van B. Dan noemen we de verzameling $\{a \in A : f(a) \in C\}$ het *inverse beeld* van C onder f. Deze deelverzameling van A noteren we ook als $f^{-1}(C)$.

Merk op dat $f^{-1}(C)$ bestaat ook als f geen inverse heeft.

I.3.22 Voorbeeld. Zij $f : \mathbb{R} \to \mathbb{R}$ gegeven door $f(x) = x^2$. Dan geldt $f^{-1}(\{-1\}) = \varnothing$, $f^{-1}(\{1\}) = \{-1,1\}$ en $f^{-1}([0,1]) = [-1,1]$. ∎

Opgaven

✍ **1.** Laat $f : \mathbb{R} \setminus \{-1\} \to \mathbb{R}$ gegeven zijn door $f(x) = (1-x)/(1+x)$. Vind $f(0)$ en voor alle $x \in \mathbb{R} \setminus \{-1,0,1\}$ vind $f(1/x)$ en $1/f(x)$.

✍ **2.** (a) Laat $f : \mathbb{R} \to \mathbb{R}$ een functie zijn en neem aan dat voor alle $x \in \mathbb{R}$ geldt dat $f(x+1) = x^2 - 5x + 1$. Vind $f(x)$.

✍ (b) Laat $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ een functie zijn en neem aan dat voor alle $x \in \mathbb{R} \setminus \{0\}$ geldt $f(1/x) = x + \sqrt{1+x^2}$. Vind $f(x)$.

✍ **3.** Zij $f : \mathbb{R} \to \mathbb{R}$ gegeven door $f(x) = \sin(x^2)$; vind alle originelen van 0, -1 en π.

[13] Het maakt natuurlijk niets uit of we de variabele x of y noemen.

4. Hieronder staan vier tweetallen functievoorschriften. Geef van elk tweetal aan of beide voorschriften dezelfde functie beschrijven, of niet.

(a) $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ en
$g : \mathbb{R} \to \mathbb{R}_{\geqslant 0}, x \mapsto x^2$.

(b) $f : \mathbb{R} \to \mathbb{R}, x \mapsto (x+1)^2$ en
$g : \mathbb{R} \to \mathbb{R}, x \mapsto 2x(\frac{x}{2}+1)+1$.

(c) $f : [0, 2\pi] \to \mathbb{R}, x \mapsto \sin(x)$ en
$g : \mathbb{R} \to \mathbb{R}, x \mapsto \sin(x)$.

(d) $f : \mathbb{R} \setminus \{1\} \to \mathbb{R}, x \mapsto x+1$ en
$g : \mathbb{R} \setminus \{1\} \to \mathbb{R}, x \mapsto \frac{x^2-1}{x-1}$.

5. (a) Laat $A = \{1,2\}$ en $B = \{1,2,3\}$. Hoeveel afbeeldingen $A \to B$ zijn er?

(b) Laat B een verzameling zijn. Hoeveel functies $f : \varnothing \to B$ zijn er?

(c) Laat A een verzameling zijn. Hoeveel functies $f : A \to \varnothing$ zijn er?

6. Geef voorbeelden van eindige verzamelingen A en B en een functie $f : A \to B$ die

(a) bijectief is,

(b) surjectief maar niet injectief is,

(c) injectief maar niet surjectief is,

(d) niet surjectief en niet injectief is.

Bewijs in elk van de onderdelen dat je voorbeeld de gewenste eigenschappen heeft.

7. Geef voorbeelden van oneindige verzamelingen A en B en een functie $f : A \to B$ die

(a) bijectief is,

(b) surjectief maar niet injectief is,

(c) injectief maar niet surjectief is,

(d) niet surjectief en niet injectief is.

Bewijs in elk van de onderdelen dat je voorbeeld de gewenste eigenschappen heeft.

8. Zij A een eindige verzameling. Voor het aantal elementen van A gebruiken we de notatie $\#A$.
Neem aan dat A en B eindige verzamelingen zijn en zij $f : A \to B$.

(a) Laat zien dat als f injectief is dan geldt $\#A \leqslant \#B$.

(b) Laat zien dat als f surjectief is dan geldt $\#A \geqslant \#B$.

✍ **9.** Laat $f : A \to B$ en $g : B \to C$ twee functies zijn. Bewijs of weerleg:

(a) Als $g \circ f$ injectief is dan is f injectief.

(b) Als $g \circ f$ injectief is dan is g injectief.

(c) Als $g \circ f$ surjectief is dan is f surjectief.

(d) Als $g \circ f$ surjectief is dan is g surjectief.

✍ **10.** Bewijs of weerleg: samenstelling van functies is commutatief, dat wil zeggen, voor alle verzamelingen A en B, en voor alle $f : A \to B$ en $g : B \to A$ geldt $f \circ g = g \circ f$. Geldt deze bewering als $A = B$?

11. Bewijs dat elke van de volgende functies een inverse heeft en vind zijn voorschrift.

(a) $f : \{0,1,2\} \to \{3,5,15\}$ gegeven door $f(0) = 3$, $f(1) = 15$ en $f(2) = 5$.

(b) $f : \mathbb{R} \to \mathbb{R}$ gegeven door $f(x) = 4x + 5$;

(c) $f : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ gegeven door $f(x) = 1/x$.

12. Beschouw $f : [1,\infty) \to \mathbb{R}$ gegeven door $f(x) = (1-5x)/x$.

(a) Bewijs dat f injectief is.

✍ (b) Vind het beeld B van f. Laat zien dat de afbeelding $g : [1,\infty) \to B$ gedefinieerd door $x \mapsto f(x)$ bijectief is en bereken de inverse van g.

✍ **13.** Voor elke van de onderstaande injectieve functies $f : A \to \mathbb{R}$, bepaal het beeld B, en bepaal de afbeelding $g : B \to A$ zodat voor alle $a \in A$ geldt $g(f(a)) = a$.

(a) $A = \mathbb{R}$ en $f(x) = 7x - 3$;

(b) $A = (-\infty, 0]$ en $f(x) = x^2$;

(c) $A = \mathbb{R} \setminus \{-2\}$ en $f(x) = (1-x)/(2+x)$;

(d) $A = [-1,0]$, $f(x) = \sqrt{1-x^2}$.

14. Laat A en B verzamelingen zijn, en $f : A \to B$ en $g : B \to A$.

(a) Bewijs dat f en g beide bijectief zijn en inversen van elkaar zijn precies dan als $g \circ f = \mathrm{id}_A$ en $f \circ g = \mathrm{id}_B$.

(b) Geef een voorbeeld waar $g \circ f = \mathrm{id}_A$ en $f \circ g \neq \mathrm{id}_B$.

15. Bewijs Lemma I.3.19.

16. Zij $f : A \to A$ een functie. Bewijs: als voor elke $a \in A$ geldt $f\big(f(a)\big) = a$ dan is f een bijectie en $f^{-1} = f$.

17. Laat $f : A \to B$ een bijectie zijn en $C \subseteq B$. Bewijs of weerleg: het beeld van C onder f^{-1} is het inverse beeld van C onder f.
(Zie Definitie I.3.5(iv) en Definitie I.3.21. Merk op dat we voor beide verzamelingen de notatie $f^{-1}(C)$ gebruiken.)

18. Laat $f : \mathbb{R} \to \mathbb{R}$ de afbeelding zijn gegeven door $f(x) = x^2$.

(a) Beschrijf de elementen van $f^{-1}(\mathbb{Z}) \cap \mathbb{Q}$.

(b) Bewijs of weerleg: $f^{-1}(\mathbb{Z}) \cap \mathbb{Q} = \mathbb{Z}$.

19. Zij $f : A \to B$ een functie. Zij V_1 en V_2 deelverzamelingen van A. Toon aan

(a) $f(V_1 \cap V_2) \subseteq f(V_1) \cap f(V_2)$;

(b) Als f injectief is, dan geldt $f(V_1 \cap V_2) = f(V_1) \cap f(V_2)$.

★ **20.** Formeel is een functie een deelverzameling van een cartesisch product. Neem eens aan dat we $(a,b) \in f$ *niet* hadden afgekort met $b = f(a)$. Laat $f : A \to B$ en $g : B \to C$ functies zijn. Geef een definitie van $g \circ f$ in termen van geordende paren, dat wil zeggen, vul de volgende zin aan:
$(a,c) \in g \circ f$ als en slechts als.....
en bewijs dat dit dezelfde afbeelding oplevert als Definitie I.3.13.
Bewijs, uitgaande van de voorgaande formulering, dat $f \circ (g \circ h) = (f \circ g) \circ h$.

21. Zij $f : \mathbb{R} \to \mathbb{R}$ een bijectie. De grafieken van f en f^{-1} zijn deelverzamelingen van $\mathbb{R}^2$. Wat is het verband tussen deze deelverzamelingen?

22. Probeer eens de interactieve opgaven over inverse functies op de WIMS systeem (zoek onder 'inverse'): `http://wims.math.leidenuniv.nl/wims/`

I.4 Aftelbare en overaftelbare verzamelingen

Aftelbare verzamelingen

Laat A en B eindige verzamelingen zijn. Dan hebben ze evenveel elementen precies dan als er een bijectie $f: A \to B$ bestaat. Om willekeurige verzamelingen met elkaar te vergelijken nemen we dit als uitgangspunt voor de volgende definitie. Verrassende resultaten zullen volgen: $\mathbb{N}$, $\mathbb{N} \times \mathbb{N}$ en $\mathbb{Q}$ hebben evenveel elementen, maar $\mathscr{P}(\mathbb{N})$ en $\mathbb{R}$ hebben meer elementen dan $\mathbb{N}$.

I.4.1 Definitie. Twee verzamelingen A en B heten *gelijkmachtig* als er een bijectie $f: A \to B$ bestaat.

I.4.2 Voorbeeld. De verzamelingen $A = \{a,b,c,d\}$ met a,b,c,d verschillend en $B = \{1,2,3,4\}$ zijn gelijkmachtig: een bijectie $f: A \to B$ is gedefinieerd door $f(a) = 1$, $f(b) = 2$, $f(c) = 3$ en $f(d) = 4$. ∎

I.4.3 Voorbeeld.

(i) De intervallen $[0,1]$ en $[0,2]$ zijn gelijkmachtig: de afbeelding $f: [0,1] \to [0,2]$ gegeven door $f(x) = 2x$ is een bijectie.
(ii) Het interval $(-\pi/2, \pi/2)$ en de verzameling $\mathbb{R}$ zijn gelijkmachtig: de afbeelding $\tan: (-\pi/2, \pi/2) \to \mathbb{R}$ is een bijectie, en bijvoorbeeld ook de afbeelding gegeven door $x \mapsto -1/(x+\pi/2) - 1/(x-\pi/2)$.
(iii) Het interval $(0,1)$ en het interval $(1,\infty)$ zijn gelijkmachtig: de afbeelding $x \mapsto 1/x$ is een bijectie.

∎

Met behulp van het begrip gelijkmachtig kunnen we een nette definitie van eindige verzameling geven.

I.4.4 Definitie. Zij A een verzameling.

(i) A heet *eindig* als een natuurlijk getal n bestaat zó dat $\{1,2,\ldots,n\}$ en A gelijkmachtig zijn (voor $n = 0$ betekent dit dat $A = \varnothing$).
(ii) A heet *aftelbaar oneindig* als A en $\mathbb{N}$ gelijkmachtig zijn.
(iii) A heet *aftelbaar* als A eindig of aftelbaar oneindig is.
(iv) A heet *overaftelbaar* als A niet aftelbaar is.

Oneindige verzamelingen zijn dus aftelbaar als ze even veel elementen als $\mathbb{N}$ hebben. Het zou duidelijk moeten zijn dat $\mathbb{N}$ zelf aftelbaar is: de identieke afbeelding $\mathrm{id}_{\mathbb{N}}: \mathbb{N} \to \mathbb{N}$ is een bijectie. Omdat $\mathbb{N}$ niet eindig is, is er tenminste één aftelbaar oneindige verzameling.

I.4.5 Voorbeeld. Intuïtief zijn er meer gehele getallen dan natuurlijke getallen maar toch is de verzameling $\mathbb{Z}$ aftelbaar: een bijectie van $\mathbb{N}$ naar $\mathbb{Z}$ is gedefinieerd bijvoorbeeld door

$$f(n) = \begin{cases} n/2 & \text{als } n \text{ even is,} \\ -(n+1)/2 & \text{als } n \text{ oneven is.} \end{cases}$$

Bewijs. We tonen eerst aan dat f injectief is. Zij $n_1, n_2 \in \mathbb{N}$ en neem aan dat $f(n_1) = f(n_2)$. Omdat $f(n) \geq 0$ als en slechts als n even is, geldt dat n_1 en n_2 ofwel beide even ofwel beide oneven zijn. In het eerste geval hebben we $n_1/2 = n_2/2$, en dus $n_1 = n_2$, en in het tweede geval $-(n_1+1)/2 = -(n_2+1)/2$ waar ook uit volgt dat $n_1 = n_2$. In beide gevallen concluderen we dus dat $n_1 = n_2$, en er geldt dat f injectief is.

Nu gaan we bewijzen dat f surjectief is. Zij $m \in \mathbb{Z}$ willekeurig. Als $m \geq 0$ dan geldt dat $2m \in \mathbb{N}$ en $f(2m) = m$, en dus ligt m in het beeld van f. Als daarentegen $m < 0$ dan geldt dat $-1-2m \in \mathbb{N}$ en $f(-1-2m) = -(-1-2m+1)/2 = m$. In beide gevallen vinden we dat m in het beeld van f ligt. We concluderen dus dat f surjectief is.

Omdat de afbeelding f zowel injectief als surjectief is, is hij bijectief. ■

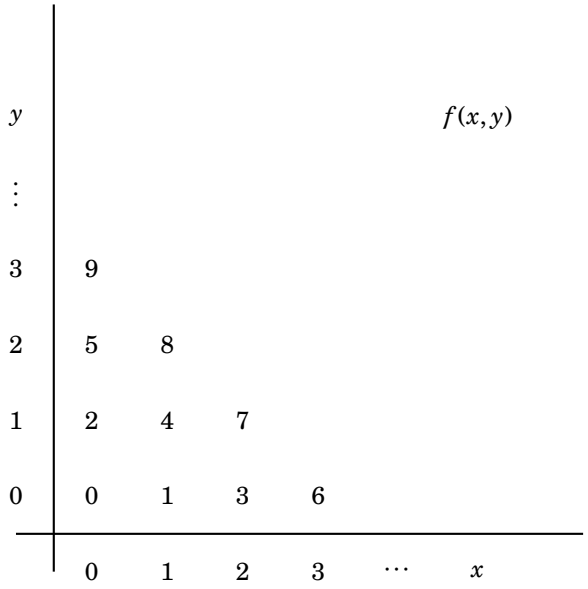
—■

Ook de verzameling $\mathbb{N} \times \mathbb{N}$ is aftelbaar.

I.4.6 Stelling. De verzameling $\mathbb{N} \times \mathbb{N}$ is aftelbaar.

Bewijs. Om te laten zien dat $\mathbb{N}\times\mathbb{N}$ aftelbaar is moeten we een bijectie vinden tussen $\mathbb{N} \times \mathbb{N}$ en $\mathbb{N}$. We zullen met een plaatje aannemelijk maken dat zo een bijectie bestaat, zonder het bewijs in detail te geven (Opgave I.4.9 geeft een mooie formule voor de f hieronder).

Beschouw de functie $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ waarbij $f(x,y)$ in de volgende tabel is weergegeven.



Figuur 1.8 – Grafische weergave van de functie $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Bijvoorbeeld $f(2,1) = 7$ en $f(4,0) = 10$. Uit de constructie is het duidelijk dat f een bijectie is. ■

Met een gelijkaardig argument kan men bewijzen dat ook $\mathbb{Q}$ aftelbaar is. Zie opgave I.4.8.

Niet elke verzameling is aftelbaar. We zullen bewijzen dat de verzameling van alle deelverzamelingen van $\mathbb{N}$ overaftelbaar is.

I.4.7 Definitie. Zij A een verzameling. De *machtsverzameling* van A is de verzameling van alle deelverzamelingen van A. Notatie: $\mathscr{P}(A)$.

I.4.8 Voorbeeld. $\mathscr{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$. —■

I.4.9 Stelling (Cantor)**.** Zij A een verzameling. Er bestaat geen surjectieve afbeelding $f : A \to \mathscr{P}(A)$.

Bewijs. Neem aan dat er een surjectie $f : A \to \mathscr{P}(A)$ bestaat. Beschouw nu de verzameling

$$B = \{x \in A : x \notin f(x)\}.$$

Aangezien $B \subseteq A$ geldt ook $B \in \mathscr{P}(A)$. Wegens de aanname dat f surjectief is, bestaat er een $x \in A$ met $f(x) = B$. Er zijn twee mogelijkheden: (i) $x \in B$ of (ii) $x \notin B$. Als (i) geldt dan geldt $x \in B$. Dus ook $x \in f(x)$, en met de definitie van B volgt $x \notin B$. Dus (i) geeft een tegenspraak. Als (ii) geldt dan weten we $x \notin B$ dus ook $x \notin f(x)$, en met de definitie van B volgt dat $x \in B$. Dus (ii) geeft ook een tegenspraak. Beide gevallen (i) en (ii) kunnen niet gelden, en dus vinden we een tegenspraak. ■

Met deze stelling kunnen we nu onmiddellijk een voorbeeld geven van een overaftelbare verzameling.

I.4.10 Gevolg. $\mathscr{P}(\mathbb{N})$ is overaftelbaar.

Bewijs. We bewijzen dit *uit het ongerijmde*. Dat wil zeggen dat we aannemen dat de uitspraak niet waar is, en dan een tegenstrijdigheid afleiden.

Neem dus aan dat $\mathscr{P}(\mathbb{N})$ aftelbaar is. Omdat $\mathscr{P}(\mathbb{N})$ niet eindig is, betekent dit dat er een bijectie $\mathbb{N} \to \mathscr{P}(\mathbb{N})$ is. Zo een bijectie is in het bijzonder surjectief, in tegenspraak met de stelling van Cantor. ■

We zullen later ook bewijzen dat $\mathbb{R}$ overaftelbaar is, maar daarvoor moeten we uiteraard eerst een definitie van $\mathbb{R}$ zien!

Opgaven

1. Hoeveel verschillende bijecties kun je vinden tussen $A = \{a, b, c, d\}$ (met a, b, c, d verschillend) en $B = \{1, 2, 3, 4\}$?

2. Laat zien dat de intervallen $(-1, 1)$ en $(2, 5)$ gelijkmachtig zijn.

3. Laat zien dat $(0, 1)$ en $\mathbb{R}$ gelijkmachtig zijn.

4. Zij $2\mathbb{N}$ de verzameling van alle even natuurlijke getallen. Bewijs dat $2\mathbb{N}$ aftelbaar oneindig is.

5. Laat zien dat de intervallen $[0, 1)$ en $(2, 5]$ gelijkmachtig zijn.

6. Beschouw $A = \{2^{-n} : n \in \mathbb{N}\}$ en $B = \{3^n : n \in \mathbb{N}\}$. Laat zien dat $A \cup B$ aftelbaar is.

✯ **7.** Laat zien dat de afbeelding $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}_{\geq 1}$ gegeven door $f(n, m) = 2^n(2m + 1)$ een bijectie is.

✯ **8.** Bewijs dat $\mathbb{Q}$ aftelbaar is.

✯ **9.** Laat zien dat de afbeelding $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ gegeven door $f(n, m) = \frac{1}{2}(n+m)(n+m+1)+m$ de bijectie uit het bewijs van Stelling I.4.6 is.

10. Zij A een verzameling en $\mathscr{P}(A)$ zijn machtsverzameling. Geef een injectieve afbeelding $f : A \to \mathscr{P}(A)$.

11. Zij $A = \{\varnothing, \{\varnothing\}\}$. Wat is $\mathscr{P}(A)$?

12. Werk uit wat er in het bewijs van Stelling I.4.9 gebeurt in het geval dat $A = \varnothing$.

13. Zij A een verzameling. Laat $\mathscr{F}(A)$ de verzameling van functies $f : A \to \{0,1\}$ zijn.

(a) Laat zien dat de afbeelding $F : \mathscr{F}(A) \to \mathscr{P}(A)$, $f \mapsto f^{-1}\{1\}$ een bijectie is, en beschrijf de inverse.

(b) Zij $f : A \to \mathscr{P}(A)$, en $B \in \mathscr{P}(A)$ als in het bewijs van Stelling I.4.9. Wat is dan het element $F^{-1}(B)$?

(c) Vergelijk deze constructie (f geeft $F^{-1}(B)$) met Cantors diagonaalmethode: `http://nl.wikipedia.org/wiki/Diagonaalbewijs_van_Cantor`.

14. (a) Laat zien dat de vereniging van twee aftelbare verzamelingen aftelbaar is.

(b) Laat zien dat de vereniging van aftelbaar veel aftelbare verzamelingen aftelbaar is.

15. Lees de wikipedia pagina 'Hilbert's paradox of the Grand Hotel': `http://en.wikipedia.org/wiki/Hilbert%27s_paradox_of_the_Grand_Hotel`.

✯ **16.** Bewijs of weerleg:

(a) de intervallen $(0,1)$ en $[0,1)$ zijn gelijkmachtig.

(b) de intervallen $[0,1)$ en $[0,1]$ zijn gelijkmachtig.

(c) de intervallen $(0,1)$ en $[0,1]$ zijn gelijkmachtig.

17. Bewijs dat elke deelverzameling van een aftelbare verzameling aftelbaar is.

I.5 Een echte toepassing: het honderdsmurfenprobleem

Het tweede deel van de titel van deze sectie doet niet erg serieus aan. Toch is de bedoeling heel serieus, namelijk, de lezer te overtuigen dat de in dit hoofdstuk behandelde wiskundige concepten (verzamelingen, afbeeldingen en eigenschappen daarvan) en methoden (probleemanalyse, preciese uitspraken, bewijzen) goed toepasbaar zijn in de échte wereld, en dat ze daarom ons vertrouwen verdienen om gebruikt te worden. We geven een verrassend voorbeeld hiervan uit de speltheorie (het vinden van een strategie met maximale kans op winst).[14] De betekenis van woorden als injectief, surjectief en bijectief zouden deel uit moeten maken van onze algemene culturele kennis. Het is teleurstellend te moeten constateren dat dit meer dan honderd jaar na Hilberts formalisering van de wiskunde nog steeds niet het geval is. Hier ligt een schone taak voor leraren!

Het probleem

We beginnen met het formuleren van het probleem van de honderd smurfen. Gargamel heeft 100 smurfen gevangen. Ze hebben allemaal verschillende namen. Gargamel spreekt ze als volgt toe.

> Ik heb jullie namen op 100 briefjes geschreven, op elk briefje één naam. Die briefjes heb ik in 100 kluisjes in een kamer gelegd, in elk kluisje één briefje. Straks worden jullie in aparte cellen opgesloten, en kunnen jullie niet meer communiceren. Dan worden jullie één voor één in de kamer met de 100 kluisjes gebracht, die allemaal dicht zijn. De kluisjes zijn genummerd van 1 tot en met 100. Eénmaal in de kamer mogen jullie dan in 50 kluisjes kijken, alléén kijken en weer dicht doen, of het papiertje met je naam erin zit. Als ook maar één van jullie het papiertje met zijn eigen naam *niet* vindt, dan worden jullie allemaal aan Azraël gevoerd. Als iedereen *wel* het papiertje met zijn eigen naam vindt, dan zijn jullie vrij. Jullie mogen nog even samen overleggen terwijl ik de briefjes in de kluisjes doe. Succes!

[14] Wie een voorbeeld kent dat dichter bij de praktijk staat wordt verzocht de schrijvers in te lichten.

Ziehier het probleem van de smurfen: wat voor strategie kunnen ze bedenken om een niet verwaarloosbare overlevingskans te hebben? Denk hier vooral zelf over na alvorens verder te lezen. En als je dan verder leest, probeer dan te bedenken waarvoor de dan ingevoerde concepten kunnen dienen. Maak nu eerst opgave I.5.1.

Permutaties

Zij A een verzameling. Een *permutatie van A* is een bijectieve afbeelding $f : A \to A$. De verzameling van permutaties van A noteren we als $\mathrm{Sym}(A)$ (wie moeite heeft met verzamelingen van functies wordt aangeraden opgave I.5.2 te maken). Deze verzameling heeft twee interessante operaties: inverse en samenstelling; voor f en g in $\mathrm{Sym}(A)$ hebben we $g \circ f$ en f^{-1}, ook beide elementen van $\mathrm{Sym}(A)$. Ook heeft $\mathrm{Sym}(A)$ een speciaal element, namelijk id_A, de identieke afbeelding van A. Samen hebben $\mathrm{Sym}(A)$, id_A, de samenstelling en de inverse de volgende eigenschappen:

1. voor alle f, g en h in $\mathrm{Sym}(A)$ geldt: $(h \circ g) \circ f = h \circ (g \circ f)$,
2. voor alle f in $\mathrm{Sym}(A)$ geldt: $\mathrm{id}_A \circ f = f = f \circ \mathrm{id}_A$,
3. voor alle f in $\mathrm{Sym}(A)$ geldt: $f^{-1} \circ f = \mathrm{id}_A = f \circ f^{-1}$.

In de algebra wordt een verzameling die voorzien is van een dergelijke structuur een *groep* genoemd. De groepen van de vorm $\mathrm{Sym}(A)$ zijn van groot belang in de wiskunde.

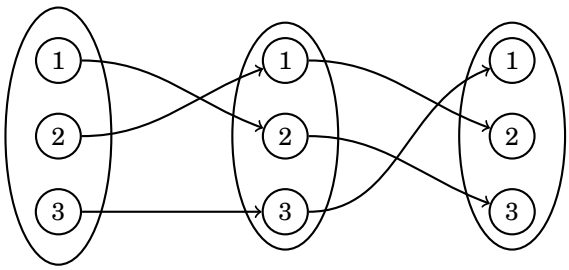
Volgens opgave I.5.3 is $\mathrm{Sym}(A)$ eindig als A eindig is, en geldt, als $n = \#A$, dat $\#\mathrm{Sym}(A) = n!$.

Voor $A = \{1, 2, \ldots, n\}$ is S_n de gebruikelijke notatie voor $\mathrm{Sym}(A)$. Een gebruikelijke notatie voor σ in S_n is $\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{smallmatrix}\right)$. In deze notatie wordt de samenstelling $\sigma \circ \tau$ (éérst τ, dan σ) van σ en τ als volgt uitgerekend:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}$$

Bijvoorbeeld geldt

$$\begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} \circ \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}, \quad \text{en niet} \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}:$$



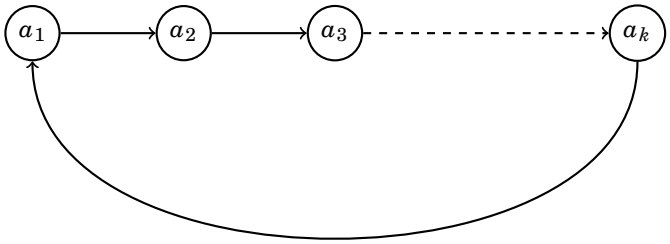
Vanzelfsprekend kan men deze notatie ook voor willekeurige eindige verzamelingen gebruiken, als men eerst de elementen nummert.

Ontbinding in disjuncte cykels

Laat A een eindige verzameling zijn. We introduceren nu een notatie voor elementen van $\mathrm{Sym}(A)$ die veel praktischer is dan de hierboven ingevoerde notatie, waarbij men een complete lijst van originelen en beelden geeft.

Voor $k \in \mathbb{N}_{\geq 1}$ heet een element $\sigma \in \mathrm{Sym}(A)$ een *k-cykel* of *cyclische permutatie van lengte k* als er k verschillende elementen $a_1, \ldots, a_k \in A$ bestaan zo dat σ de

identiteit is op $A \setminus \{a_1,\ldots,a_k\}$ en op $\{a_1,\ldots,a_k\}$ werkt als de cyclische verschuiving



We noteren zo'n element als $(a_1,a_2,\ldots,a_k)$. Let op: deze notatie is niet uniek, want $(a_1,a_2,\ldots,a_k) = (a_2,\ldots,a_k,a_1)$, enzovoorts; elk element in de k-cykel kan de eerste positie innemen. Verder zijn 1-cykels gelijk aan id_A.

Twee cykels $(a_1,a_2,\ldots,a_k)$ en $(b_1,b_2,\ldots,b_l)$ heten *disjunct* als geen enkele a_i gelijk is aan een b_j, met andere woorden, als $\{a_1,a_2,\ldots,a_k\} \cap \{b_1,b_2,\ldots,b_l\} = \varnothing$.

Als σ en τ disjuncte cykels zijn, dan geldt $\sigma\circ\tau = \tau\circ\sigma$, want 'ze bewegen verschillende elementen van A'. Dit heet: σ en τ *commuteren*. Hieruit volgt (Opgave I.5.5) dat voor alle $n \in \mathbb{N}$ geldt dat $(\sigma\circ\tau)^n = \sigma^n\tau^n$. Hierbij definiëren we $\sigma^0 = \mathrm{id}_A$, want dan geldt voor alle $n,m \in \mathbb{N}$ dat $\sigma^{n+m} = \sigma^n \circ \sigma^m$.

De volgende stelling geeft ons de beloofde meer praktische notatie voor permutaties.

I.5.1 Stelling. Zij A een eindige niet-lege verzameling. Dan is ieder element van $\mathrm{Sym}(A)$ een samenstelling van paarsgewijs disjuncte cykels.

Bewijs. We voeren het bewijs met inductie naar $n := \#A$ (in een volgend hoofdstuk zullen we het inductieprincipe uitgebreid behandelen). Als $n = 1$ is id_A het enige element van $\mathrm{Sym}(A)$, en id_A is een 1-cykel. De stelling is in ieder geval correct voor $n = 1$. Laat nu $n > 1$ en neem aan dat de stelling waar is voor verzamelingen met minder dan n elementen. Laat nu A een verzameling met $\#A = n$, en laat $\sigma \in \mathrm{Sym}(A)$. Kiezen we $a \in A$, dan komen er in de oneindige rij $a,\sigma(a),\sigma^2(a),\ldots$ slechts eindig veel verschillende elementen voor. Laat $k > 0$ het kleinste positieve getal zijn waarvoor $\#\{a,\sigma(a),\sigma^2(a),\ldots,\sigma^k(a)\} < k+1$. Dan is er een unieke $j \in \mathbb{N}$ is met $0 \le j < k$ en $\sigma^k(a) = \sigma^j(a)$. Dan passen we σ^{-1} j keer toe en vinden dat $a = \sigma^{k-j}(a)$. De minimaliteit van k betekent dat $j = 0$, en dus $\sigma^k(a) = a$. Laat $A_0 := \{a,\sigma(a),\sigma^2(a),\ldots,\sigma^{k-1}(a)\}$ en $A_1 := A \setminus A_0$. Dan geldt $\#A_0 = k$ en $\#A_1 = n-k$, en $\sigma|_{A_0}$ is een k-cykel. Als $A_1 = \varnothing$ dan is σ dus een k-cykel. Neem nu aan dat A_1 niet leeg is. Omdat $\sigma|_{A_0}$ een permutatie van A_0 is, is $\sigma|_{A_1}$ een permutatie van A_1. Volgens de inductiehypothese is $\sigma|_{A_1}$ een samenstelling van disjuncte cykels. Dus σ is een samenstelling van disjuncte cykels. ∎

De honderd smurfen

Op dit moment zijn we klaar om de smurfen een goede raad te kunnen geven. Maar we willen dat de lezer zelf het plezier ondervindt van het ontdekken van een overlevingsstrategie. Daarom verklappen we het nogal ongelofelijke feit dat er een strategie is voor de smurfen waarmee ze een overlevingskans hebben van $1 - \sum_{k=51}^{100} 1/k \approx 1 - \ln(2) \approx 0.31$. Om de lezer te helpen stellen we wat vragen, hopende dat dat voldoende is om hem/haar op een paar goede ideeën te brengen.[15]

- Stel je voor dat je een smurf bent, en dat je in de kamer met de kluisjes aankomt. Dan moet je een kluisje kiezen, en dan nog 49 andere. Moet het van tevoren afgesproken zijn in welk kluisje je als eerste kijkt, of zou dat aan het toeval kunnen worden overgelaten?

[15] Wie er niet in slaagt en daardoor slapeloze nachten heeft kan de auteurs van deze tekst om een oplossing vragen.

- We beschrijven de situatie wiskundig. Laat dus S de verzameling van smurfen zijn. Als de smurfen afspreken welk kluisje ze als eerste openmaken, dan hebben ze dus een afbeelding $f : S \to \{1,\dots,100\}$ gekozen. Wat voor afbeelding zouden ze moeten kiezen? Is het zinvol als ze allemaal hetzelfde kluisje als eerste openmaken?
- Wat zit er ook alweer in de kluisjes? Geeft dat ook een afbeelding?

Als je een idee hebt voor de strategie van de smurfen, maar dan moeite hebt met het berekenen van de kans dat ze overleven, kun je natuurlijk eerst eens kijken naar het geval dat er minder smurfen zijn.

Veel plezier!

Opgaven

1. Bereken de kans dat de 100 smurfen overleven, als ze allemaal willekeurig, volgens toeval, 50 kluisjes kiezen.

2. Schrijf alle elementen van $\mathrm{Sym}(\varnothing)$, $\mathrm{Sym}(\{1\})$, $\mathrm{Sym}(\{1,2\})$ en $\mathrm{Sym}(\{1,2,3\})$ op.

3. Laat A een eindige verzameling zijn, en laat $n = \#A$. Bewijs dat $\mathrm{Sym}(A)$ eindig is en dat $\#\mathrm{Sym}(A) = n!$.

4. Laat $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{smallmatrix}\right) \in \mathrm{S}_{12}$.

(a) Geef σ^{-1} in dezelfde notatie.

(b) Geef σ als samenstelling van disjuncte cykels.

(c) Bereken σ^{2015} (samenstelling van 2015 σ's).

5. Laat A een eindige verzameling zijn, $r \in \mathbb{N}_{\geq 1}$, en $\sigma_1,\dots,\sigma_r$ paarsgewijs disjuncte cykels zijn in $\mathrm{Sym}(A)$. Bewijs dat voor alle $n \in \mathbb{N}$ geldt dat

$$(\sigma_1 \circ \cdots \circ \sigma_r)^n = \sigma_1^n \circ \cdots \circ \sigma_r^n.$$

I.6 Enkele historische opmerkingen

Georg Cantor (Duits wiskundige, 1845–1918)[16] kwam door zijn werk aan trigonometrische reeksen ($\sum_{n\geq 0} a_n \cos(nx) + \sum_{n>0} b_n \sin(nx)$) tot de noodzaak systematischer dan daarvóór eigenschappen van deelverzamelingen van $\mathbb{R}$ te bestuderen. Bijvoorbeeld wilde hij verschil maken tussen aftelbare en overaftelbare deelverzamelingen. De verzamelingentheorie was aldus geboren, rond 1870.

Niet iedereen was gelukkig met deze nieuwe tak aan de boom van de wiskunde. Sterker, sommigen waren ronduit vijandig tegen dit soort ideeën. Kronecker, die het standpunt innam dat wiskunde constructief moest zijn, moest niets van hebben van dit soort nieuwlichterij dat er bijecties zouden bestaan tussen $\mathbb{R}$ en $\mathbb{R}^2$; hij noemde Cantor "een bederver van de jeugd". Henri Poincaré noemde verzamelingentheorie "een ernstige ziekte die de wiskunde had geïnfecteerd".

Daarentegen zag David Hilbert wél het belang van Cantors werk in, met name voor zijn eigen programma om de wiskunde van een stevig fundament te voorzien. Een bekend citaat van Hilbert is "Niemand zal ons verdrijven uit het paradijs dat

[16] `http://www-history.mcs.st-and.ac.uk/` is een prachtige website met levensbeschrijvingen van veel wiskundigen

Cantor heeft gecreëerd". Uiteindelijk heeft Hilbert gelijk gekregen: verzamelingentheorie is nu de 'standaardtaal' geworden waarin alle wiskunde wordt geschreven.

Het zou mooi zijn als termen als injectief, surjectief en bijectief algemener bekend waren, want ze zijn de moeite waard. Het neerbuigend doen over verzamelingentheorie omdat het zo triviaal is dat er niet over hoeft te worden nagedacht, of het doen alsof het iets onbegrijpelijks voor nerds is, zou niet meer van deze tijd moeten zijn.

Enige problemen die tot verwarring leidden in de ontwikkeling van de verzamelingentheorie en de formalisering van de wiskunde zijn sindsdien opgelost. Cantors informele opzet is door Zermelo (1908) met een toevoeging van Fraenkel (1922) geaxiomatiseerd (niet vastleggen wat de objecten zijn, maar wel vastleggen wat hun gedrag is), vanwaar de letters 'Z' en 'F' in de naam 'ZFC' van het axiomastelsel (de 'C' staat voor het keuzeaxioma). Voor een beschrijving van dit axiomastelstel zie Appendix VIII.2.

Een belangrijke vraag is of er verzamelingen zijn die strikt groter zijn dan $\mathbb{N}$ en strikt kleiner zijn dan $\mathbb{R}$. De *continuüm hypothese* (CH) zegt dat dit niet zo is. De vraag of CH waar of onwaar is, is probleem nummer 1 op Hilberts lijst (1900) van de 23 belangrijkste problemen voor de 20ste eeuw. In 1940 bewees Gödel dat als ZFC consistent is, dat dan ZFC+CH consistent is, en in 1963 bewees Cohen dat als ZFC consistent is, dat dan ZFC+*niet*CH consistent is.

Een minder belangrijk maar grappiger probleem is de *Banach-Tarski paradox* waarover de opgave hieronder.

Opgaven

1. Lees `http://en.wikipedia.org/wiki/Banach-Tarski_paradox` en vergelijk met `http://nl.wikipedia.org/wiki/Banach-tarskiparadox`. Voor leuke artikelen hierover, zie [French] en [Hart].

I.7 Over verzamelingen in de schoolwiskunde

Hierboven wordt opgemerkt dat heel de wiskunde in termen van verzamelingenleer kan worden geformuleerd. Dat heeft grote voordelen: alle onderdelen van de wiskunde worden verbonden door ze in de verzamelingenleer een gemeenschappelijke basis te geven, je hebt in de axiomatische opbouw alleen axioma's nodig voor verzamelingen en je hebt een heldere, eenduidige, gemeenschappelijke taal. Vanuit didactisch oogpunt heeft het echter ook nadelen. Verzamelingen zijn bijvoorbeeld hele statische objecten, terwijl je bij bijvoorbeeld functies soms graag in termen van beweging denkt. Er zullen ook maar weinig mensen zijn die in de dagelijkse omgang met het getal 3 dit beschouwen als $\{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$, zoals in Appendix VIII.3 gebeurt.

Desalniettemin was men zo gecharmeerd van de verzamelingenleer dat men in de jaren '60 van de vorige eeuw de verzamelingenleer, met de bijbehorende axiomatische opbouw van de wiskunde, ook in het voortgezet onderwijs stevig wilde neerzetten. Dit wordt de *New Math*-beweging genoemd. Dit is bijvoorbeeld het begin van de methode *Moderne wiskunde* uit 1968 - het betreft het brugklasboek

voor alle niveaus:

Algebra

1. Verzamelingen

{1, 2, 3, 4, 5, 6, 7}

{a, e, i, o, u}

§ 1. Inleiding

Dit eerste hoofdstuk van je wiskundeboek gaat over *verzamelingen*. Je bent al gewend te spreken over „mijn verzameling postzegels" of „de verzameling suikerzakjes van mijn broertje".
Het is echter ook mogelijk een bepaald groepje mensen een verzameling te noemen. Voorbeelden zijn: het eerste elftal van Ajax, de gemeenteraad van Middelburg, de dansclub „De Skotse Trije" uit Sneek.
De zwerm bijen in de tuin van mijn buurman is een verzameling dieren.

Er zijn in onze taal veel woorden, die een verzameling aanduiden, bijvoorbeeld: onze *klas* leerlingen, het *paar* schoenen dat ik aan heb, het *spel* schaakstukken van mijn vader.

OPDRACHT

Bedenk zelf een paar voorbeelden van verzamelingen. Denk daarbij aan woorden als kudde, school en dergelijke.

Als leerlingen gevraagd werd een kwadratische vergelijking op te lossen, zou hun oplossingsproces er veertig jaar geleden zo uit hebben moeten zien[17]:

$$\{x \in \mathbb{R} : x^2 - 5x + 6 = 0\} = \{x \in \mathbb{R} : (x-2)(x-3) = 0\} =$$
$$\{x \in \mathbb{R} : x - 2 = 0\} \cup \{x \in \mathbb{R} : x - 3 = 0\} = \{2, 3\}.$$

In havo en vwo heeft deze aanpak, mede door toedoen van Hans Freudenthal, nooit echt voet aan de grond gekregen. Op mavo (het oude vmbo-t) echter wel, zoals blijkt

[17] Uit: Goffree, *Honderd jaar wiskundeonderwijs*.

uit deze examenopgaven uit 1968 en 1969[18]:

Als $(9,2) \in \{(x,y) : 5x + py = 39\}$, dan is p gelijk aan
a. -6
b. -3
c. 3
d. dat kan men niet weten

A = {gelijkbenige driehoeken},
B = {rechthoekige driehoeken},
C = {gelijkzijdige driehoeken}.
Dan geldt:
a. $A \cap B = \varnothing$
b. $A \cap C = \varnothing$
c. $B \cap C = \varnothing$
d. geen van deze beweringen is juist

Overigens was het probleem dat veel docenten het nut van de invoering van verzamelingenleer niet begrepen. Erger nog, het blijkt dat ook de schoolboekauteurs er soms een rommeltje van maakten.

Hier zijn nog twee opgaven uit *Moderne wiskunde*:

5. In figuur 8 zijn de volgende verzamelingen voorgesteld:

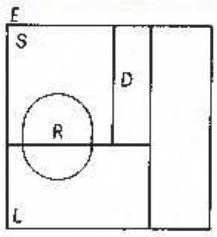


Fig.8

E is de verzameling van de in 1946 in ons land gebruikte machines. S, D, L en R zijn deelverzamelingen van E.
S is de verzameling van de stoommachines
D is de verzameling van de machines met dieselmotor
L is de verzameling van de elektrisch aangedreven machines
R is de verzameling van de spoorweglokomotieven.

Maak zo'n diagram waarvan je veronderstelt, dat het overeenkomt met de toestand van 1970.

1 Onderzoek of de volgende beweringen waar zijn of niet waar zijn:

a. De verzameling van de leerlingen in je klas die langer zijn dan 2 m is $\varnothing$.

b. Als $A = \{v, x, z, q, k\}$ en $B = \{x, z, p\}$, dan is $B \subset A$.

c. Voor deze verzamelingen A en B is $A \cap B = \{x, z\}$.

d. 23 behoort tot de verzameling van de delers van 506.

e. Elke verzameling heeft minstens één element.

f. Als K de verzameling is van de klinkers en L die van de letters, dan is $K \subset L$.

g. Als $x \in A$ en $A \subset B$, dan is $x \in B$.

h. Als $X \subset Y$, dan is $X \cap Y = X$.

i. Als $A \cap B = C$, dan is $C \subset A$ en $C \subset B$.

[18] ibid.

I.8 Over functies in de schoolwiskunde

We hebben gezien dat domein en codomein onderdeel uitmaken van de definitie van een functie. Als je een functie introduceert, moet je dus vermelden wat domein en codomein zijn - anders is het betekenisloos. In de schoolwiskunde, waar we bijna alleen werken met functies van een deelverzameling van $\mathbb{R}$ naar $\mathbb{R}$, doet men dit niet. Daar is het heel gebruikelijk om te vragen: "Bepaal het domein van de functie $f(x) = \sqrt{2-x}$."

Merk overigens op dat in dit zinnetje nog iets gebeurt dat niet past bij de definities uit deze tekst. Je zou moeten spreken over "de functie $f : \mathbb{R} \to \mathbb{R}$, die gegeven wordt door $f(x) = \sqrt{2-x}$." Immers is $f(x)$ een *functiewaarde* en niet de functie zelf. Hoe het ook zij, de genoemde gebruiken zijn ingesleten in de schoolwiskunde en aangezien het werkt, doet bijna niemand er moeilijk over.

In de tekst is opgemerkt dat een functie kan worden gegeven door een formule, een grafiek of een tabel. Een belangrijke vaardigheid, die met name centraal staat in vmbo, is om deze representaties in elkaar om te zetten. De didactiek die hierbij hoort, is die van *vertaalvaardigheden*.

Hoewel functies in de schoolwiskunde, wanneer ze expliciet onder die naam worden gebruikt, bijna altijd functies van een deelverzameling van $\mathbb{R}$ naar $\mathbb{R}$ zijn, kom je ook nog andere voorbeelden tegen. Hier zijn enkele voorbeelden:

- Symmetrieën in de onderbouw. Een symmetrie van het vlak is een functie $f : \mathbb{R}^2 \to \mathbb{R}^2$ die afstanden behoudt. In de schoolwiskunde wordt een symmetrie echter niet als functie gedefinieerd (waaruit blijkt dat de verzamelingenleer inderdaad niet ver in de schoolwiskunde is doorgedrongen). Merk overigens op dat het gebruik van functies voor symmetrieën lastige didactische uitdagingen met zich zou meebrengen. Is bijvoorbeeld s_i (met $i = 1,2$) spiegelen in een bepaalde lijn ℓ_i, dan betekent $s_1 \circ s_2$ volgens onze definitie van samenstellen van functies: eerst spiegelen in ℓ_2 en daarna in ℓ_1 – anders dan we zouden verwachten.
- In vwo Wiskunde B komen parametervoorstellingen voor. Dit zijn functies $f : \mathbb{R} \to \mathbb{R}^2$. Bij Wiskunde D komen complexe functies aan bod. Functies $f : \mathbb{R}^2 \to \mathbb{R}$ komen we, enigszins impliciet, tegen als families van functies f_a. Het begrip inversefunctie heeft een plaats in Wiskunde B.
- Hoewel voor kansen bij Wiskunde A een functienotatie $P(\cdots)$ wordt gebruikt, wordt geen duidelijkheid gegeven over wat het domein van deze 'kansfunctie' zou kunnen zijn.

II LOGICA

Dit hoofdstuk gaat over de *vorm* van wiskundige uitspraken en de *methodes* die in de wiskunde worden gebruikt om waarheid vast te stellen. We kijken hier op metaniveau naar wiskunde. De *mathematische logica* probeert te beschrijven wat correcte uitspraken zijn en daar is dit vakgebied in hoge mate succesvol in. Wiskundigen over de hele wereld zijn zeer eensgezind in wat zij acceptabele formuleringen en bewijzen vinden — alleen in uithoeken van de wiskunde wijkt men hier soms wel eens van af en zelfs dan kan men precies uitleggen wát er anders is. Het is kenmerkend voor wiskunde dat het zich zo 'exact' en eenvoudig laat beschrijven - de 'echte' wereld, met empirische disciplines zoals onderwijskunde, laat zich helaas niet goed in zo'n kader vangen. Je kunt echter wel proberen zo precies en gestructureerd mogelijk te werken en deze vaardigheid van *analytisch denken* wordt vaak beschouwd als een van de doelen van het schoolvak wiskunde.

II.0.1 Voorbeeld. Wiskundige uitspraken zijn ondubbelzinnig: iedere uitspraak heeft een unieke interpretatie. In het gewone taalgebruik is dat niet het geval en daarom is gewone taal dus niet zonder meer bruikbaar in de wiskunde. Bekijk de zin "De man zag de piramide op de heuvel met een verrekijker." In Figuur 2.1 staan twee interpretaties van deze zin getekend. Je kunt er zelf nog twee verzinnen[1].

Figuur 2.1 – Twee interpretaties van de zin "De man zag de piramide op de heuvel met een verrekijker."

II.0.2 Voorbeeld. Wiskundige uitspraken zijn precies. Om dat te bereiken, moeten er heldere afspraken worden gemaakt over de betekenis van symbolen en woorden. Dat is in de wiskunde veel makkelijker dan in bijvoorbeeld de rechtswetenschappen. Een belangrijke taak van de Hoge Raad, het hoogste rechtsprekende orgaan in Nederland, is het duiden van de interpretatie van wetteksten. Regelmatig valt de Hoge Raad daarbij terug op de vermeende 'intentie van de wetgever'.

[1] Uit lesmateriaal *Logisch redeneren* van Doorman en Roodhart voor Wiskunde C.

II.1 Propositielogica

Een *propositie* is een uitspraak die danwel waar, danwel onwaar (niet waar) is[2]. Dergelijke uitspraken staan in de wiskunde centraal. Wiskundeboeken staan bijvoorbeeld vol met *stellingen*: dit zijn proposities waarvan de waarheid door middel van een bewijs is vastgesteld.

II.1.1 Voorbeeld. Bekijk de propositie: "Iedere functie $f : \mathbb{R} \to \mathbb{R}$ heeft een nulpunt en $3 + 5 = 8$" (uiteraard is deze propositie niet waar). In dit geval valt op dat de propositie eigenlijk uit twee proposities bestaat. De vorm is 'P en Q', waarbij P de propositie "iedere functie $f : \mathbb{R} \to \mathbb{R}$ heeft een nulpunt" is en Q de propositie "$3 + 5 = 8$." In de logica gaat het over de *vorm* en niet over de *inhoud*: we zien een uitspraak van de vorm 'P en Q'; dat onze proposities P en Q over functies en getallen gaan, is daarbij niet relevant. ∎

Conjunctie

Een propositie van de vorm 'P en Q' heet een *conjunctie*. We noteren het symbolisch als

$$P \wedge Q.$$

Een conjunctie is vaak herkenbaar aan het woordje 'en', maar niet altijd: 'zowel P als Q' is bijvoorbeeld ook een formulering die een conjunctie aangeeft. Een uitspraak over twee proposities P en Q is een conjunctie als het geïnterpreteerd moet worden als "de uitspraak is waar precies dan als P en Q beide waar zijn."

De letters P en Q zijn *propositievariabelen*. Substitueren we voor P en Q concrete proposities, dan hangt de waarheid van de propositie $P \wedge Q$ alleen af van de waarheid van P en Q. Deze afhankelijkheid kunnen we aangeven in een *waarheidstabel*, waarvan links in Figuur 2.2 die van de conjunctie is weergegeven. In een waarheidstabel staat 0 voor onwaar en 1 voor waar.

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

P	$\neg P$
0	1
1	0

Figuur 2.2 – Drie waarheidstabellen. Van links naar rechts die van conjunctie, disjunctie en negatie. De op-een-na-laatste regel van de linker tabel zegt bijvoorbeeld: "als P waar is en Q onwaar, dan is $P \wedge Q$ onwaar."

Disjunctie

Een ander voorbeeld van een samengestelde proposities is de *disjunctie*. Een disjunctie heeft de vorm 'P of Q', hetgeen we noteren als

$$P \vee Q.$$

De waarheidstabel van de conjunctie is de middelste in Figuur 2.2. Deze waarheidstabel leidt tot de volgende interpretatie: "Substitueren we voor P en Q proposities, dan is $P \vee Q$ waar, precies dan als minstens één van de proposities P en Q waar is."

[2] Achter deze simpele definitie gaan een hoop filosofische nuances schuil. Binnen de kaders van deze tekst gaan we daar niet op in.

II.1.2 Opmerking. In de wiskunde is *afgesproken* het woordje 'of' op deze manier te interpreteren, want in het dagelijks taalgebruik komt regelmatig de interpretatie van *exlusieve-of* voor: of P is waar, of Q is waar, maar niet allebei. Zie Opgave II.1.1.

Ook het woordje 'en' wordt in het dagelijks taalgebruik vaak anders gebruikt, namelijk om een tijdsvolgordelijkheid aan te geven: "Hij kwam te laat en miste zijn vlucht" betekent iets anders dan "Hij miste zijn vlucht en kwam te laat". Dit laat zien dat in het dagelijks taalgebruik 'en' niet *commutatief* is. In de wiskunde is dat wel het geval: $P \wedge Q$ en $Q \wedge P$ hebben dezelfde interpretatie. Ook $\vee$ is commutatief.

Negatie

De *ontkenning* of *negatie* van P noteren we als

$$\neg P.$$

Per definitie geldt dat $\neg P$ waar is precies dan als P onwaar is. De waarheidstabel van de negatie staat rechts in Figuur 2.2. Een ontkenning herken je vaak aan het woordje 'niet', dat soms kan zijn opgenomen in notaties: $2 \neq 3$, $-1 \notin \mathbb{N}$.

We noemen negatie, conjunctie en disjunctie *logische operatoren*. Met behulp hiervan kun je willekeurig lange samengestelde propositie maken, zoals die van de vorm

$$(\neg P) \vee (Q \wedge (R \wedge S)).$$

Merk op dat we haakjes moeten gebruiken om aan te geven hoe de uitspraak geïnterpreteerd moet worden. In Opgave II.1.2 zul je zien dat de volgorde bij combinaties met enkel één soort logische operatoren van geen belang is — bijvoorbeeld zijn de proposities

$$(P \wedge Q) \wedge R \qquad \text{en} \qquad P \wedge (Q \wedge R)$$

beide waar precies dan als zowel P, als Q, als R waar is en daarom kunnen we de haakjes weglaten:

$$P \wedge Q \wedge R.$$

Bij combinaties van negaties, conjuncties en disjuncties zijn haakjes echter wel essentieel. Hier moeten we dus preciezer zijn dan in de normale taal gebruikelijk is, waar we nooit haakjes gebruiken (hoewel we meestal wel begrijpen hoe we het moeten interpreteren). We maken één afspraak, namelijk dat negatie voor disjunctie en conjunctie gaat. Dus

$$\neg P \wedge Q$$

moet geïnterpreteerd worden als

$$(\neg P) \wedge Q \qquad \text{(en niet als } \neg(P \wedge Q)\text{)}.$$

Logisch equivalent

Bij waarheidstabellen van samengestelde proposities kun je de tabel in stapjes opbouwen. Dat is in Figuur 2.3 gebeurd voor de propositie $\neg(\neg P \wedge \neg Q)$. In de figuur is ook nogmaals de waarheidstabel van de disjunctie $P \vee Q$ opgenomen. Beide proposities[3] zijn op dezelfde manier afhankelijk van de waarheid van P en Q — ze zijn logisch equivalent. In het algemeen geldt dat twee proposities die samen afhangen van propositievariabelen $P_1, P_2, \ldots, P_n$ *logisch equivalent* zijn, als hun waarheid op dezelfde manier afhangt van de waarheid van $P_1, P_2, \ldots, P_n$.

P	Q	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg(\neg P \wedge \neg Q)$
0	0	1	1	1	0
0	1	1	0	0	1
1	0	0	1	0	1
1	1	0	0	0	1

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

Figuur 2.3 – Links de waarheidstabel van $\neg(\neg P \wedge \neg Q)$ en rechts die van de disjunctie $P \vee Q$. Deze uitspraken zijn logisch equivalent.

Implicatie

Er zijn nog twee belangrijke logische operatoren die in de wiskunde gebruikt worden: de *implicatie* $\Rightarrow$ en de *bi-implicatie* $\Leftrightarrow$. De waarheidstabellen staan in Figuur 2.4. De implicatie $P \Rightarrow Q$ herken je vaak de formulering 'als P, dan Q.' De bi-implicatie $P \Leftrightarrow Q$ kent meerdere formuleringen, die niet alle even fraai zijn: 'P dan en slechts dan als Q,' 'P als en slechts als Q,' 'P precies dan als Q,' 'P is equivalent met Q,' 'een noodzakelijke en voldoende voorwaarde voor P is Q.' Er geldt (Opgave II.1.5):

$$\begin{array}{lll} P \Leftrightarrow Q & \text{is logisch equivalent met} & (P \Rightarrow Q) \wedge (Q \Rightarrow P), \\ P \Rightarrow Q & \text{is logisch equivalent met} & Q \vee \neg P. \end{array}$$

II.1.3 Opmerking. Bij het gebruik van implicaties in de wiskunde zijn er twee veelvoorkomende verwarring:

- Een implicatie wordt geïnterpreteerd als een bi-implicatie. Een docent zegt bijvoorbeeld tegen zijn klas: "Als iedereen voor de toets een voldoende haalt, trakteer ik op taart." De volgende les trakteert de docent op taart, maar dat betekent nog niet dat iedereen een voldoende heeft gehaald! Misschien is de docent wel jarig of zo. Bij het oplossen van vergelijkingen kom je de volgende situatie vaak tegen: begin met de vergelijking die moet worden opgelost; schrijf gevolgen op en werk toe naar een uitspraak die er uitziet als een antwoord; stel vervolgens dat de gevonden uitspraak ook echt het antwoord is (zie Figuur 2.5). Men heeft hier onbewust aangenomen dat er in ieder gevolg steeds sprake is van een bi-implicatie.
- Een implicatie $P \Rightarrow Q$ wordt geïnterpreteerd als 'P is waar en dus is Q ook waar.' Ook dat zie je vaak in handgeschreven uitwerkingen, waar leerlingen het pijltje '$\Rightarrow$' gebruiken in de betekenis van 'daaruit volgt' (de driepuntjesnotatie $\therefore$ zou hier wel correct zijn). Zelfs de schoolboeken leren dit aan, bijvoorbeeld bij de euclidische meetkunde in vwo Wiskunde B of D (Figuur 2.5).

P	Q	$P \Rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

P	Q	$P \Leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

Figuur 2.4 – De waarheidstabellen van implicatie en bi-implicatie.

[3] Vanaf dit moment introduceren we een kleine slordigheid in het taalgebruik. Een uitdrukking als $P \vee Q$ is eigenlijk geen propositie. Pas als we concrete proposities voor P en Q substitueren, krijgen we een propositie.

scan leerlinguitwerking en scan schoolboek

Figuur 2.5 – Twee veelgemaakte fouten rondom implicaties. Links: bij het oplossen van vergelijkingen worden vaak impliciet omgekeerde implicaties gebruikt. Rechts: het pijltje krijgt soms de betekenis van 'daaruit volgt'.

Opgaven

✍ **1.** In deze opgave introduceren we de logische operator *exclusief of* (ook wel 'XOR'), die we met $\veebar$ zullen noteren. De waarheidstabel is als volgt:

P	Q	$P \veebar Q$
0	0	0
0	1	1
1	0	1
1	1	0

(a) Geef een definitie van $P \veebar Q$ in termen van de logische operatoren $\vee$, $\wedge$ en $\neg$ en bewijs dat je definitie correct is.

(b) Met $\veebar$ en $\wedge$ kun je omgekeerd de logische operator $\vee$ definiëren. Doe dat.

2. Gebruik bij de volgende onderdelen steeds een waarheidstabel.

(a) Laat zien dat $\vee$ associatief is — met andere woorden: laat zien dat $P \vee (Q \vee R)$ logisch equivalent is met $(P \vee Q) \vee R$.

(b) Doe hetzelfde voor $\wedge$.

(c) Laat zien dat $P \vee (Q \wedge R)$ en $(P \vee Q) \wedge R$ niet logisch equivalent zijn.

Het gedrag van $\wedge$ en $\vee$ doet je misschien denken aan het gedrag van optellen en vermenigvuldigen. Ook optellen en vermenigvuldigen zijn immers associatief, terwijl in combinaties van optellen en vermenigvuldigen de volgorde waarin je de bewerkingen uitvoert belangrijk is. Voor combinaties van optellen en vermenigvuldigen in er een distributieve wet: $x \cdot (y+z) = x \cdot y + x \cdot z$.

(d) Onderzoek of zo'n distributieve wet ook bestaat voor $\wedge$ en $\vee$.

3. Deze opgave gaat over de *wetten van De Morgan*:

$$\begin{array}{lll} \neg(P \vee Q) & \text{is logisch equivalent met} & \neg P \wedge \neg Q \\ \neg(P \wedge Q) & \text{is logisch equivalent met} & \neg P \vee \neg Q \end{array}$$

(a) Bewijs deze wetten.

(b) Generaliseer de wetten naar langere conjuncties en disjuncties: $\neg(P_1 \vee P_2 \vee \cdots \vee P_n)$ en $\neg(P_1 \wedge P_2 \wedge \cdots \wedge P_n)$.

De wetten van de Morgan hebben een analogon in de verzamelingenleer. Hierbij spelen vereniging en doorsnede de rol van 'of' en 'en' en wordt de negatie vervangen door het complement.

(c) Geef de corresponderende wetten voor verzamelingen.

(d) Geef een heuristisch 'bewijs' voor deze wetten door venndiagrammen te tekenen.

4. Deze opgave gaat over het concept *logische equivalentie*.

(a) Bewijs dat twee proposities P en Q logisch equivalent zijn, als en slechts dan als de propositie $P \Leftrightarrow Q$ waar is.

(b) Toon aan dat de proposities P en $P \wedge (Q \vee \neg Q)$ logisch equivalent zijn. (In twee equivalente proposities hoeven dus niet precies dezelfde propositievariabelen voor te komen.)

5. (a) Bewijs met behulp van een waarheidstabel dat $P \Rightarrow Q$ logisch equivalent is met $Q \vee \neg P$.

(b) Vind een propositie waarin je naast P, Q en haakjes enkel de logische operatoren $\neg$ en $\wedge$ gebruikt, die logisch equivalent is met $P \Rightarrow Q$.

6. Een *tautologie* is een propositie die voor alle waarden van de propositievariabelen waar is. Een voorbeeld van zo'n tautologie is $P \vee \neg P$.

(a) Toon aan dat $P \vee \neg P$ inderdaad een tautologie is.

(b) Toon aan dat $P \Rightarrow P$ een tautologie is.

(c) Onderzoek of $P \Rightarrow (Q \Rightarrow P)$ een tautologie is.

(d) Onderzoek of $Q \Rightarrow (Q \Rightarrow P)$ een tautologie is.

(e) Onderzoek of $\neg P \Leftrightarrow (P \Rightarrow (Q \wedge \neg Q))$ een tautologie is.

(f) Bedenk zelf nog drie tautologieën.

II.2 Kwantoren

De propositielogica uit de vorige paragraaf is nog niet toereikend. In de wiskunde kom je vaak uitspraken zoals deze tegen: "voor alle getallen x geldt ...." Op de plaats van de puntjes komt dan een uitspraak waarin het getal x voorkomt en dat we met $P(x)$ zullen noteren. Strikt genomen is $P(x)$ hier geen propositie, maar een *propositiefunctie*: $P(x)$ is pas een uitspraak die waar of niet waar is als je voor x een concreet getal substitueert.

Neem een verzameling U. We introduceren de volgende symbolen:

- de *universele kwantor*: $\forall_{x \in U} P(x)$ betekent "voor alle $x \in U$ is $P(x)$ waar" ($\forall$ is de letter A van 'Alle' op zijn kop);
- de *existentiekwantor*: $\exists_{x \in U} P(x)$ betekent "er bestaat een $x \in U$ waarvoor $P(x)$ waar is" ($\exists$ is een gespiegelde E van 'Er is' of 'Existeert').

II.2.1 Voorbeeld. Het beroemde *vermoeden van Goldbach* luidt:

Ieder even getal groter dan 2 is de som van twee priemgetallen.

Met behulp van de verzamelingen E van even getallen en P van priemgetallen kan dit vermoeden als volgt worden genoteerd:

$$\forall_{n \in E}(n > 2 \Rightarrow \exists_{p \in P} \exists_{q \in P}(n = p + q)).$$

Zie Opgave II.2.1 en II.2.2 voor een uitgebreidere analyse. ∎

II.2.2 Voorbeeld. De tussenwaardestelling uit de analyse zegt dat de grafiek van een continue functie $\mathbb{R} \to \mathbb{R}$ een nulpunt heeft zodra één punt van de grafiek onder en een ander punt van de grafiek boven de x-as ligt. Deze stelling zou je als volgt kunnen formuleren, waarbij $C^0(\mathbb{R})$ de verzameling continue functies $\mathbb{R} \to \mathbb{R}$ is:

$$\forall_{f \in C^0(\mathbb{R})} \forall_{a \in \mathbb{R}} \forall_{b \in \mathbb{R}} \big(f(a)f(b) < 0 \Rightarrow \exists_{x \in \mathbb{R}}(f(x) = 0)\big).$$

(De tussenwaardestelling wordt meestal sterker geformuleerd: het domein hoeft niet heel $\mathbb{R}$ te zijn en x kan tussen a en b worden gekozen — deze details laten we voor het gemak hier achterwege.) ∎

II.2.3 Voorbeeld. In het vorige hoofdstuk ben je al enige kwantoren tegengekomen. Zo is volgens Definitie I.3.1 een *functie* een geordend tripel (A,B,f) met $f \subset A \times B$ dat voldoet aan de volgende eigenschap:

$$\text{voor alle } a \in A \text{ is er een } \textit{unieke } b \in B \text{ zodat } (a,b) \in f.$$

In onze symbolen ziet dat er zo uit:

$$\forall_{a\in A}\Big(\exists_{b\in B}((a,b)\in f) \wedge \forall_{b\in B}\forall_{b'\in B}\big(((a,b)\in f \wedge (a,b')\in f) \Rightarrow b = b'\big)\Big).$$

Vaak wordt dit afgekort tot

$$\forall_{a\in A}\exists!_{b\in B}((a,b)\in f),$$

waarbij '$\exists!$' uitdrukt dat er een *uniek* element bestaat. Zie verder Opgave II.2.3. ∎

II.2.4 Opmerking. Wederom biedt de taal veel variatie. Zeg je bijvoorbeeld: "Deze vergelijking heeft een oplossing", dan herken je hier het impliciete gebruik van een existentiekwantor. Kwantoren lijken soms verborgen ("de oppervlakte van een driehoek is een half keer basis keer hoogte"). Met name in schoolboeken is men niet altijd duidelijk in welke kwantoren men gebruikt. Zo vindt je de formule

$$\sin(2x) = 2\sin(x)\cos(x),$$

waarmee bedoeld wordt dat deze gelijkheid geldt *voor alle* $x \in \mathbb{R}$, terwijl elders

$$\sin(2x) = \sin(x)$$

juist een uitnodiging is om deze vergelijking op te lossen (want *er is* ...). In literatuur over algebradidactiek vind je meer informatie over de verschillende *rollen van variabelen* in de schoolwiskunde.

Volgorde

Ook bij het gebruik van kwantoren is de volgorde belangrijk. We doen een aantal observaties:

- Kwantoren van dezelfde soort commuteren. Dat betekent dat $\forall_{x\in U}\forall_{y\in V}(P(x,y))$ en $\forall_{y\in V}\forall_{x\in U}(P(x,y))$ logisch equivalent zijn en idem voor twee keer $\exists$ achter elkaar. Soms worden de kwantoren daarom zelfs als één genoteerd: $\forall_{x,y\in W}$ betekent $\forall_{x\in W}\forall_{y\in W}$.
- Bij verschillende kwantoren is het anders: $\forall_{x\in U}\exists_{y\in V}(P(x,y))$ is wat anders dan $\exists_{y\in V}\forall_{x\in U}(P(x,y))$. In Opgave II.2.5 gaan we hier nader op in.
- Bij verwisselen van een kwantor en negatie, verandert de soort kwantor:

$$\begin{array}{lll} \neg\forall_{x\in U}P(x) & \text{is logisch equivalent met} & \exists_{x\in U}\neg P(x); \\ \neg\exists_{x\in U}P(x) & \text{is logisch equivalent met} & \forall_{x\in U}\neg P(x). \end{array}$$

Opgaven

✍ **1.** Zij E de verzameling van even getallen en $P = \{2,3,5,\ldots\}$ de verzameling priemgetallen.

(a) Vind een propositiefunctie $V(x)$, uitgedrukt in logische symbolen en $+$, zodat geldt

$$E = \{x \in \mathbb{Z} : V(x)\}.$$

(b) Vind ook een propositiefunctie $W(x)$ zodat geldt

$$P = \{x \in \mathbb{N} : W(x)\}.$$

2. In Voorbeeld II.2.1 is het vermoeden van Goldbach als volgt geformuleerd:

$$\forall_{n\in E}(n > 2 \Rightarrow \exists_{p\in P}\exists_{q\in P}(n = p + q)).$$

Hier is een alternatieve formulering:

$$\forall_{n\in E}\exists_{p\in P}\exists_{q\in P}(n > 2 \Rightarrow (n = p + q)).$$

Bewijs dat beide formulering equivalent zijn.

3. Zij U een verzameling en $P(x)$ een propositiefunctie over elementen $x \in U$. In Voorbeeld II.2.3 is al even de kwantor '$\exists!$' geïntroduceerd die uitdrukt dat er een uniek element bestaat.

(a) Vind een propositie die equivalent is met $\exists!_{x\in U}P(x)$, waarin enkel de kwantoren $\forall$ en $\exists$ voorkomen.

(b) Vind een propositie waarin enkel de kwantoren $\forall$ en $\exists$ voorkomen, die uitdrukt dat er precies twee elementen x zijn waarvoor $P(x)$ geldt.

4. Bewijs of weerleg:

(a) $\forall_{x\in\varnothing}(x = x)$.

(b) $\forall_{x\in\varnothing}(x \neq x)$.

(c) $\exists_{x\in\varnothing}(x = x)$.

(d) $\exists_{x\in\varnothing}(x \neq x)$.

5. Toon met een voorbeeld aan dat de volgorde van *verschillende* kwantoren uitmaakt: $\forall$ en $\exists$ commuteren niet.

6. Maak de multiple-choicequiz over kwantoren op `http://scherk.pbworks.com/w/page/14864234/Quiz%3A%20Logic`.

II.3 Bewijzen

Deze paragraaf is meer beschouwend van aard. We zullen eerst de vraag bespreken wat een bewijs is. Daarna zullen we vanaf een wat hoger standpunt naar bewijzen kijken en verschillende belangrijke bewijsmethoden bespreken.

Redeneerregels

We analyseren hoe een bewijs van een propositie R eruit ziet. Een (formeel of geïdealiseerd) bewijs bestaat uit een rij proposities met toelichting: je start met propositie 1, vervolgens schrijf je propositie 2 op en zo ga je verder tot je uiteindelijk bij een propositie belandt die gelijk is aan de propositie R die je wilde bewijzen. Uiteraard mag je niet zomaar willekeurige proposities opschrijven — in iedere stap moet je je aan *redeneerregels* houden. In de toelichting geef je per propositie aan welke redeneerregel je hebt toegepast om tot de propositie te komen.

Het blijkt dat een handvol redeneerregels volstaat om iedere ware uitspraak te bewijzen[4]. Deze redeneerregels passen veel wiskundigen onbewust en op intuïtie toe (ze zijn 'nogal logisch'). Je vindt de redeneerregels in Appendix VIII.1. Om een beeld te geven, zijn hier twee voorbeelden:

'$\Rightarrow$'-eliminatie Als je al proposities van de vorm P en $P \Rightarrow Q$ hebt gevonden, mag je Q als propositie toevoegen aan je bewijs. (Dit noemen logici de *modus ponendo ponens*, al zul je dit woord in wiskundeteksten niet snel tegenkomen.)

[4] Dit resultaat staat bekend als Gödels *volledigheidsstelling*, dat niet moet worden verward met de *onvolledigheidsstellingen*, waarover in een opmerking later meer.

'⇒'-introductie Je mag in je bewijs een willekeurige propositie P opnemen, hier vervolgens met de redeneerregels een resultaat Q uit afleiden, en vervolgens $P \Rightarrow Q$ aan je bewijs toevoegen. Vanaf dat moment mag je het gedeelte van je bewijs beginnend bij P en eindigend bij Q niet meer gebruiken om nieuwe resultaten af te leiden. (Vergelijk dit met een subroutine in programmeren.)

Verder mag je op een willekeurig moment in je bewijs een *axioma* of een al eerder bewezen stelling opnemen.

II.3.1 Opmerking. Formalisme. De redeneerregels zijn zo precies, dat het mogelijk is om computers bewijzen te laten controleren. De software die dit doet, noem je een *proof checker*. Voorwaarde is wel dat een bewijs in de symboolnotatie is opgeschreven en dat de bewijzen in voldoend kleine stapjes uiteen zijn gerafeld. Dat blijkt zelfs voor eenvoudige resultaten een hels karwij, hoewel moderne proof checkers al een groot deel van het werk uit handen kunnen nemen. De droom van veel wiskundigen is dat proof checkers straks het werk van de *peer reviewer* van tijdschriften kunnen overnemen daar waar het gaat om bepalen van de correctheid van een publicatie.

Computers controleren enkel de regels, maar begrijpen natuurlijk niet wat de proposities die ze voorgelegd krijgen betekenen. De proposities worden behandeld als rijtjes symbolen en wiskunde wordt een 'spel met symbolen'. Dit leidt tot het vakgebied van de bewijstheorie, waarin je de structuur van stellingen en bewijzen bestudeert. De bewijstheorie is ontwikkeld door de wiskundige Hilbert, die er meteen een heel ambitieus programma aan koppelde: hij wilde voor de wiskunde axioma's en redeneerregels formuleren waarvan je kunt *bewijzen* dat het mogelijk is om iedere propositie te bewijzen of weerleggen, terwijl je tegelijkertijd kunt *bewijzen* dat zich geen paradoxen kunnen voordoen (zoals die van Russell, zie Voorbeeld I.0.1). Hoewel het veel sterke deelresultaten heeft opgeleverd, liet Gödel in de loop van de vorig eeuw met zijn beroemde *onvolledigheidsstellingen* zien dat Hilberts programma onhaalbaar was. Desalniettemin zijn door de formalisatie van de wiskunde de fundamenten voor de huidige wiskunde gelegd en mede daarom is Hilberts werk zeer nuttig geweest.

II.3.2 Opmerking. De praktijk. We hebben een geïdealiseerde beschrijving van een wiskundig bewijs gegeven. In de praktijk wordt niet enkel met de abstracte symboolnotatie gewerkt en maken wiskundige grotere denkstappen dan enkel de elementaire redeneerregels. Ook komt het vaak voor dat bepaalde bewijzen "aan de lezer worden overgelaten" of als "evident" of "triviaal" worden afgedaan. Een bewijs dat in alle formalistische details is opgeschreven, kan voor mensen onleesbaar lang of saai zijn. Maar bovenden leidt te veel detaillering af van belangrijke functies die een bewijs heeft naast verificatie: een 'mooi' bewijs geeft bijvoorbeeld ook een intuïtief inzicht in de reden dat een stelling waar is[5]. Voorts blijkt dat een formeel bewijs op papier slecht beschrijft hoe wiskundigen denken, informeel communiceren en tot nieuwe resultaten komen[6].

Bewijsmethodes

We zullen nu een aantal strategieën benoemen die je kunt gebruiken om proposities te bewijzen. Deze noemen we ook wel *bewijsmethodes*. We beginnen met twee strategieën om stellingen van de vorm $P \Rightarrow Q$ te bewijzen.

Direct bewijs

Begin je bewijs met de aanname dat P waar is. Leid hier vervolgens uit af dat Q waar is. Op grond hiervan mag je concluderen dat de propositie $P \Rightarrow Q$ waar is. We herkennen hier de toepassing van een van de redeneerregels die hierboven als

[5] Deze functies van bewijzen zijn voor de schoolwiskunde bijvoorbeeld uitgewerkt door De Villiers (2006): Rol en functie van het bewijs in de dynamische meetkunde, *Euclides 81*(4), blz. 184–188.

[6] Zie bijvoorbeeld de beschouwing van Thurston (1994): On Proof and Progress in Mathematics, *Bulletin of the American Mathematical Society 30*(2), blz 161–177. Thurston is winnaar van een Fields medal, de nobelprijs van de wiskunde. Het artikel is beschikbaar op internet onder arXiv:math/9404236

voorbeeld is gegeven. Je kunt het ook aan de hand van de waarheidstabel van de implicatie (links in Figuur 2.4) legitimeren. Immers, als *niet* geldt dat P waar is, dan is de implicaties $P \Rightarrow Q$ waar ongeacht de waarheid van Q. We hoeven dus alleen maar de gevallen te onderzoeken waarin P waar is en in ons bewijs laten we zien dat dan Q ook altijd waar is.

Contrapositie

Begin je bewijs met de aanname dat Q *niet* waar is. Leid hier vervolgens uit af dat P ook niet waar is. Op grond hiervan mag je concluderen dat de propositie $P \Rightarrow Q$ waar is. Immers, als *wél* geldt dat Q waar is, dan is de implicaties $P \Rightarrow Q$ waar ongeacht de waarheid van P. Zie wederom de waarheidstabel van de implicatie. We hoeven dus alleen maar de gevallen te onderzoeken waarin Q onwaar is en in ons bewijs laten we zien dat dan P ook altijd onwaar is.

II.3.3 Voorbeeld. We bewijzen voor $a, b \in \mathbb{Z}$:

$$\text{Als } a^2 + b^2 \text{ een viervoud is, dan is } ab \text{ even.}$$

Volgens de contrapositiemethode volstaat het te bewijzen:

$$\text{Als } ab \text{ oneven is, dan is } a^2 + b^2 \text{ geen viervoud.}$$

Stel dus dat ab oneven is. Dan zijn a en b beide oneven en dus zijn er $r, s \in \mathbb{Z}$ zodat $a = 2r + 1$ en $b = 2s + 1$. Hieruit volgt:

$$a^2 + b^2 = (2r+1)^2 + (2s+1)^2 = 4(r^2 + r + s^2 + s) + 2$$

en dus is $a^2 + b^2$ een viervoud-plus-twee en dus geen viervoud. ∎

Tegenspraak

In een bewijs met contrapositie moet je aantonen dat een propositie P niet waar is, of, equivalent, dat $\neg P$ wél waar is. Een strategie om dit te doen is het *bewijs met tegenspraak*. Dit heet ook wel *bewijs uit het ongerijmde* of *reductio ad absurdum*. Je hebt hier in Voorbeeld I.2.7 al mee te maken gehad.

Om te bewijzen dat $\neg P$ geldt, start je het bewijs met de aanname dat P waar is en leid je hieruit een tegenspraak (onwaarheid) af. Daaruit mag je concluderen dat P niet waar is. Immers, je bewijst eigenlijk dat $P \Rightarrow Q$ waar is voor een zekere propositie Q die onwaar is. Uit de waarheidstabel voor implicatie volgt dan dat P ook niet waar is.

II.3.4 Voorbeeld. Irrationaliteit van $\sqrt{2}$. Een klassiek bewijs uit het ongerijmde is dat van de volgende propositie:

$$\textit{Er bestaat geen } x \in \mathbb{Q} \textit{ met } x^2 = 2.$$

Stel er is wél een $x \in \mathbb{Q}$ waarvoor dit geldt. We schrijven nu x als een gereduceerde breuk: $x = a/b$ met $a, b \in \mathbb{Z}$, $b \neq 0$, waarbij a en b geen gemeenschappelijke factoren hebben groter dan 1. Uit $x^2 = (a/b)^2 = 2$ volgt

$$a^2 = 2b^2.$$

Dus is a^2 even, hetgeen impliceert dat a zelf ook even is. Dus is er een $c \in \mathbb{Z}$ met $a = 2c$, hetgeen leidt tot

$$2c^2 = b^2$$

en dus is b ook even. Maar dat betekent dat a en b de gemeenschappelijke factor 2 hebben; tegenspraak. ∎

Gevalsonderscheiding

Om met gevalsonderscheiding een propositie P te bewijzen, toon je eerst aan dat $Q_1 \vee Q_2 \vee \cdots \vee Q_n$ geldt voor bepaalde proposities Q_i $(1 \leqslant i \leqslant n)$. Vervolgens toon je voor iedere i aan $Q_i \Rightarrow P$. Het volgende voorbeeld illustreert deze methode. Gevalsonderscheidingen worden door wiskundigen vaak als weinig elegant beschouwd.

II.3.5 Voorbeeld. Bekijk de vergelijking:

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1 \qquad \text{met } 0 < a \leqslant b \leqslant c \text{ en } a, b, c \in \mathbb{N}.$$

Oplossingen (a, b, c) van deze vergelijking zijn $(2,3,6)$, $(2,4,4)$ en $(3,3,3)$. We willen bewijzen dat dit de enige oplossingen zijn. Daarvoor onderscheiden we verschillende gevallen.

- $a = 1$. In dat geval moet gelden $\frac{1}{b} + \frac{1}{c} = 0$ en dat kan niet.
- $a = 2$. In dat geval moet gelden $\frac{1}{b} + \frac{1}{c} = \frac{1}{2}$. We onderscheiden een paar deelgevallen:
  - $b = 2$. In dat geval moet gelden $\frac{1}{c} = 0$ en dat kan niet.
  - $b = 3$ of $b = 4$. Dit geeft twee van de drie oplossingen die hierboven zijn genoemd.
  - $b \geqslant 5$. Omdat $c \geqslant b$ volgt $\frac{1}{b} + \frac{1}{c} \leqslant \frac{2}{5} < \frac{1}{2}$ en zijn er dus geen oplossingen.
- $a = 3$. In dat geval moet gelden $\frac{1}{b} + \frac{1}{c} = \frac{2}{3}$. We onderscheiden weer deelgevallen:
  - $b = 3$. Dit geeft de derde oplossing die hierboven al is genoemd.
  - $b \geqslant 4$. Omdat $c \geqslant b$ volgt $\frac{1}{b} + \frac{1}{c} \leqslant \frac{1}{2} < \frac{2}{3}$ en zijn er dus geen oplossingen.

∎

Equivalentie

Het bewijzen van de equivalentie $P \Leftrightarrow Q$ heeft heel vaak de structuur van twee afzonderlijke bewijzen: je bewijst eerst $P \Rightarrow Q$ en daarna $Q \Rightarrow P$.

Bewijs universaliteit

Er is ook een aantal bewijsmethodes voor stellingen waar kwantoren in voorkomen. We richten ons eerst op de universele kwantor. Als je een uitspraak van de vorm $\forall_{x \in U} P(x)$ wil bewijzen, kun je twee strategieën volgen:

1. Je begint je bewijs met "Neem een willekeurig element $x \in U$." en je probeert vervolgens om $P(x)$ aan te tonen.
2. Je neemt aan dat er een element $x \in U$ bestaat waarvoor $P(x)$ *niet* geldt en leidt hieruit een tegenspraak af.

II.3.6 Voorbeeld. Als illustratie van de eerste bewijsmethode, bewijzen we dat de som van twee even getallen even is:

$$\forall_{a,b \in E}(a + b \in E),$$

waarbij we de verzameling even getallen E gebruiken. Per definitie geldt

$$x \in E \Leftrightarrow \exists_{r \in \mathbb{Z}} x = 2r.$$

Laat $a, b \in E$. Per definitie zijn er dan elementen $r, s \in \mathbb{Z}$ zodat $a = 2r$ en $b = 2s$. Voor de som geldt dan $a + b = 2r + 2s = 2(r + s)$. Nemen we dus $t = r + s$, dan geldt dat $t \in \mathbb{Z}$ en $a + b = 2t$; per definitie geldt daarom $a + b \in E$. ∎

Bewijs existentie

Evenzo geldt voor de existentiële kwantor dat als je een uitspraak van de vorm $\exists_{x \in U} P(x)$ wil bewijzen, je twee dingen kunt doen:

1. Je beschrijft een element $x \in U$ aan waarvoor $P(x)$ geldt.

2. Je neemt aan dat voor alle $x \in U$ geldt dat $P(x)$ onwaar is en leidt vervolgens een tegenspraak af.

Deze laatste strategie leidt tot een zogenaamd *non-constructief bewijs*: je toont aan dat er een object bestaat dat een bepaalde eigenschap heeft, zonder dat je weet welk object dat is. Dat gebeurt bijvoorbeeld bij de tussenwaardestelling uit Voorbeeld II.2.2 hierboven: je weet dat een functie een nulpunt heeft, zonder te weten wat dit nulpunt is.

II.3.7 Voorbeeld. Een non-constructief bewijs. Als illustratie van de laatste bewijsmethode, geven we het klassieke bewijs dat er positieve irrationale getallen $a, b \in \mathbb{R}^+ \setminus \mathbb{Q}$ bestaan, zodat a^b rationaal is (dus $a^b \in \mathbb{Q}$).

Stel dat voor alle $a, b \in \mathbb{R}^+ \setminus \mathbb{Q}$ geldt dat $a^b \notin \mathbb{Q}$. Omdat $\sqrt{2} \notin \mathbb{Q}$ (zie Voorbeeld II.3.4), volgt uit onze aanname dat

$$\sqrt{2}^{\sqrt{2}} \in \mathbb{R}^+ \setminus \mathbb{Q}.$$

Noemen we dit getal a en nemen we $b = \sqrt{2}$, dan geldt dus

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

en dit is rationaal, in tegenspraak met onze aanname. Hiermee is de stelling bewezen.

Merk op dat dit een non-constructief bewijs is, omdat we nog steeds niet weten welk van de twee voorbeelden

$$a = b = \sqrt{2} \qquad \text{of} \qquad a = \sqrt{2}^{\sqrt{2}},\ b = \sqrt{2}$$

voldoet aan de gevraagde eigenschap. ∎

Opgaven

1. De redeneerregels en het axiomasysteem van de wiskunde is vrij complex. In deze opgave bekijken we een eenvoudiger systeem[7].

- We gebruiken enkel de symbolen M, I en U.
- Er is slechts één axioma: MI
- Er zijn de volgende redeneerregels, waarbij x en y staan voor willekeurige (eindige) reeksen symbolen:
  1. uit xI mag je xIU afleiden,
  2. uit Mx mag je Mxx afleiden,
  3. uit xIIIy mag je xUy afleiden,
  4. uit xUUy mag je xy afleiden.

(a) Bewijs de volgende stelling: MIU

(b) Bewijs de volgende stelling: MIUIU

De volgende twee onderdelen zijn bewijstheoretisch van aard: bewijzen-over-stellingen.

(c) Toon aan dat in een stelling het aantal I's nooit een drievoud is.

(d) Is MU een stelling?

2. Vind een voldoende en noodzakelijk voorwaarde voor $n \in \mathbb{N}$ zodat $\sqrt{n} \in \mathbb{Q}$. Bewijs je bewering.

★ **3.**

(a) Bewijs dat ${}^2\log 3 \notin \mathbb{Q}$.

(b) Vind een voldoende en noodzakelijke voorwaarde voor $a, b \in \mathbb{N}$ met $a > 1$ en $b > 0$, zodat ${}^a\log b \notin \mathbb{Q}$.

4. Bepaal alle natuurlijke getallen n tussen 0 en 100 waarvoor $n(n-1)$ op twee nullen eindigt (in decimale notatie).

II.4 Stellingen en definities

Stellingen zijn proposities waarvan door middel van een bewijs de waarheid is vastgesteld. Ook lemma's en corollaria zijn stellingen — de enige reden dat er een ander woord wordt gebruikt, is een didactische: een lemma is een hulpstelling, een corollarium is een betrekkelijk makkelijk te bewijzen gevolg van een stelling. *Definities* daarentegen zijn afspraken die we met elkaar maken over de betekenis van nieuwe symbolen of woorden — een definitie proberen te bewijzen is onzinnig. Achter dit simpele onderscheid blijken toch wat nuances schuil te gaan. We bespreken echter eerst een paar eenvoudige voorbeelden.

II.4.1 Voorbeelden. i) $x \neq y$ betekent $\neg(x = y)$. ii) In de vlakke meetkunde wordt een *cirkel* met middelpunt P en straal r gedefinieerd als de verzamelingen punten die afstand r tot P hebben. Iedere keer dat in een tekst de term 'cirkel' voorkomt, kun je dit vervangen door "verzameling punten die ...". iii) De uitdrukking "x is even" kun je vervangen door "er bestaat een $r \in \mathbb{Z}$ zodat $x = 2r$." Op deze manier kun je de eigenschap 'even' van getallen definiëren.

II.4.2 Voorbeelden. Een rechthoek is een bijzonder voorbeeld van een parallellogram. Dat komt omdat een definitie van parallellogram bijvoorbeeld is: "een vierhoek waarvan overstaande zijden evenwijdig zijn;" en een rechthoek voldoet aan deze eigenschap. Dat een rechthoek een parallellogram is, is echter een gevolg van een *keuze* die mensen hebben gemaakt in de definitie. Het zou ook te verdedigen zijn om aan de definitie van een parallellogram toe te voegen "... en waarvan de hoeken niet recht zijn" — om historische redenen heeft men hier niet voor gekozen.

Het onderscheid tussen definitie en stelling wordt minder helder als een symbool wordt geïntroduceerd voor een object waarvan het bestaan eerst moet zijn bewezen. In dat geval lijkt een definitie niet meer een simpele afkorting. Er zijn verschillende manieren om hier mee om te gaan, maar die vallen buiten het bestek van deze tekst. We volstaan hier met enkele voorbeelden.

II.4.3 Voorbeelden. i) Een stelling in de analyse zegt dat er een uniek getal $e \in \mathbb{R}$ bestaat zodat de functie $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto e^x$ gelijk is aan zijn afgeleidefunctie f'. Dit is per definitie het getal van Euler. ii) Een precieze definitie van de *oppervlakte* van vlakke figuren is best ingewikkeld. Als we het hebben over 'de oppervlakte van een figuur' dan gaan daar een hoop stellingen achter schuil over bestaan van bepaalde limieten. iii) $\sqrt{2}$ is het positieve reële getal x waarvoor geldt $x^2 = 2$. Deze definitie is zinvol omdat je kunt bewijzen dat zo'n getal x bestaat en dat deze bovendien uniek is.

Equivalente definities

De volgende figuur komt soms ook voor in wiskundeteksten:

[7] Bron: Hofstadter (1979), *Gödel, Escher, Bach: an Eternal Golden Braid*.

Een ... is een ... dat voldoet aan een van de volgende equivalente eigenschappen ....

Ook hier komen definitie en stelling samen, want je moet immers bewijzen dat de eigenschappen inderdaad equivalent zijn. Je zou dit kunnen oplossen door één van de eigenschappen in de definitie te gebruiken en vervolgens de andere eigenschappen in een stelling op te nemen, maar hier wordt niet altijd voor gekozen.

II.4.4 Voorbeeld. In de schoolwiskunde kom je equivalente definities tegen bij vlakke figuren. Nemen we als voorbeeld de ruit, dan is één definiërende eigenschap dat het een parallellogram is waarvan de zijden even lang zijn. Een andere definiërende eigenschap is dat het een parallellogram is waarvan de diagonalen elkaar loodrecht snijden. Eén van de einddoelen bij vwo Wiskunde D is dat leerlingen deze equivalentie kunnen bewijzen. ∎

II.4.5 Opmerking. Definities komen niet uit de lucht vallen. Belangrijk is dat een definitie *bruikbaar* is. Zo is er bijvoorbeeld voor gekozen om 1 per definitie geen priemgetal te laten zijn. Dat zou de notie van priemgetal namelijk minder bruikbaar maken: unieke priemfactorisatie gaat bijvoorbeeld niet meer op als je willekeurig vaak factoren 1 kunt toevoegen. Een ander voorbeeld is de definitie van a^x ($a > 0$) voor niet-gehele machten x. Die is zo gekozen dat de rekenregels die gelden voor $x \in \mathbb{N}$ uitbreiden naar $x \in \mathbb{R}$; zie Opgave II.4.4. Het lukt niet om op consistente manier aan 0^0 betekenis te geven; het zal in deze tekst handig blijken om $0^0 = 1$ af te spreken, maar hier is onder wiskundigen geen consensus over en veel wiskundigen stellen dat 0^0 ongedefinieerd is.

Opgaven

✍ **1.** In de schoolwiskunde wordt de vergelijking

$$(\text{omtrek}) = \pi \times (\text{diameter})$$

geïntroduceerd als relatie tussen omtrek en diameter van een cirkel.

(a) Is hier sprake van een stelling of een definitie? Waarom?

(b) Dezelfde vraag, maar nu voor de formule $(\text{oppervlakte}) = \pi r^2$.

2. (Dit is een discussievraag voor in een groep.)

(a) Wat is een acceptabele definitie van een *vierhoek*? Houd in je definitie rekening met de vraag of je ook niet-convexe figuren wil toelaten, of figuren waarvan twee zijden elkaar snijden.

(b) Wat is een acceptabele definitie van een hoek? Wat betekent het vervolgens als je zegt dat twee hoeken gelijk zijn? En is volgens jouw definitie een gestrekte hoek (180°) ook een hoek?

3. Formuleer steeds minstens drie equivalente definities van de volgende vierhoeken en bewijs dat de definities equivalent zijn. Je kunt in deze opgave gebruik maken van de gebruikelijke begrippen uit de euclidische meetkunde (zoals 'vierhoek', 'diagonaal-van-een-vierhoek' of 'evenwijdig').

(a) Vierkant

(b) Parallellogram

(c) Vlieger

✯ **4.** In de onderbouw wordt eerst de uitdrukking a^b geïntroduceerd met $a > 0$ en b een positief geheel getal.

(a) Geef in dit geval de definitie. (N.B. Als je een grotere uitdaging wil, probeer dan recursie te gebruiken zoals beschreven in Paragraaf IV.3.)

Op grond van deze definitie kun je een aantal rekenregels bewijzen:

> *Voor alle $a > 0$ en voor alle b en c positief geheel geldt $a^b \cdot a^c = a^{b+c}$ en $(a^b)^c = a^{bc}$ en $a^1 = a$.*

(b) Bewijs deze stelling. Gebruik daarbij de definitie uit het vorige onderdeel.

Vervolgens wordt betekenis gegeven aan a^0 en aan a^b in het geval b negatief, maar nog steeds geheel is: $a^0 = 1$ en als $a^b = \frac{1}{a^{-b}}$. Dit is een definitie, maar wel een logische keuze voor een definitie; de rekenregels uit voorgaande stellingen worden nu immers 'opgerekt' naar niet-positieve, gehele exponenten.

(c) Leg uit wat hiermee wordt bedoeld.

(d) Geef een acceptabele definitie van a^b met $a > 0$ en $b \in \mathbb{Q}$. Leg uit waarom dit een acceptabele definitie is.

(e) Hoe zit het met $b \in \mathbb{R}$ (en nog steeds $a > 0$)?

(f) Analyseer wat er aan de hand is als $a \leqslant 0$.

II.5 Enkele historische opmerkingen

Het waren de Grieken die de strenge, deductieve manier van redeneren in de wiskunde introduceerden, met als hoogtepunt de axiomatische opbouw van de meetkunde in de *Elementen* van Euclides (ca. 300 v.C.). De Grieken hadden een rijke traditie in de logica, die ze overigens net zo goed op wiskunde, op spraakkunst (retoriek) als op andere kennisdomeinen toepasten. Het hoogtepunt was de logica van de Stoïcijnse denkers: bij Philo van Megara vinden we bijvoorbeeld de eerste waarheidstabel (van de implicatie) en later gaf Chrysippus van Soli een axiomatische beschrijving van propositielogica.

De studie van redenering vond vóór de Griekse al in diverse culturen plaats. In India was dit het verst ontwikkeld. In de *Rigveda* (hindoeïstische verzen uit ca. 1500 v.C.) werd al gekeken naar de structuur van uitspraken met negaties. Al voor Euclides beschreef Pāṇini een formeel systeem, namelijk de grammatica van het Sanskriet in 3.996 regels — zijn werk is later inspiratie geweest voor de eerste programmeertalen. Ook in China was er voor de Grieken al de bloeiende Mohistische school, die een logica beschreef die dichter bij het dagelijks taalgebruik ligt dan de rigide mathematische logica.

Al deze ontwikkelingen, van Stoa, de Indiërs of de Chinezen, heeft echter geen invloed gehad op de ontwikkeling in de Europese logica vanaf de Middeleeuwen. Slechts één logisch werk van de Grieken genoot bekendheid en de impact daarvan was bijzonder groot. Dit was het *Organon* van Aristoteles (384–322 v.C.). Aristoteles' logica was verre van volmaakt, maar zijn invloed was zo groot dat velen meenden dat de logica een uitontwikkelde discipline was. Hoogtepunt van het Aristotelische denken is de *scholastische* traditie, waarin Willem van Ockham in de 13de eeuw bijvoorbeeld de wetten van De Morgan beschreef, die later in de 19de eeuw zouden worden herontdekt. Met de wetenschappelijk revolutie kwam er aan de hegemonie van Aristoteles een einde. Zo introduceerde Bacon begin 17de eeuw in zijn *novum organum* de voor empirische wetenschappen zo belangrijke inductieve methode als alternatieve manier van kennisgaring. Belangrijke drijfveer voor de wetenschappelijke traditie was het beschikbaar komen van veel meer Griekse kennis, behouden en soms aanzienlijk verrijkt door Arabische geleerden zoals de voor de logica belangrijk Ibn Sina (Avicenna) en Ibn Rushd (Averroës).

Richten we ons specifiek op de mathematische logica, dan vinden we de eerste significante ontwikkeling bij Leibniz (1646–1716). Leibniz was een vermaard Duits filosoof en met Newton grondlegger van de analyse (onze notaties voor differentiëren en integreren zijn bijvoorbeeld van hem afkomstig). Zijn droom was de ontwikkeling van een *characteristica universalis*: een universele symbooltaal om redeneringen in uit te drukken. Leibniz ontwikkelde een symbolische logica, maar hield dit geheim en omdat Leibniz' tekst pas in 1903 gepubliceerd werd, kon het in de negentiende eeuw onafhankelijk worden ontwikkeld door George Boole (Engeland, 1979–1984).

De grootste doorbraak, de ontwikkeling van de predikatenlogica en de uitvinding van de kwantoren, werd gedaan door de Duitser Gottlob Frege (1848–1925) in zijn *Begriffschrift*. De predikatenlogica bleek zo'n krachtige taal, dat er met Frege een filosofische stroming ontstond die het *logicisme* wordt genoemd. De logicisten stellen dat alle wiskundige uitspraken zijn te reduceren tot zuiver logische uitspraken over eigenschappen van willekeurige objecten, zonder dat er daarbij axioma's moeten worden aangenomen. Het logicisme bereikte het hoogtepunt met de publicatie van de *Principia mathematica*, waar Bertrand Russell (1872–1970) een belangrijk aandeel in had. Dit omvangrijke werk heeft grote invloed gehad in de ontwikkeling van de twintigste eeuwse mathematische logica, maar ook daarbuiten genoot het een soort cultstatus — onder meer vanwege een citaat op bladzijde 379 (!) van dit werk dat aankondigde dat uit een daar geformuleerde stelling later zou volgen dat $1+1=2$. Het logicisme als fundament van de wiskunde zou uiteindelijk geen voet aan de grond krijgen, omdat het niet goed lukte reële getallen te introduceren zonder axioma's aan te nemen.

Een stroming die naast het logicisme opkwam, was het formalisme van de Duitser David Hilbert (1862–1943). Het formalisme, dat wiskunde beschouwt als betekenisloze manipulatie van symbolen, is in de eerdere paragrafen al aan bod gekomen. Het formalisme is nog steeds zeer invloedrijk, omdat het een objectieve meetlat lijkt te bieden voor de correctheid van wiskundige uitspraken. In deze traditie kunnen de belangrijke resultaten van Gödel en Cohen worden geplaatst, die al eerder in deze tekst aan de orde zijn gekomen.

De mathematische logica is nog steeds een actief onderzoeksgebied op het raakvlak van wiskunde en filosofie. In Nederland is er met name in Nijmegen een actieve onderzoeksgroep, waar men zich onder meer richt op het controleren van bewijzen met computers en zelfs zogenaamde *proof assistants*: computers die ondersteuning bieden bij het vinden van bewijzen. De Eindhovense hoogleraar De Bruijn was in Nederland de eerste die zich met *proof checkers* bezig hield in zijn project Automath.

In deze historische opmerkingen kan de originele en geheel eigen insteek van de Nederlandse wiskunde Brouwer (1881–1966) niet ongenoemd blijven. Brouwer stelde in zijn *intuïtionisme* grenzen aan de kracht van de logica. Hij vond het bijvoorbeeld vreemd dat we 'door de logica' niet-constructieve bewijzen konden leveren. Daarom verwierp hij de *wet van de uitgesloten derde*, oftewel de aanname dat een wiskundige uitspraak waar of niet waar is. Dit leidt tot een geheel eigen soort wiskunde.

In de schoolwiskunde zijn al deze ontwikkelingen niet direct zichtbaar, maar de nadruk op structuur en verzamelingenleer die hand in hand ging met stromingen als formalisme en logicisme is wel zichtbaar geworden — zie het vorige hoofdstuk. Toch is logisch leren redeneren vaak wel een belangrijke doelstelling van het wiskundeonderwijs. Typerend is de plek van de euclidische meetkunde in het voortgezet onderwijs. Hoewel dit onderwerp op universiteiten bijna nooit in het curriculum is opgenomen en het in geen enkele niet-wiskundige vervolgopleiding terugkomt, is het de laatste twee eeuwen vaker wel dan niet op school gedoceerd. Het idee is dat de euclidische meetkunde het prototype is van een axiomatisch systeem, zonder de cognitieve ruis van lastige algebraïsche expressies en ingewik-

kelde kwesties rondom de opbouw van getalsystemen. Het leren van euclidische meetkunde zou ‘de geest scherpen’ (terwijl algebra geleerd wordt ‘voor vlijt’). Over de waarheid hiervan zul je zelf een oordeel moeten vormen. . . .

In de 21ste eeuw lijkt logica een wat prominentere plaats in het schoolcurriculum te hebben. Bij het schoolvak informatica speelt het een rol, het heeft een tijd in het natuurkundeprogramma gezeten bij meet-, stuur- en regelsystemen en in Wiskunde D kan het als keuzeonderwerp worden gedaan. In Wiskunde C is logisch redeneren vanaf 2015 een verplicht onderdeel uit het examenprogramma. Wiskunde C bereidt voor op vervolgstudies als taalwetenschappen en rechten en het idee is dat logica in dit soort disciplines heel relevant is.

III GEREEDSCHAPPEN

We zullen in dit hoofdstuk, als aanvulling op hoofdstuk I, nog twee soorten wiskundige structuren op verzamelingen behandelen:

- *Operaties.* Het gaat hier om samenstellen van elementen. Denk hierbij aan optellen of vermenigvuldigen.
- *Relaties.* Het gaat hier om vergelijken van elementen. Denk aan 'is kleiner dan' of 'is gelijk aan'.

We zullen operaties en relaties in verzamelingentaal formuleren. Dat maakt dit hoofdstuk vrij abstract. De abstractie betaalt zich in de volgende hoofdstukken uit. We zullen in de loop van deze tekst namelijk verschillende getalssystemen (zoals $\mathbb{Z}$ en $\mathbb{R}$) introduceren en daarna ook vectorruimten. Omdat we operaties en relaties dan al in abstracte termen hebben beschreven, hoeven we niet steeds opnieuw operaties als optelling en hun eigenschappen te introduceren als iets nieuws. We richten ons in dit hoofdstuk dus op de *structuur* en niet op de concrete inhoud. Dit noemen we *abstraheren* en hierin schuilt de kracht van de wiskunde!

Hoewel abstract, zul je merken dat je in concrete gevallen al heel vertrouwd bent met de theorie in dit hoofdstuk. Als je een passage lastig vindt, kun je een concreet getallenvoorbeeld in gedachte nemen en aan de hand hiervan de notatie doorgronden. Die vertrouwdheid is er mogelijk niet meer bij het laatste gedeelte van dit hoofdstuk over restklassen en quotiëntverzamelingen. Dit is heel belangrijk gereedschap in veel gebieden van de wiskunde en stelt ons bijvoorbeeld in staat om nieuwe getalssystemen te definiëren op grond van bestaande.

III.0.1 Voorbeeld. Rond de jaren '70 leefde het idee dat je de wiskunde reeds op school vanaf het fundament van verzamelingen en natuurlijke getallen moet opbouwen. Eigenschappen van operaties en relaties waren daarbij belangrijk. In schoolboeken werd hier al in de eerste klas uitgebreid bij stilgestaan (Figuur 3.1).
—■

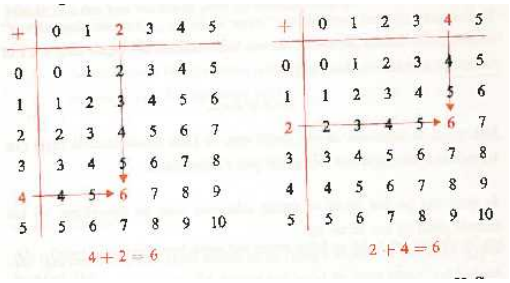
III.1 Operaties

Operatie

III.1.1 Definitie. Zij V een verzameling. Een *(binaire) operatie* op een verzameling V is een functie

$$\bigcirc\colon \quad V \times V \to V.$$

Voor $a, b \in V$ noteren we het beeld van (a, b) met $a \bigcirc b$.



Figuur 3.1 – Een illustratie van de commutatieve eigenschap van optelling uit het de editie van 1968 van *Moderne wiskunde* voor klas 1.

III.1.2 Voorbeelden. Optellen van gehele getallen is een operatie

$$+: \quad \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$

De notatie $a+b$ voor het beeld van $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ is natuurlijk overbekend. Ook aftrekken en vermenigvuldigen van gehele getallen is een operatie.

Voorbeelden van operaties kom je niet alleen tegen bij de bekende getalsverzamelingen. Bij lineaire algebra wordt bijvoorbeeld de *vectoroptelling* als operatie geïntroduceerd. De operatie wordt met hetzelfde symbool, namelijk '+', aangegeven. Ook op verzamelingen van matrices zijn er bekende operaties: in de verzameling M_n van n bij n-matrices, bijvoorbeeld, is er optellen, aftrekken en vermenigvuldiging. In Paragraaf I.5 ben je de verzameling $\mathrm{Sym}(A)$ van permutaties op een verzameling A tegengekomen; samenstellen van permutaties is een operatie op $\mathrm{Sym}(A)$.

III.1.3 Opmerking. Delen, zelfs in $\mathbb{R}$, is geen operatie omdat je niet door nul mag delen. Delen is een zogenaamde *partiële operatie*: een functie $\bigcirc$ van een deelverzameling $W \subset V \times V$ naar V. In het geval van delen in $\mathbb{R}$ is het domein dan $W = \mathbb{R} \times (\mathbb{R} \setminus \{0\})$.

In het geval van een operatie op een verzameling V, zeggen we soms dat V *gesloten is* onder die operatie. In het licht van bovenstaande definitie is dat raar taalgebruik, tenzij de operatie al in een grotere verzameling is gedefinieerd en we deze willen beperken tot een deelverzameling; bijvoorbeeld: de verzameling even getallen is gesloten onder de optelling $+: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ (en overigens ook onder de vermenigvuldiging).

Associatief en commutatief

De rekenoperaties op getalverzamelingen voldoen aan heel veel eigenschappen, die we in de schoolcontext vaak rekenregels noemen. Enkele van deze zijn 'elementair' in de zin dat ze in vrij korte formules te vangen zijn en dat ingewikkeldere rekenregels uit ze zijn af te leiden. We zullen er in deze paragraaf een aantal benoemen. We beginnen met de volgende twee regels:

III.1.4 Definitie. Zij $\bigcirc$ een operatie op een verzameling V.

- De operatie $\bigcirc$ is *associatief* als voor alle $a,b,c \in V$ geldt

$$a \bigcirc (b \bigcirc c) = (a \bigcirc b) \bigcirc c.$$

- De operatie $\bigcirc$ is *commutatief* als voor alle $a,b \in V$ geldt

$$a \bigcirc b = b \bigcirc c.$$

III.1.5 Voorbeelden. Uiteraard voldoen de operatie optellen en vermenigvuldigen op een getalverzameling zoals $\mathbb{Z}$, of $\mathbb{R}$ aan deze twee eigenschappen. Aftrekken als operatie op bijvoorbeeld $\mathbb{Z}$ is niet associatief en ook niet commutatief. Dat geldt ook voor delen als operatie op $\mathbb{R} \setminus \{0\}$. Zie Opgave III.1.2.

Een klassiek voorbeeld van een niet-commutatieve operatie die wel associatief is, is matrixvermenigvuldiging. Voor twee vierkante matrices A en B geldt niet noodzakelijk $A \cdot B = B \cdot A$. Een ander voorbeeld van een operatie die niet commutatief is, is samenstellen van permutaties in $\mathrm{Sym}(A)$ voor een verzameling A met meer dan twee elementen (Opgave III.1.5).

De associatieve eigenschap maakt dat we geen afspraken hoeven te maken over het herhaald toepassen van een operatie. Zo kun je $1+2+3$ op twee manieren interpreteren en associativiteit zegt dat beide manieren hetzelfde resultaat geven: $(1+2)+3 = 3+3 = 6$, respectievelijk $1+(2+3) = 1+5 = 6$.

III.1.6 Opmerking. Aftrekken is niet associatief. Een uitdrukking zoals $3-2-1$ is dan ook niet betekenisvol, tenzij je met elkaar afspreekt dat je dit bijvoorbeeld van links naar rechts interpreteert. Hetzelfde geldt voor delen (als operatie in bijvoorbeeld $\mathbb{R} \setminus \{0\}$): in het algemeen is $a/(b/c)$ niet gelijk aan $(a/b)/c$. Soms leidt dat tot problemen, met name in handgeschreven teksten of bij het werken met de rekenmachine — want wat betekent

$$\frac{\frac{6}{3}}{2} \qquad ???$$

Bij machtverheffen is er een soortgelijk probleem: a^{a^a} is betekenisloos. Zie verder Opgave III.1.2. Je zult in al deze gevallen dus haakjes moeten gebruiken, of met verschillende lettergroottes je bedoeling duidelijk moeten maken.

We hebben al genoemd dat de uitdrukking $a_1+a_2+a_3$ betekenisvol is omdat optellen associatief is. Via een inductief argument (dat technisch toch nog vrij ingewikkeld is), kun je hetzelfde bewijzen voor iedere *eindige* som $a_1+a_2+\cdots+a_r$. Bij 'oneindige sommen' moet je voorzichtig zijn — pieker bijvoorbeeld maar eens over

$$1+(-1)+1+(-1)+1+(-1)+\cdots.$$

Een nette behandeling van 'oneindige sommen' is via het concept van *reeksen* en voorgaand voorbeeld is dan ook geen bonafide (d.w.z. convergente) reeks.

Neutraal element

We richten ons nu op elementen die een speciale eigenschap hebben ten opzichte van een operatie.

III.1.7 Definitie. Zij $\bigcirc$ een operatie op een verzameling V. Een element $e \in V$ is een *neutraal element* voor de operatie $\bigcirc$ als voor alle $a \in V$ geldt

$$a \bigcirc e = a \qquad \text{en} \qquad e \bigcirc a = a.$$

In $\mathbb{Z}$ is 0 een neutraal element voor optelling en is 1 een neutraal element voor vermenigvuldiging. In plaats van over *een* neutraal element wordt meestal over *het* neutrale element gesproken. De onderbouwing hiervan komt uit de volgende stelling.

III.1.8 Stelling. Zij $\bigcirc$ een operatie. Als er een neutraal element is voor $\bigcirc$, dan is deze uniek.

Bewijs. Stel e en e' zijn beide neutrale elementen. Dan geldt

$$e = e \bigcirc e' = e',$$

waar in de linker gelijkheid is gebruikt dat e' een neutraal element is en in de rechter gelijkheid dat e dit is. ∎

Inverse

III.1.9 Definitie. Zij $\bigcirc$ een operatie op een verzameling V met neutraal element $e \in V$. Zij verder $a \in V$. Een *inverse* van a voor de operatie $\bigcirc$ is een element $b \in V$ waarvoor geldt

$$a \bigcirc b = e \qquad \text{en} \qquad b \bigcirc a = e.$$

III.1.10 Stelling. Stel dat $\bigcirc$ een associatieve operatie is met een neutraal element. Dan heeft ieder element hoogstens één inverse.

Bewijs. Noteer het neutrale element met e. Stel b en b' zijn beide inverses van a. Dan geldt

$$b = b \bigcirc e = b \bigcirc (a \bigcirc b') = (b \bigcirc a) \bigcirc b' = e \bigcirc b' = b'.$$

∎

III.1.11 Voorbeelden. In $\mathbb{Z}$ (of $\mathbb{R}$) heeft ieder element a een inverse voor optellen, namelijk $-a$. Er geldt immers $a + (-a) = 0$ en 0 is het neutrale element voor optellen. Er is het volgende verband met de operatie aftrekken:

$$a - b = a + (-b);$$

we zullen aftrekken zelfs op deze manier *definiëren*. Merk op dat het minteken hier twee betekenissen heeft: aan de linkerkant van de formule staat het voor een operatie en aan de rechterkant voor een functie $\mathbb{Z} \to \mathbb{Z}$ die b op zijn inverse afbeeldt. Op een rekenmachine zijn dit altijd twee verschillende knoppen, waarbij de operatie met $\boxed{-}$ en de functie soms met $\boxed{(\text{-})}$ wordt aangegeven. Voor leerlingen kan dit verwarrend zijn. De schoolboeken *Getal en ruimte* en *Moderne wiskunde* gebruiken vaak twee enigszins verschillende symbolen: de 'functie-min' is een streepje dat iets hoger en kleiner is als de 'operatie-min'.

Definiëren we de operatie aftrekken op bovenstaande manier, dan geldt inderdaad de gewenste eigenschap

$$(a - b) + b = a.$$

Om dit te bewijzen, gebruiken we de associatieve eigenschap:

$$(a - b) + b = (a + (-b)) + b = a + ((-b) + b) = a + 0 = a.$$

Voor vermenigvuldigen in $\mathbb{R}$ kunnen we een zelfde soort opmerking maken, behalve dat we 0 moeten uitsluiten. Ieder element $a \neq 0$ heeft een inverse die we met a^{-1} of met $\frac{1}{a}$ of met $1/a$ noteren. Delen kunnen we dan definiëren als

$$\frac{a}{b} = a \cdot b^{-1}.$$

Aftrekken en delen worden meestal niet in definities van algebraïsche structuren genoemd. Ze kunnen immers gedefinieerd worden aan de hand van optellen en vermenigvuldigen, maar ze hebben minder mooie eigenschappen (zoals associativiteit).

Distributieve eigenschap

We benoemen nu een eigenschap die twee operaties met elkaar in verband brengt. Waar we in het voorgaande een abstract symbool '$\bigcirc$' hebben gebruikt, kiezen we er nu voor om te werken met twee concrete symbolen.

III.1.12 Definitie. Laat $+_V$ en $\cdot_V$ twee operaties op een verzameling V zijn. De operatie $\cdot_V$ is *distributief over* $+_V$ als voor alle $a,b,c \in V$ geldt

$$a \cdot_V (b +_V c) = (a \cdot_V b) +_V (a \cdot_V c)$$

en

$$(b +_V c) \cdot_V a = (b \cdot_V a) +_V (c \cdot_V a).$$

III.1.13 Opmerking. Voor commutatieve operaties zijn de twee voorwaarden natuurlijk equivalent en volstaat het benoemen van één van de twee gelijkheden. Let ook op de haakjes aan de rechterkant van het gelijkheidsteken. Vaak wordt een *voorrangsregel* afgesproken: vermenigvuldigen gaat voor optellen. Ook wordt $\cdot$ vaak weggelaten als dat niet tot verwarring leidt. De distributieve eigenschap luidt dan

$$a(b+c) = ab + ac.$$

In Opgave V.1.2 leidt je het volgende, voor de schoolwiskunde centrale, gevolg van de distributieve eigenschap af:

$$(a+b)(c+d) = ac + ad + bc + bd.$$

Opgaven

✍ **1.** Zonder de afspraak 'vermenigvuldigen gaat voor delen,' heb je heel veel haakjes nodig.

(a) Zet alle haakjes in de formule $x^3 + 2x^2 + 3x + 4$.

(b) Zonder associativiteit van + zijn nog meer haakjes nodig; zet deze ook.

2. (a) Leg met een voorbeeld uit waarom aftrekken en delen (bijvoorbeeld in $\mathbb{R}$ resp. $\mathbb{R}\setminus\{0\}$) associatief noch commutatief zijn.

(b) Hoe zit het met machtsverheffen (in $\mathbb{N}\setminus\{0\}$)?

(c) En met logartime $\log_a b$ (in het VO genoteerd als ${}^a\log b$) als partiële operatie in $\mathbb{R}$? (We hebben associativiteit en commutativiteit niet gedefinieerd voor partiële operaties, maar onderzoek gewoon iedere variant die betekenisvol is.)

3. Een oud ezelsbruggetje luidt 'Meneer Van Dalen Wacht Op Antwoord'. De eerste letters staan voor Machtsverheffen, Vermenigvuldigen, Delen, Worteltrekken, Optellen en Aftrekken en het ezelsbruggetje geeft aan in welke volgorde je deze operaties moet uitvoeren. Sommige docenten onderwijzen deze regel nog wel. In hoeverre is dat juist? (Merk overigens op dat delen bijna altijd met een deelstreep wordt aangegeven en dat een regel in dat geval overbodig is, omdat voorrang grafisch is weergegeven. Idem voor worteltrekken—waar alles onder de staart van de wortel staat—en machtsverheffen—waar alles in de superscript staat. In leerlingwerk gaat dit weleens fout als ze het wortelteken niet doortrekken of als het onduidelijk is of iets nu wel of niet hoog genoteerd staat.)

✍ **4.** Leerlingen maken soms fouten als $(x+3)^2 = x^2 + 3^2$. Welke niet-bestaande fundamentele rekenregel gebruiken zij hier ten onrechte? Geef deze regel ook een naam.

5. In Paragraaf sect:permutatie is de notatie $\mathrm{Sym}(A)$ geïntroduceerd voor de verzameling permutaties van een verzameling A. Samenstelling is een operatie op deze verzameling.

(a) Bewijs dat deze operatie commutatief is als en slechts dan als A hoogstens twee elementen bevat.

(b) Bewijs dat er een neutraal element is voor deze operatie.

(c) Bewijs dat ieder element een inverse heeft.

6. In de eerste editie van *Moderne Wiskunde* uit 1968 wordt in het eersteklasdeel uitvoerig ingegaan op rekenregels. Ter oefening definieert het lesboek op $\mathbb{N}$ enkele fantasie-operaties. We citeren:
"$*$ betekent: verdubbel het eerste getal en tel er het tweede bij op."
"$\square$ betekent: kwadrateer het eerste getal en tel er het tweede bij op."
"$\triangle$ betekent: vermeerder het eerste getal met 10 en tel er het tweede bij op."

Er geldt bijvoorbeeld $5 * 4 = 14$ en $10\square 1 = 101$.

(a) Onderzoek of $*$, $\square$ en $\triangle$ commutatief en associatief zijn.

(b) Kun je zelf een originele operatie verzinnen die commutatief is, maar niet associatief?

(c) En andersom?

(d) En zowel commutatief als associatief?

✍ **7.** Voor de natuurlijke getallen geldt: vermenigvuldigen is herhaald optellen en machtsverheffen is herhaald vermenigvuldigen. Definieer een nieuwe operatie '$\uparrow$' als herhaald machtsverheffen:

$$a \uparrow n = a^{\left(a^{\left(a^{\cdot^{\cdot^{\cdot}}}\right)}\right)} \qquad (n \text{ keer een } a).$$

(Een formele definitie gebruikt recursie, maar dat wordt in het volgende hoofdstuk pas behandeld.)

(a) Bereken $2 \uparrow 1$, $2 \uparrow 2$, $2 \uparrow 3$ en $2 \uparrow 4$.

(b) Schat hoe groot $2 \uparrow 5$ is.

(c) Is $\uparrow$ associatief?

(d) Is $\uparrow$ commutatief?

(e) Waarom is een definitie analoog aan $\uparrow$ waarbij de haakjes andersom staan (machtsverheffen is niet associatief!) minder interessant?

Deze truc kun je nogmaals toepassen, en nogmaals.... Op deze manier beschrijf je al snel onvoorstelbaar grote getallen. Zie `http://nl.wikipedia.org/wiki/Knuths_pijlomhoognotatie` (waar $\uparrow$ genoteerd wordt als $\uparrow\uparrow$). Zie ook een artikel van Dick Klingens in het tijdschrift voor wiskundeleraren *Euclides* (special over getallen, 2012).

✍ **8.** Deze opgave gaat over de vraag in hoeverre het mogelijk is oneindig als een getal te beschouwen. We bekijken twee kandidaten: (i) de verzameling $\mathbb{Z}_\infty = \mathbb{Z} \cup \{\infty\}$ en (ii) de verzameling $\mathbb{Z}_{\pm\infty} = \mathbb{Z}_\infty \cup \{\infty'\}$, waarbij ∞ en ∞' twee verschillende (willekeurig gekozen) elementen zijn die beide niet in $\mathbb{Z}$ voorkomen. We willen optellen en vermenigvuldigen op $\mathbb{Z}$ uitbreiden naar operaties op $\mathbb{Z}_\infty$ of $\mathbb{Z}_{\pm\infty}$, waarbij we de rekenregels als associativiteit en distributiviteit of het bestaan van een inverse voor optelling het liefst willen behouden. Onderzoek in hoeverre dat mogelijk is.

III.2 Relaties

Een relatie is een uitspraak (een propositie) over twee elementen die waar of onwaar is. Bekende voorbeelden van relaties zijn $=$, $\neq$, $\leqslant$ en $>$. Een precieze definitie gebruikt de taal van verzamelingen.

Relatie

III.2.1 Definitie. Zij V een verzameling. Een *(binaire) relatie* op V is een deelverzameling $R \subset V \times V$. Voor $a, b \in V$ noteren we $a\ R\ b$ voor $(a,b) \in V$. Meestal gebruiken we in plaats van een letter (zoals R) een symbool (zoals $<$ of $\sim$). De notatie $a \not R\ b$ staat voor $(a,b) \notin V$.

We bekijken in deze paragraaf twee soorten relaties: eerst lineaire ordening en daarna equivalentierelaties. Voor de leesbaarheid gebruiken we in de definitie van lineaire ordening het bekende symbool $\leqslant$, maar bedenk dat dit een algemene, abstracte definitie is die los staat van de interpretatie van $\leqslant$ als 'kleiner dan of gelijk aan'.

Lineaire ordening

III.2.2 Definitie. Een relatie $\leqslant$ op een verzameling V is een *lineaire ordening* (ook wel *totale ordening* genoemd) als voor alle $a, b, c \in V$ geldt:

- $(a \leqslant b \wedge b \leqslant a) \Rightarrow a = b$,
- $a \leqslant b \vee b \leqslant a$,
- $(a \leqslant b \wedge b \leqslant c) \Rightarrow a \leqslant c$.

Het intuïtieve model dat hierbij hoort, is dat van de *getallenlijn*.

Equivalentierelatie

III.2.3 Definitie. Een *equivalentierelatie* is een relatie $\sim$ op een verzameling V die aan de volgende drie voorwaarden voldoet:

- *Reflexiviteit.* $\forall_{a \in V}\ a \sim a$,
- *Symmetrie.* $\forall_{a,b \in V}\ a \sim b \implies b \sim a$,
- *Transitiviteit* $\forall_{a,b,c \in V}\ (a \sim b \wedge b \sim c) \implies a \sim c$.

Equivalentieklasse

Zij $\sim$ een equivalentierelatie op een verzameling V en laat $a \in V$. De *equivalentieklasse* van a onder $\sim$ is de verzameling van alle elementen van V die equivalent zijn met a. Notatie:

$$[a]_\sim = \{b \in V \mid b \sim a\}.$$

Kan er geen verwarring zijn, dan wordt vaak $[a]$ gebruikt in plaats van $[a]_\sim$. Een element $b \in [a]$ (bijvoorbeeld a zelf) noemen we een *representant* van $[a]$. De *quotiëntverzameling* van $\sim$ is de verzameling equivalentieklassen:

$$V/\sim = \big\{[a] \,\big|\, a \in V\big\}.$$

III.2.4 Voorbeelden. i) Voor iedere verzameling V definieert $=$ een equivalentierelatie. Voor deze equivalentierelatie zijn de equivalentieklassen en de quotiëntverzameling niet zo interessant. Omdat er voor $a \in V$ maar één element is equivalent met a (namelijk a zelf), geldt $[a] = \{a\}$ en $R/= = \{\{a\} \mid a \in V\}$.

ii) Daarentegen zijn $\neq$ en, op getalsverzamelingen, $\leqslant$, $\geqslant$, $<$ en $>$ géén equivalentierelaties. De eerste twee zijn wél lineaire ordeningsrelaties.

ii) Bekijk de eindige verzameling $V = \{1,2,3,4\}$. Definiëren we

$$R = \big\{\{1,1\},\{2,2\}\{2,3\},\{2,4\},\{3,2\},\{3,3\},\{3,4\},\{4,2\},\{4,3\},\{4,4\}\big\} \subset V \times V,$$

dan is R een equivalentierelatie op V. De equivalentieklassen zijn

$$[1] = \{1\} \quad \text{en} \quad [2] = [3] = [4] = \{2,3,4\}.$$

De quotiëntverzameling bestaat dus uit twee elementen.

iii) Definieer een relatie $\equiv_2$ op $\mathbb{Z}$ door $a \equiv_2 b$ precies dan als a en b dezelfde *pariteit* hebben — dat wil zeggen, ze zijn óf beide even óf beide oneven. Dit is een equivalentierelatie. Er zijn twee equivalentieklassen: de verzameling even getallen en de verzameling oneven getallen. De quotiëntverzameling wordt vaak genoteerd met $\mathbb{Z}_2$ of $\mathbb{Z}/2\mathbb{Z}$ en de 'verzameling restklassen modulo 2' genoemd. Zie het volgende voorbeeld voor een uitleg van deze naamgeving.

III.2.5 Stelling. Stel dat $\bigcirc$ een operator is en $\sim$ een equivalentierelatie op een verzameling V. Stel verder dat geldt

$$\forall_{a,b,c,d \in V} \quad (a \sim c \wedge b \sim d) \implies a \bigcirc b \sim c \bigcirc d.$$

Dan is er een unieke operator $\triangle$ op $R/\sim$ waarvoor geldt

$$\forall_{a,b \in V} \quad [a] \triangle [b] = [a \bigcirc b].$$

Voorts is $\triangle$ associatief (resp. commutatief) als $\bigcirc$ dat is. Voor een neutraal element e (resp. inverse b van a) onder $\bigcirc$ geldt dat $[e]$ (resp. $[b]$) een neutraal element (resp. inverse van $[a]$) is onder $\triangle$.

Compatibel

We noemen een operator en equivalentierelatie die aan de voorwaarde van de stelling voldoen *compatibel*. De operatie $\triangle$ noemen we de *geïnduceerde operatie*.

Bewijs. Zie Opgave III.2.1. ■

III.2.6 Voorbeeld. We veralgemeniseren het voorgaande voorbeeld. Zij n een geheel getal en noteer met $n\mathbb{Z}$ de verzameling veelvouden van n:

$$n\mathbb{Z} = \{rn \mid r \in \mathbb{Z}\} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}.$$

Definieer een relatie op $\mathbb{Z}$ door

$$a \equiv_n b \iff (a - b) \in n\mathbb{Z}.$$

Dit is een equivalentierelatie waarbij de quotiëntverzameling wordt genoteerd met $\mathbb{Z}_n$ of $\mathbb{Z}/n\mathbb{Z}$. De quotiëntverzameling wordt de 'verzameling restklassen modulo n genoemd. In deze quotiëntverzameling is er vanwege compatibiliteit een operatie optellen en vermenigvuldigen. Zie voor details en concrete voorbeelden Opgaven III.2.3 en III.2.4. Merk overigens op dat de equivalentierelatie vaak als volgt wordt genoteerd:

$$a \equiv b \pmod{n}.$$

Modulair rekenen of klokrekenen kom je soms in het voortgezet onderwijs tegen, bijvoorbeeld bij Wiskunde D. ■

Opgaven

1. Geef een bewijs van Stelling III.2.5.

2. (a) Bepaal alle lineaire ordeningen op de verzameling $\{1, 2, 3\}$.

(b) Hoeveel lineaire ordeningen zijn er op een verzameling met n elementen?

3. (a) Geef een zo concreet mogelijk beschrijving van de verzameling restklassen modulo 5.

(b) In $\mathbb{Z}$ zijn er maar twee elementen die een inverse voor vermenigvuldiging hebben, namelijk 1 en -1. Onderzoek welke elementen in $\mathbb{Z}/5\mathbb{Z}$ een inverse hebben.

(c) Doe hetzelfde voor $\mathbb{Z}/4\mathbb{Z}$.

(d) Veralgemeniseer voorgaande twee vragen naar inverses in $\mathbb{Z}/n\mathbb{Z}$ voor willekeurige n.

4. (a) Bewijs dat $\equiv_n$ inderdaad een equivalentierelatie op $\mathbb{Z}$ is.

(b) Zij $A \subset \mathbb{Z}$. Wat zijn noodzakelijke en voldoende voorwaarde voor A zodat

$$a \sim b \iff (a-b) \in A$$

een equivalentierelatie op $\mathbb{Z}$ definieert?

(c) Onder welke aanvullende voorwaarden is de equivalentierelatie compatibel met optellen? (Of zijn er geen aanvullende voorwaarden nodig?)

(d) Idem voor vermenigvuldigen.

5. (a) In Opgave III.2.4 heb je gezien dat er operaties 'optellen' en 'vermenigvuldigen' op $\mathbb{Z}/2\mathbb{Z}$ zijn. In Opgave II.1.1 ben je de notatie $\veebar$ tegengekomen voor 'exclusief of'. Onderzoek het verband tussen $\veebar$ en $\wedge$ enerzijds en $\mathbb{Z}/2\mathbb{Z}$ met optelling en vermenigvuldiging anderzijds. Betrek hierin ook de wetten van De Morgan uit Opgave II.1.3.

(b) Laat P, Q, R en S proposities zijn. Kun je nu zonder veel werk nagaan of

$$((P \veebar Q) \wedge (R \veebar S)) \iff ((P \wedge R) \veebar (P \wedge S) \veebar (Q \wedge R) \veebar (Q \wedge S))$$

een tautologie is?

IV NATUURLIJKE GETALLEN EN VOLLEDIGE INDUCTIE

Gebruikmakend van de voorafgaande drie hoofdstukken over verzamelingen en over logica gaan we de natuurlijke getallen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ met hun optelling, vermenigvuldiging en ordening en de basiseigenschappen daarvan wat formeler behandelen. In andere woorden, we zijn klaar om de wiskunde in te duiken. In het volgende hoofdstuk wordt dan hetzelfde gedaan voor de gehele en rationale getallen, waarna de lange reis wordt voortgezet naar de reële en complexe getallen.

Wat betekent het, dat we nu wiskunde gaan doen, uitgaand van logica en ZFC? In dit hoofdstuk betekent het dat we de verzameling van natuurlijke getallen, met optelling en vermenigvuldiging, axiomatisch behandelen, en laten zien hoe daar nieuwe uitspraken uit volgen. In Appendix VIII.3 wordt beschreven hoe het bestaan en de uniciteit in ZFC te bewijzen zijn.

Voordat we echt aan het werk gaan willen we nog een beschrijving geven van wat wij denken dat wiskundigen moeten doen, in de stijl van de eed van Hippocrates voor medici.

> *Wiskundigen geloven in de consistentie van ZFC zolang het tegendeel niet bewezen is. Zij geven stellingen die in de taal van ZFC geformuleerd kunnen worden en zij geven bewijzen van die stellingen die zo begrijpelijk mogelijk zijn voor hun collega's. Op verzoek helpen ze collega's hun werk te begrijpen. Met het oog op de komst van betrouwbare proofcheckers proberen ze bewijzen te geven die met zo min mogelijk moeite uitgewerkt kunnen worden tot formele bewijzen.*

IV.1 Axioma's voor $\mathbb{N}$

Alhoewel we allemaal weten, of misschien denken te weten, wat natuurlijke en gehele getallen zijn, en wat de gebruikelijke operaties als optelling en vermenigvuldiging daarop zijn, is het goed om een korte lijst eigenschappen, ofwel *axioma's*, te geven die deze getalsystemen precies karakteriseren. Het doel hiervan is dat er dan geen dubbelzinnigheid is over wat we wel en niet mogen aannemen. Een ander gevolg van de axiomatische benadering is dat het er niet meer toe doet wat ieder onder ons denkt dat natuurlijke getallen precies zijn, zolang ze maar aan de axioma's voldoen (denk hierbij maar aan de vele manieren waarop natuurlijke getallen geïmplementeerd kunnen worden in computers, als die een oneindig geheugen zouden hebben). De axioma's worden dan als uitgangspunt genomen in het bewijzen van weer andere beweringen over het getalsysteem $\mathbb{N}$.

Axioma's voor $\mathbb{N}$

We beginnen met de eigenschappen van de natuurlijke getallen en optelling. De *gegevens* zijn:

(a) een verzameling $\mathbb{N}$;
(b) elementen 0 en 1 in $\mathbb{N}$;
(c) een operatie $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a,b) \mapsto a+b$, de optelling;
(d) een operatie $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a,b) \mapsto ab$, de vermenigvuldiging.

De optelling voldoet aan de volgende *axioma's*:

(N0) de optelling is *commutatief*: $\forall a,b \in \mathbb{N},\ a+b = b+a$;
(N1) de optelling is *associatief*: $\forall a,b,c \in \mathbb{N},\ (a+b)+c = a+(b+c)$;
(N2) 0 is *neutraal* voor de optelling: $\forall a \in \mathbb{N},\ 0+a = a$ en $a+0 = a$;
(N3) de *schrapwet* geldt voor de optelling: $\forall a,b,c \in \mathbb{N},\ (a+b = a+c) \Rightarrow b = c$;
(N4) de elementen 0 en 1 zijn verschillend.

Bovenstaande eigenschappen gelden bijvoorbeeld ook voor de optelling van reële getallen. De twee axioma's hieronder zijn specifiek voor $\mathbb{N}$.

(N5) er is geen $a \in \mathbb{N}$ met $1+a = 0$ (m.a.w. 0 is het 'kleinst');
(N6) axioma van *inductie*: als $A \subseteq \mathbb{N}$ voldoet aan de eigenschappen $0 \in A$ en $(a \in A) \Rightarrow (1+a \in A)$, dan $A = \mathbb{N}$.

De bovenstaande axioma's beschrijven $\mathbb{N}$ met de elementen 0, 1 en de optelling volledig. Dit betekent het volgende. Men kan bewijzen (met behulp van Stelling IV.3.1) dat de bovenstaande lijst de gegevens $(\mathbb{N}, 0, 1, +)$ uniek karakteriseert, in de zin dat als $(\mathbb{N}', 0', 1', +')$ aan deze eigenschappen voldoet, er een unieke bijectie $f : \mathbb{N} \to \mathbb{N}'$ is zodat $f(0) = 0'$, $f(1) = 1'$, en zodat voor alle $a,b \in \mathbb{N}$ geldt dat $f(a+b) = f(a) +' f(b)$.

De intuïtieve beschrijving $\{0,1,2,3,\ldots\}$ van de verzameling natuurlijke getallen is te interpreteren in $\mathbb{N}$ door de getallen $2,3,\ldots$ te definiëren als $2 = 1+1$, $3 = 1+1+1$, $4 = 1+1+1+1$, $\ldots$.[1]

We hebben nog niets gezegd over de vermenigvuldiging in $\mathbb{N}$. Deze kan men uit de optelling construeren, maar in plaats daarvan zullen we de vermenigvuldiging hier axiomatisch vastleggen.

(N7) de vermenigvuldiging is *commutatief*: voor alle $a,b \in \mathbb{N}$ geldt $ab = ba$;
(N8) de vermenigvuldiging is *associatief*: voor alle $a,b,c \in \mathbb{N}$ geldt $(ab)c = a(bc)$;
(N9) 1 is *neutraal* voor de vermenigvuldiging: voor alle $a \in \mathbb{N}$ geldt $1 \cdot a = a$ en $a \cdot 1 = a$;
(N10) de *distributieve* wet geldt: voor alle $a,b,c \in \mathbb{N}$ geldt $a(b+c) = ab+ac$.

Terecht kan men opmerken dat de lijst eigenschappen toch nog vrij lang is. Een veel kortere karakterisering van de verzameling natuurlijke getallen met de afbeelding $a \mapsto a+1$ is gegeven door Peano's axioma's, zie Appendix VIII.3. In die appendix wordt ook het bestaan van een systeem $(\mathbb{N}, 0, 1, +, \cdot)$ afgeleid uit een Peano-systeem, en het bestaan van een Peano-systeem wordt bewezen in ZFC.

Alle bekende rekenregels kan men nu in principe afleiden uit de bovenstaande axioma's. Bijvoorbeeld:

IV.1.1 Propositie. Voor alle $n \in \mathbb{N}$ geldt $n \cdot 0 = 0$.

Bewijs. Zij $n \in \mathbb{N}$. Uit **(N2)** volgt $n \cdot 0 + 0 = n \cdot 0$. Uit **(N2)** volgt ook dat $0 = 0+0$, we hebben dus

$$n \cdot 0 + 0 = n \cdot 0 = n \cdot (0+0).$$

Axioma **(N10)** geeft nu $n \cdot (0+0) = n \cdot 0 + n \cdot 0$. Samen met bovenstaande formule levert dit

$$n \cdot 0 + 0 = n \cdot 0 + n \cdot 0.$$

Met de schrapwet **(N3)** leiden we nu af $0 = n \cdot 0$, hetgeen we moesten bewijzen. ∎

[1] Wie hier vragen over heeft wordt gevraagd contact op te nemen met Bas.

Ongelijkheden

Uit de optelling op $\mathbb{N}$ kunnen we ook een lineaire relatie $\leq$ definiëren als volgt:

$$n_1 \leq n_2 \quad \Leftrightarrow \quad \text{er is een } m \in \mathbb{N} \text{ met } n_1 + m = n_2.$$

De notatie $n_1 < n_2$ is een afkorting voor "$n_1 \leq n_2$ en $n_1 \neq n_2$". Analoog definiëren we $\geq$ en $>$.

IV.2 Volledige inductie

We beschrijven nu een belangrijke techniek om beweringen over natuurlijke getallen te bewijzen. Deze bewijstechniek is gerechtvaardigd door het axioma van inductie, **(N6)** in de lijst van axioma's voor $\mathbb{N}$.

Stel je voor dat we een uitspraak, geformuleerd in de taal van ZFC, van het type 'Voor alle $n \in \mathbb{N}$ geldt ...' willen bewijzen. We kunnen als volgt aan het werk gaan: we gaan eerst na dat de uitspraak juist is voor 0, en daarna laten we zien dat voor alle $n \in \mathbb{N}$ geldt dat *als* de uitspraak waar is voor n, *dan* ook voor $n+1$. Het axioma van inductie (ook wel Principe van Volledige Inductie geheten) garandeert nu dat de uitspraak juist is voor elk natuurlijk getal, want de deelverzameling $A \subseteq \mathbb{N}$ (die bestaat vanwege het afscheidingsaxioma uit Appendix VIII.2) van alle natuurlijke getallen waarvoor de uitspraak juist is, voldoet aan de twee eisen van het axioma van inductie, zodat $A = \mathbb{N}$. Een bewijs van dit type heet een *bewijs met volledige inductie*.

We illustreren de techniek aan de hand van een paar voorbeelden.

IV.2.1 Voorbeeld. We gaan bewijzen dat voor alle $n \in \mathbb{N}$ geldt:

$$\sum_{k=0}^{n} 2k = n(n+1).$$

We gebruiken inductie naar n.
STAP 1: Voor $n = 0$ volgt dit uit $2 \cdot 0 = 0 = 0 \cdot (0+1)$.
STAP 2: Laat $n \in \mathbb{N}$. Neem aan dat $\sum_{k=0}^{n} 2k = n(n+1)$ (dit heet de *inductieveronderstelling* of *inductiehypothese*). Dan geldt:

$$\sum_{k=0}^{n+1} 2k = \sum_{k=0}^{n} 2k + 2(n+1) \overset{(IV)}{=} n(n+1) + 2(n+1) = (n+1)(n+2).$$

De tweede gelijkheid op de regel hierboven volgt op grond van de inductieveronderstelling. ∎

Algemener kunnen we zo uitspraken van het type 'Voor alle $n \geqslant N$ geldt ...' bewijzen. We controleren dan de bewering voor $n = N$ en laten daarna weer zien dat voor alle $n \geq N$ geldt dat *als* de bewering voor n, *dan* ook voor $n+1$. Het axioma van inductie is dan van toepassing op de verzameling A van alle $k \in \mathbb{N}$ zó dat de bewering juist is voor $n = N + k$.

IV.2.2 Voorbeeld. Zij $x \neq 1$ een reëel getal. We bewijzen dat voor elk natuurlijk getal $n \geqslant 1$ geldt

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1.$$

STAP 1: De bewering is waar voor $n = 1$:

$$\frac{x^1 - 1}{x - 1} = \frac{x - 1}{x - 1} = 1.$$

STAP 2: Laat $n \geqslant 1$. Neem aan dat $(x^n-1)/(x-1) = x^{n-1}+x^{n-2}+\cdots+x^2+x+1$ (dit is de *inductieveronderstelling*). Dan geldt:

$$\begin{aligned}\frac{x^{n+1}-1}{x-1} &= \frac{x^{n+1}-x^n+x^n-1}{x-1}\\ &= \frac{x^n(x-1)}{x-1}+\frac{x^n-1}{x-1}\\ &= x^n+\frac{x^n-1}{x-1}\\ &\overset{(IV)}{=} x^n+x^{n-1}+x^{n-2}+\cdots+x^2+x+1.\end{aligned}$$

De laatste gelijkheid geldt op grond van de inductieveronderstelling. ∎

Binomium van Newton

We besluiten deze paragraaf met een stelling die voor de uitdrukking $(a+b)^n$, waarbij $n \in \mathbb{N}$ positief is, een mooie formule geeft. We spreken af dat voor alle $x \in \mathbb{R}$ geldt $x^0 = 1$.

Voor $n \in \mathbb{N}$ definiëren we $n!$ (spreek uit "*n-faculteit*") als:

$$n! = 1 \cdot 2 \cdot \cdots \cdot n,$$

met de afspraak dat $0! = 1$. (In de volgende paragraaf wordt het gebruik van $\cdots$ in deze definitie gerechtvaardigd, zie IV.3.3) Voor n en k in $\mathbb{N}$ met $k \leq n$ definiëren we de binomiaalcoëfficiënt $\binom{n}{k}$ (spreek uit "*n boven k*") als

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

IV.2.3 Stelling (Binomium van Newton)**.** Voor alle reële getallen a en b en elke $n \in \mathbb{N}$ geldt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k.$$

Bewijs. Laat $a, b \in \mathbb{R}$. STAP 1: De bewering is waar voor $n = 0$:

$$(a+b)^0 = 1 \qquad \text{en} \qquad \binom{0}{0}a^0b^0 = 1.$$

STAP 2: Laat $n \in \mathbb{N}$. Neem aan dat $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$ (dit is de *inductieveronderstelling*). Dan geldt

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n\\ &\overset{(IV)}{=} (a+b)\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k\\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1}\\ &= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=0}^{n-1}\binom{n}{k}a^{n-k}b^{k+1} + b^{n+1}.\end{aligned}$$

Door verschuiven van de sommatieindex in de tweede som krijgen we

$$\begin{aligned}\sum_{k=0}^{n-1}\binom{n}{k}a^{n-k}b^{k+1} &= \sum_{k=1}^{n}\binom{n}{k-1}a^{n-(k-1)}b^k\\ &= \sum_{k=1}^{n}\binom{n}{k-1}a^{n+1-k}b^k.\end{aligned}$$

We gebruiken nu de identiteit uit Opgave IV.2.17:

$$\begin{aligned}(a+b)^{n+1} &= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n+1-k} b^k + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) a^{n+1-k} b^k + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^k + b^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k.\end{aligned}$$

■

Welordening van $\mathbb{N}$.

Een fundamenteel gevolg van het axioma van inductie is dat elke niet-lege deelverzameling van $\mathbb{N}$ een kleinste element bevat.

IV.2.4 Stelling. Welordening van $\mathbb{N}$ Zij V een niet-lege deelverzameling van $\mathbb{N}$. Dan bestaat er een $v \in V$ zodat voor alle $w \in V$ geldt $w \geq v$.

Bewijs. Neem aan dat voor alle $v \in V$ er een $w \in V$ is met $w < v$. Hieruit volgt dat $0 \notin V$. Zij $A \subset \mathbb{N}$ de volgende verzameling

$$A = \{n \in \mathbb{N} : \text{voor alle } m \in \mathbb{N} \text{ met } m \leq n \text{ geldt } m \notin V\}.$$

Omdat $0 \notin V$ geldt $0 \in A$.

Neem nu aan dat $n \in A$, dus dan zitten $0, 1, \ldots, n$ niet in V. Als $n+1 \in V$ dan is $n+1$ een kleinste element in V, in tegenspraak met onze aanname, dus $n+1 \notin V$. Maar nu volgt dus dat $n+1 \in A$.

Omdat $0 \in A$ en omdat uit $n \in A$ volgt dat $n+1 \in A$, impliceert **(N6)** dat $A = \mathbb{N}$. Maar dan volgt dat $V = \varnothing$, een tegenspraak. ■

Opgaven

✍ **1.** Laat $a \in \mathbb{N}$ met $a \neq 0$. Bewijs uit de axioma's dat er een unieke $b \in \mathbb{N}$ is met $a = b+1$.

2. Zij $a, b \in \mathbb{N}$. Neem aan dat $ab = 0$. Bewijs dat $a = 0$ of $b = 0$. (*Hint*: gebruik voorgaande opgave, en gebruik dat voor alle $n \in \mathbb{N}$ geldt $n \cdot 0 = 0$, zie Propositie IV.1.1.)

3. Doe nog een keer opgaven a en b van Opgave II.4.4, en vergelijk je uitwerkingen met die van de eerste keer.

4. Bewijs met behulp van volledige inductie dat voor alle natuurlijke getallen $n \geqslant 1$ de volgende formules gelden:

(a) $1 - 3 + 5 - 7 + \cdots + (-1)^{n-1}(2n-1) = (-1)^{n-1} n$;

(b) $1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n+1)(2n+1)/6$.

✍ **5.** Verzin zelf een formule voor

$$1 + 3 + 5 + \cdots + (2n+1)$$

en bewijs met behulp van volledige inductie dat je formule juist is voor elk natuurlijk getal n.

6. Bewijs met behulp van volledige inductie dat voor alle natuurlijke getallen $n \geqslant 1$ de volgende formules gelden:

(a) $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\dfrac{1}{3\cdot 4}+\cdots+\dfrac{1}{n\cdot(n+1)}=\dfrac{n}{n+1}$;

(b) $\dfrac{1}{1\cdot 3}+\dfrac{1}{3\cdot 5}+\dfrac{1}{5\cdot 7}+\cdots+\dfrac{1}{(2n-1)(2n+1)}=\dfrac{n}{2n+1}$.

7. Bewijs met behulp van volledige inductie: voor alle $n \geqslant 1$ geldt:

$$\sum_{k=1}^{n} 4k^3 = n^2(n+1)^2.$$

8. Bewijs met behulp van volledige inductie dat voor elke $n \in \mathbb{N}$ geldt $2^n > n$.

9. Bewijs met behulp van volledige inductie dat voor elk natuurlijk getal $n \geqslant 4$ geldt $n! > 2^n$.

✍ **10.** Bewijs met behulp van volledige inductie dat voor elk natuurlijk getal n het getal $11^n - 4^n$ deelbaar is door 7.

11. Bewijs met behulp van volledige inductie dat de som van de derde machten van drie opeenvolgende natuurlijke getallen deelbaar is door 9.

12. Gegeven zijn n punten in $\mathbb{R}^2$, $n \geqslant 3$, met de eigenschap dat geen drie punten op een lijn liggen. Bewijs met behulp van volledige inductie dat de punten door $n(n-1)/2$ verschillende lijnen te verbinden zijn, en niet door minder lijnen.

13. Bewijs met behulp van volledige inductie dat voor alle $n \geqslant 1$ geldt dat n verschillende lijnen in het platte vlak die door de oorsprong gaan het vlak in $2n$ gebieden verdelen.

14. Zij x een reëel getal. Laat zien met behulp van volledige inductie dat voor elke $n \in \mathbb{N}$ geldt

$$|\sin nx| \leqslant n|\sin x|.$$

✍ **15.** Zij $P(n)$ de bewering 'n^2+3n+1 is een even getal'. Laat zien dat voor elke $n \in \mathbb{N}$ geldt

als $P(n)$ waar is dan is $P(n+1)$ waar.

Geldt $P(n)$ voor elke $n \in \mathbb{N}$? Verklaar je antwoord.

✍ **16.** Vind de fout in het volgende 'bewijs met volledige inductie' dat alle mensen op dezelfde dag jarig zijn:
Voor $n \in \mathbb{N}$ met $n \geq 1$, zij P_n de bewering: 'in elke verzameling van n mensen is iedereen op dezelfde dag jarig.'
STAP 1: Als we slechts één mens beschouwen is de bewering P_1 duidelijk juist.
STAP 2: Laat $n \geq 1$, en neem aan dat in elke verzameling van n mensen iedereen op dezelfde dag jarig is. Stel dat we nu $n+1$ mensen hebben. We kunnen ze nummeren: $m_1, m_2, \ldots, m_{n+1}$. Beschouw nu de verzamelingen $A = \{m_1, m_2, \ldots, m_n\}$ en $B = \{m_2, \ldots, m_n, m_{n+1}\}$. Beide verzamelingen hebben n elementen en dus volgens de inductieveronderstellig is iedereen in A op dezelfde dag jarig, maar ook iedereen in B heeft de verjaardag op dezelfde dag. Hieruit volgt dat iedereen in $A \cup B$ ook op dezelfde dag jarig is.
Volgens het Principe van Volledige Inductie kunnen we concluderen dat P_n juist is voor elke $n \geqslant 1$, en dus zijn alle mensen op dezelfde dag jarig.

17. Bewijs de volgende eigenschappen van de binomiaalcoëfficiënten.

(a) Laat zien dat voor alle $1 \leqslant m \leqslant n$ de volgende identiteit geldt:

$$\binom{n}{m-1} + \binom{n}{m} = \binom{n+1}{m}.$$

(b) Laat zien dat voor alle $1 \leqslant m \leqslant n$ de volgende identiteit geldt:

$$\sum_{k=m}^{n} \binom{k}{m} = \binom{n+1}{m+1}.$$

(c) Toon aan: voor alle $n \in \mathbb{N}$ geldt

$$\sum_{m=0}^{n} \binom{n}{m} = 2^n.$$

(d) Toon aan: voor alle $n \in \mathbb{N}$, $n \geqslant 1$ geldt

$$\sum_{m=0}^{n} \binom{n}{m} (-1)^m = 0.$$

(e) Toon aan dat $\binom{n}{m} \in \mathbb{N}$ voor alle $n, m \in \mathbb{N}$ met $n \geqslant m$.

(f) Bewijs dat als n een priemgetal is dan is $\binom{n}{m}$ deelbaar door n voor elke $m \in \mathbb{N}$ met $1 \leqslant m \leqslant n-1$.

✯ **18.** Toon aan dat $\binom{n}{k}$ het aantal manieren is om k mensen uit een groep van n mensen te kiezen.

IV.3 De recursiestelling

Soms is het nodig functies met domein $\mathbb{N}$ *recursief* te definiëren. De volgende stelling legt uit wat we hier precies mee bedoelen. Wie deze stelling wil gebruiken om uit de Peano-axioma's andere resultaten af te leiden, zoals bijvoorbeeld het bestaan van een getalsysteem $(\mathbb{N}, 0, 1, +, \cdot)$, moet hieronder $n+1$ lezen als $S(n)$, de successor van n.

IV.3.1 Stelling. Laat X een verzameling zijn, $x \in X$, en $F\colon X \to X$ een afbeelding. Dan is er een unieke $f\colon \mathbb{N} \to X$ zó dat:

$$f(0) = x \text{ en voor alle } n \in \mathbb{N} \text{ geldt } f(n+1) = F(f(n)).$$

Bewijs. Het idee van het bewijs is simpelweg dat we de grafiek van f moeten maken. Laat Y de verzameling zijn van alle deelverzamelingen $\Gamma \subseteq \mathbb{N} \times X$ met de eigenschappen:

1. $(0, x) \in \Gamma$;
2. als $(n, y) \in \Gamma$, dan $(n+1, F(y)) \in \Gamma$.

Omdat $\mathbb{N} \times X$ aan deze twee eigenschappen voldoet, is Y niet leeg. Laat nu f de doorsnede zijn van alle elementen van Y. We gaan bewijzen dat f de gevraagde functie is.

We bewijzen met inductie dat voor alle $n \in \mathbb{N}$ er een $y \in X$ is met $(n, y) \in f$. Dit is duidelijk voor $n = 0$: voor iedere $\Gamma \in Y$ geldt dat $(0, x) \in \Gamma$, dus $(0, x) \in f$. Laat nu $n \in \mathbb{N}$, en neem aan dat $(n, y) \in f$. Dan geldt voor alle $\Gamma \in Y$ dat $(n, y) \in \Gamma$, en dus ook dat $(n+1, F(y)) \in \Gamma$, en dus dat $(n+1, F(y)) \in f$.

Nu bewijzen we met inductie dat voor alle $n \in \mathbb{N}$ geldt dat er ten hoogste één $y \in X$ is met $(n, y) \in f$.
Stap 1. Stel dat $(0, y) \in f$ met $y \neq x$. Dan is $f \setminus \{(0, y)\}$ ook een element van Y. Maar dan geldt $(0, y) \notin f$, want f is de doorsnede van alle $\Gamma \in Y$, en dus bevat in $f \setminus \{(0, y)\}$. Deze tegenspraak bewijst dat er geen $y \in X$ is met $y \neq x$ en $(0, y) \in f$.
Stap 2. Laat $n \in \mathbb{N}$, en neem aan dat er precies één $y \in X$ is met $(n, y) \in f$. Stel nu dat er een $y' \in X$ is met $y' \neq F(y)$ en $(n+1, y') \in f$. Dan is $f \setminus \{(n+1, y')\}$ ook een element van Y. Maar dan geldt $(n+1, y') \notin f$, want f is de doorsnede van alle $\Gamma \in Y$, en dus bevat in $f \setminus \{(n+1, y')\}$. Deze tegenspraak bewijst dat er geen $y' \in X$ is met $y' \neq F(y)$ en $(n+1, y') \in f$.

We hebben nu bewezen dat f een functie van $\mathbb{N}$ naar X is. We hebben al bewezen dat $f(0) = x$. We moeten nog bewijzen dat voor alle $n \in \mathbb{N}$ geldt dat $f(n+1) = F(f(n))$. Laat $n \in \mathbb{N}$. Dan is $(n, f(n)) \in f$, dus geldt voor alle $\Gamma \in Y$ dat $(n, f(n)) \in \Gamma$. Maar dan geldt voor alle $\Gamma \in Y$ dat $(n+1, F(f(n))) \in \Gamma$. Dus $(n+1, F(f(n))) \in f$, hetgeen betekent dat $f(n+1) = F(f(n))$.

Nu moeten we nog bewijzen dat f de enige functie is met de gevraagde eigenschappen. Laat $g : \mathbb{N} \to X$ een functie zijn met die eigenschappen. Dan is (de grafiek van) g een element van Y, en dus geldt dat $f \subseteq g$. Maar dan geldt $f = g$ omdat f en g functies zijn. ∎

IV.3.2 Gevolg. Laat X een verzameling zijn. Laat $g : \mathbb{N} \times X \to X$, en $x \in X$. Dan is er een unieke $f : \mathbb{N} \to X$ met:

$$f(0) = x \text{ en voor alle } n \in \mathbb{N} \text{ geldt } f(n+1) = g(n, f(n)).$$

Bewijs. Laat $F : \mathbb{N} \times X \to \mathbb{N} \times X$ gegeven zijn door $F(a, y) = (a+1, g(a, y))$. Vanwege de vorige stelling is er een unieke $h : \mathbb{N} \to \mathbb{N} \times X$ met $h(0) = (0, x)$, en met, voor alle $n \in \mathbb{N}$, $h(n+1) = F(h(n))$. Laat $h_1 : \mathbb{N} \to \mathbb{N}$ en $h_2 : \mathbb{N} \to X$ gedefinieerd zijn als volgt: voor elke $n \in \mathbb{N}$ geldt

$$h(n) = (h_1(n), h_2(n)).$$

Dan geldt:

$$\begin{aligned} (h_1(0), h_2(0)) &= (0, x), \\ (\forall n \in \mathbb{N}) : (h_1(n+1), h_2(n+1)) &= h(n+1) = F(h(n)) = F(h_1(n), h_2(n)) = \\ &= (h_1(n)+1, g(h_1(n), f(h_1(n)))). \end{aligned}$$

Met inductie volgt nu dat voor alle $n \in \mathbb{N}$: $h_1(n) = n$. En dus geldt dat $h_2(0) = x$, en voor alle $n \in \mathbb{N}$: $h_2(n+1) = g(n, h_2(n))$. Uit inductie volgt ook dat h_2 de enige functie is met deze eigenschappen. ∎

faculteit

Als eerste toepassing definiëren we de functie 'faculteit' van $\mathbb{N}$ naar $\mathbb{N}$.

IV.3.3 Definitie. Laat $n \mapsto n!$ de unieke functie van $\mathbb{N}$ naar $\mathbb{N}$ zijn, met de eigenschappen: $0! = 1$, en voor alle $n \in \mathbb{N}$ geldt $(n+1)! = (n+1) \cdot n!$. (We passen hier Gevolg IV.3.2 toe, met $X = \mathbb{N}$, $x = 1$ en $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a, b) \mapsto (a+1)b$.)

IV.3.4 Definitie. Voor $n, k \in \mathbb{N}$ met $k \leq n$ definiëren we een rationaal getal door:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

De getallen $\binom{n}{k}$ heten *binomiaalcoëfficiënten*.

binomiaalcoëfficiënt

Per definitie is $\binom{n}{k}$ in $\mathbb{Q}$, maar uit Opgave IV.2.17 volgt $\binom{n}{k} \in \mathbb{N}$.

V GETALSSYSTEMEN

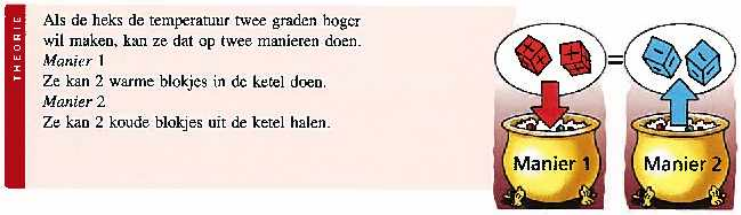
In dit hoofdstuk kijken we naar *getalssystemen*. Dat is geen precies gedefinieerd wiskundig begrip, maar een wat losse term om allerlei soorten getallen onder te vangen, zoals natuurlijke, reële of complexe. We noemen dit 'systemen' en niet 'verzamelingen', omdat de getalsverzamelingen zijn voorzien van structuren zoals optellen of vermenigvuldigen.

Er zijn veel redenen om het systeem van natuurlijke getallen, het onderwerp van het vorige hoofdstuk, uit te breiden naar andere getalssystemen zoals $\mathbb{Z}$ of $\mathbb{R}$. Dergelijke uitbreidingen hebben in de geschiedenis van de wiskunde tot grote conceptuele problemen geleid. De Grieken bijvoorbeeld beschouwden $\sqrt{2}$ niet als een getal; de grote Arabische wiskundige al-Chwarizmi plaatste vergelijkingen van de vorm $x^2 + bx = c$ in een andere categorie als $x^2 + c = bx$; in Engeland werden tot ver in de negentiende eeuw academische discussies gevoerd over het bestaan van negatieve getallen en breuken; en de introductie van 'de wortel uit -1' (bijvoorbeeld bij Wiskunde D op het vwo) lijkt nog steeds met enige magie omgeven.

Doel van dit hoofdstuk is het mysterie weg te nemen door te laten zien hoe de moderne wiskunde omgaat met uitbreidingen van getalssystemen. Dat gebeurt vanuit twee perspectieven: *structureel* en *constructief*. In het structurele perspectief richten we ons op de structuur van algebraïsche operaties. Met behulp van de eigenschappen voor rekenoperaties uit hoofdstuk III zullen we komen tot axiomatisch beschrijvingen van getalssystemen, zoals we dat in het vorige hoofdstuk al voor $\mathbb{N}$ hebben gedaan. Vanuit het oogpunt van de schoolwiskunde is deze systematisering een belangrijk doel dat in dit hoofdstuk wordt bereikt. Bij het constructieve perspectief buigen we ons over de vraag hoe je getalssystemen kunt 'maken' met enkel verzamelingstheoretische technieken. Voor het doen van wiskunde is eigenlijk alleen het eerste perspectief relevant. Sterker nog: over de structuur van getalssystemen als $\mathbb{Z}$ of $\mathbb{R}$ zijn alle wiskundigen het wel eens, maar er zijn heel veel verschillende manieren om deze getalssystemen te construeren en de methode die we in deze tekst kiezen leidt natuurlijk niet tot andere kennis over getallen dan wanneer er andere keuzes gemaakt zouden zijn. Toch behandelen we het constructieve perspectief wel, zij het pas aan het einde van het hoofdstuk, omdat het illustreert hoe de wiskunde uit verzamelingen kan worden opgebouwd.

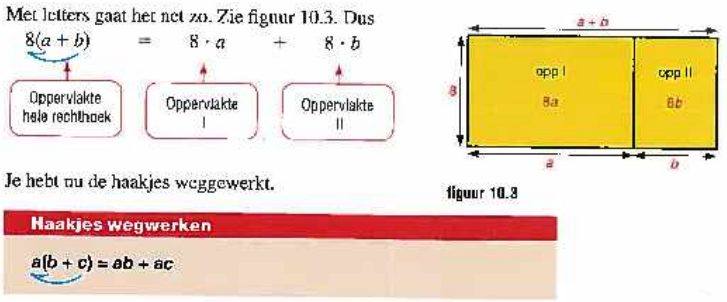
V.0.5 Voorbeeld. Negatieve getallen worden in de onderbouw geïntroduceerd. Hierbij zul je als docent belangrijke didactische keuzes moeten maken. De getallenlijn is een natuurlijke metafoor om negatieve getallen te introduceren, maar enkel op grond hiervan zal het voor leerling niet meteen duidelijk zijn hoe met negatieve getallen gerekend kan worden. Schoolboeken gebruiken soms 'denkmodellen' om dit uit te leggen, zoals de heks (zie Figuur 5.1). Het gebeurt ook dat docenten rekenregels zoals 'min keer min is plus' gewoon poneren.

Ook als leerlingen eenmaal vertrouwd zijn geraakt met negatieve getallen,



Figuur 5.1 – Het denkmodel van de heks voor rekenen met negatieve getallen in het schoolboek *Moderne wiskunde*.

krijg je nog af en toe met de uitbreiding van positieve getallen naar negatieve getallen te maken. Dat gebeurt bijvoorbeeld bij machtsverheffen: $3^2 = 3 \cdot 3$, maar wat betekent 3^{-2} (of nog erger: $3^{-\pi}$)? Het gebeurt ook bij de introductie van de distributieve eigenschap, die in schoolmethodes bijna altijd inzichtelijk wordt gemaakt door middel van een oppervlaktemodel (zie Figuur 5.2), waarbij de lengtes noodzakelijkerwijs niet negatief zijn. ▬



Figuur 5.2 – De distributieve eigenschap van optelling in het schoolboek *Getal & Ruimte*.

V.0.6 Voorbeeld. In de bovenbouw komen bij veel wiskundevakken asymptoten van functies ter sprake en bij Wiskunde B op vwo ook formele limietberekeningen. Dat vraagt om zorgvuldige formuleringen. Leerlingen hebben soms de neiging dingen op te schrijven als $\frac{1}{0} = \infty$ en in het wat losser taalgebruik ontvalt een docent ook wel eens dit soort uitspraken. Waarom moeten we hier zo zorgvuldig zijn? En als je 'de wortel uit -1' kennelijk gewoon als getal kunt beschouwen, waarom kun je dan niet iets soortgelijks doen voor 'delen door nul'? We zullen in dit hoofdstuk zien dat kennis van de structuur van getalssystemen voor dit soort vragen essentieel is. ▬

V.1 Een klein beetje algebra

In de algebra bestudeer je verzamelingen met operaties die diverse eigenschappen hebben. In deze tekst lichten we twee structuren uit, namelijk ringen en lichamen. De definities hiervan zijn erg abstract. Het voordeel van deze abstracte aanpak is dat je allerlei rekenregels die in diverse systemen gelden maar een keer hoeft te bewijzen — dat is de kracht van algebra! In het vak "Algebra/Getaltheorie" zal dit voordeel nog duidelijker blijken.

Ring

V.1.1 Definitie. Een *ring* is een systeem $(R, +_R, \cdot_R, 0_R, 1_R)$ (dat gemakshalve vaak wordt genoteerd met enkel R) bestaande uit:

- een verzameling R,
- een operatie $+_R$ op R die *optellen* wordt genoemd,
- een operatie $\cdot_R$ op R die *vermenigvuldigen* wordt genoemd,
- elementen 0_R en 1_R in R,

waarvoor geldt:

1. de operatie optelling
   (a) is associatief en commutatief (dus $a +_R (b +_R c) = (a +_R b) +_R c$ en $a +_R b = b +_R a$ voor alle $a, b, c \in R$),
   (b) heeft 0_R als neutraal element,
   (c) heeft een inverse (genoteerd met $-_R a$) voor ieder element $a \in R$;
2. de operatie vermenigvuldiging
   (a) is associatief (dus $a \cdot_R (b \cdot_R c) = (a \cdot_R b) \cdot_R c$ voor alle $a, b, c \in R$),
   (b) heeft 1_R als neutraal element;
3. vermenigvuldiging is distributief over optelling (dus $a \cdot_R (b +_R c) = a \cdot_R b +_R a \cdot_R c$ en $(b +_R c) \cdot_R a = b \cdot_R a +_R c \cdot_R a$ voor alle $a, b, c \in R$).

Een *commutatieve ring* is een ring R waar de vermenigvuldiging ook nog eens commutatief is (dus $a \cdot_R b = b \cdot_R a$ voor alle $a, b \in R$).

V.1.2 Voorbeelden. De verzameling gehele getallen $\mathbb{Z}$ met de gebruikelijke optelling en vermenigvuldiging en elementen 0 en 1 is een commutatieve ring. Dat geldt ook voor de reële getallen $\mathbb{R}$. Het systeem van natuurlijke getallen is géén ring, omdat geen enkel element uitgezonderd 0 een inverse onder optelling heeft.

De verzameling $M_n(\mathbb{R})$ van $n \times n$-matrices met reële coëfficiënten met optelling en vermenigvuldiging van matrices (zie Hoofdstuk VII) is ook een ring. Deze ring is niet commutatief als $n > 1$.

De verzameling $\mathbb{R}[X]$ van polynomen $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ met reële coëfficiënten geeft een commutatieve ring wanneer we voor optelling en vermenigvuldiging gewoon het optellen en vermenigvuldigen van polynomen nemen.

We schreven hierboven dat veel bekende rekenregels in een ring geldig zijn — maar je zal ze natuurlijk wel eerst moeten bewijzen! Om een idee te geven, noemen we er een paar in de categorie 'min maal min is plus'.

V.1.3 Stelling. In een ring R geldt voor alle $a, b \in R$:

i) $a \cdot_R 0_R = 0_R \cdot_R a = 0_R$,
ii) $-_R(a +_R b) = (-_R a) +_R (-_R b)$,
iii) $-_R(-_R a) = a$,
iv) $-_R(a \cdot_R b) = (-_R a) \cdot_R b = a \cdot_R (-_R b)$.
v) $(-_R a) \cdot_R (-_R b) = a \cdot_R b$.

Bewijs. (i) Er geldt

$$a \cdot_R 0_R = a \cdot_R (0_R +_R 0_R) = a \cdot_R 0_R +_R a \cdot_R 0_R.$$

Tel nu bij de linker en rechter term van de gelijkheid de inverse van $a \cdot_R 0_R$ op en we krijgen $0_R = a \cdot_R 0_R$. Op soortgelijke manier volgt $0_R = 0_R \cdot_R a$. (Vergelijk dit met het bewijs van Propositie IV.1.1 — zie je het subtiele verschil?)

De overige onderdelen zijn onderwerp van Opgave V.1.1. ∎

Lichaam

Het zal je zijn opgevallen dat er zelfs in een commutatieve ring een asymmetrie is tussen optellen en vermenigvuldigen: aftrekken (gedefinieerd als in Voorbeeld III.1.11) kan wel, maar delen kan niet. In een lichaam kan dit wel:

V.1.4 Definitie. Een *lichaam* (Vlaams: *veld*, Engels: *field*) is een commutatieve ring $(F, +_F, \cdot_F, 0_F, 1_F)$ met $0_F \neq 1_F$ waarin ieder element ongelijk aan 0_F een inverse onder vermenigvuldiging heeft. De inverse van $a \in F$ noteren we met a_F^{-1}.

Eindig lichaam

V.1.5 Voorbeelden. De systemen van rationale ($\mathbb{Q}$), reële ($\mathbb{R}$) en complexe ($\mathbb{C}$) getallen zijn voorbeelden van lichamen.

In Voorbeeld III.2.6 is voor ieder geheel getal n de verzameling $\mathbb{Z}/n\mathbb{Z}$ van *restklassen modulo n* gedefinieerd, inclusief optelling en vermenigvuldiging. Dit vormt een commutatieve ring. In Opgave III.2.3 ontdek je dat deze ring een lichaam is precies dan als $|n|$ een *priemgetal* is. Dit is een voorbeeld van een *eindig lichaam*. Voor een priemgetal p is het gebruikelijk de ring $\mathbb{Z}/p\mathbb{Z}$ te noteren met $\mathbb{F}_p$. Zie ook Opgave V.1.6.

In de volgende stelling gebruiken we de notatie $\frac{a}{c}$ voor ac^{-1} en we laten voor het gemak de subscript $_R$ weg.

V.1.6 Stelling. Zij F een lichaam met $a, b, c, d \in F$ en $c, d \neq 0$.

i) als $ab = 0$, dan $a = 0$ of $b = 0$;
ii) $\frac{a}{c} \cdot \frac{b}{d} = \frac{ab}{cd}$;
iii) $(\frac{c}{d})^{-1} = \frac{d}{c}$;
iv) $\frac{a}{c} + \frac{b}{d} = \frac{ad+bc}{cd}$;
v) $\frac{a}{c} = \frac{ad}{cd}$.

Bewijs. Zie Opgave V.1.7. ∎

Homomorfisme

In het eerste hoofdstuk hebben we gekeken naar afbeeldingen (functies) tussen twee verzamelingen. In de algebra kijk je met name naar een speciale klasse van afbeeldingen, namelijk diegene die de *structuur* van optelling en vermenigvuldiging behouden.

V.1.7 Definitie. Gegeven twee ringen R en S. Een *homomorfisme* van R naar S is een functie $f : R \to S$ waarvoor geldt:

- optelling blijft behouden: voor alle $a, b \in R$ geldt $f(a +_R b) = f(a) +_S f(b)$;
- vermenigvuldiging blijft behouden: voor alle $a, b \in R$ geldt $f(a \cdot_R b) = f(a) \cdot_S f(b)$;
- de eenheid van vermenigvuldiging blijft behouden: $f(1_R) = 1_S$.

Je zou misschien verwachten dat ook geëist moet worden dat de eenheid voor optelling behouden blijft, maar dat volgt uit de andere voorwaarden:

V.1.8 Lemma. Voor een homomorfisme van ringen $f : R \to S$ geldt $f(0_R) = 0_S$ en voor alle $a \in R$ geldt $f(-_R a) = -_S f(a)$. Als a een inverse a_F^{-1} heeft in R, dan geldt bovendien dat $f(a_R^{-1})$ de inverse is van $f(a)$ in S: dus $f(a_R^{-1}) = (f(a))_S^{-1}$.

Bewijs. Er geldt

$$f(0_R) = f(0_R +_R 0_R) = f(0_R) +_S f(0_R).$$

Trekken we nu in de linker en rechter term van deze vergelijking $f(0_R)$ af, dan krijgen we $0_S = f(0_R)$.

Voorts geldt:

$$f(-_R a) + f(a) = f((-_R a) +_R a) = f(0_R) = 0_S$$

en dus is $f(-_R a)$ de inverse van $f(a)$ in S.

En ten slotte:

$$f(a_R^{-1}) \cdot_S f(a) = f(a_R^{-1} \cdot_R a) = f(1_R) = 1_S.$$

■

Isomorfisme

V.1.9 Definitie. Een *isomorfisme* is een homomorfisme $f : R \to S$ waarvoor geldt dat er een homomorfisme $f^{-1} : S \to R$ bestaat zodat $f \circ f^{-1} = \mathrm{id}_S$ en $f^{-1} \circ f = \mathrm{id}_R$. (Hier staat id_R voor de identiteitsafbeelding $R \to R$, $x \mapsto x$.)

De notatie $R \cong S$ betekent: er bestaat een isomorfisme $R \to S$. We zeggen dan dat R en S *isomorf* zijn.

Discussie isomorfisme

Als $f : R \to S$ een isomorfisme is, dan vertalen f en f^{-1} alle eigenschappen van R en S als ringen in elkaar. Het woord 'isomorfisme' is opgebouwd uit 'iso' (Grieks voor 'gelijk') en 'morf' (Grieks voor 'vorm'). Deze term wordt in de wiskunde ook voor andere objecten dan ringen gebruikt (bijvoorbeeld in Hoofdstuk VII voor vectorruimten). Als in de wiskunde een eigenschap van een bepaald soort object wordt gegeven (bijvoorbeeld 'commutatief' voor ringen) dan is het goed om na te gaan of de eigenschap equivalent is voor isomorfe objecten. Als dat niet zo is, dan betreft het een gevaarlijke definitie en degene die die definitie maakt verdient de vraag of hij/zij het echt zo bedoelt.

V.1.10 Stelling. Een bijectief homomorfisme is een isomorfisme.

Bewijs. Zie Opgave V.1.8. ■

Geordende ring

V.1.11 Definitie. Een *geordende ring* is een ring R met een relatie $\leqslant$ waarvoor geldt:

- $\leqslant$ is een lineaire ordening;
- voor alle $a, b, c \in R$ geldt $a \leqslant b \Rightarrow a +_R c \leqslant b +_R c$;
- voor alle $a, b, c \in R$ geldt $(a \leqslant b \wedge 0_R \leqslant c) \Rightarrow a \cdot_R c \leqslant b \cdot_R c$.

Een element $a \in R \setminus \{0_R\}$ heet *positief* als $0 \leqslant a$ en *negatief* als $a \leqslant 0_R$. De deelverzameling van positieve elementen noteren we met R_+.
Als R een lichaam is en een geordende ring, dan noemen we het een *geordend lichaam*.

Let op de extra voorwaarde $0_R \leqslant c$ in de laatste eigenschap. Bij vermenigvuldiging met negatieve getallen 'klapt het teken om' (Opgave V.1.9). Merk ook op dat 'niet negatief' niet hetzelfde is als 'positief' — deze fout wordt wel eens gemaakt, hoewel er ook (briljante) wiskundeteksten zijn waar in wordt afgesproken (!) dat 0 ook positief wordt genoemd. We definiëren de *absolutewaardefunctie* $R \to R$, $a \mapsto |a|$ door

$$|a| = \begin{cases} a & \text{als } a \text{ niet negatief is,} \\ -_R a & \text{als } a \text{ negatief is.} \end{cases}$$

Uit Opgave V.1.9 volgt $0_R \leqslant |a|$.

Opgaven

✍ **1.** Bewijs de nog niet bewezen onderdelen van Stelling V.1.3.

2. Zij R een ring en zij a, b, c en d elementen van R. Bewijs dat

$$(a+b)(c+d) = ac + ad + bc + bd.$$

(We hebben voor het gemak de index $_R$ uit de notatie weggelaten.)

3. In de ring van gehele getallen geldt de volgende eigenschap:

$$ab = 0 \qquad \Longrightarrow \qquad a = 0 \quad \vee \quad b = 0.$$

Dit geldt echter niet in iedere ring! (Een commutatieve ring met $0 \neq 1$ waarvoor deze eigenschap geldt, wordt in de algebra een *integriteitsdomein* genoemd.)

(a) Geef een tegenvoorbeeld van de vorm $\mathbb{Z}/n\mathbb{Z}$ voor een zekere $n \in \mathbb{Z}$.

(b) Geef een tegenvoorbeeld in de ring $M_2(\mathbb{R})$ van 2×2-matrices met reële coëfficiënten.

(c) Laat zien dat de eigenschap in een *lichaam* wel altijd geldt.

4. Zij $f : R \to S$ en $g : S \to T$ twee homomorfismes van ringen. Bewijs dat de samenstelling $g \circ f$ ook een homomorfisme is.

5. Als $n \in \mathbb{N}$ en $a \in R$, dan kunnen we een nieuw element in R construeren door a precies n keer bij zichzelf op te tellen. We noteren dit element met na, hetgeen niet verward moet worden met de vermenigvuldiging binnen R. Een precieze definitie gebruikt recursie.

(a) Geef een formele definitie met behulp van recursie.

(b) Onderzoek of de volgende rekenregels gelden:

$$\begin{aligned} (n+m)a &= na + ma; & (nm)a &= n(ma); \\ n(a+b) &= na + nb; & n(ab) &= (na)b. \end{aligned}$$

De *canonieke functie* $c : \mathbb{N} \to R$ is de functie gedefinieerd door $c(n) = n1_R$. Voor deze functie geldt $c(0) = 0_R$, $c(1) = 1_R$, $c(n+m) = c(n) + c(m)$ en $c(nm) = c(n) \cdot_R c(m)$.

(c) Bewijs deze uitspraken.

(d) Definieer een afbeelding $f : \mathbb{Z} \to M_n(\mathbb{R})$ (naar de ring van $n \times n$-matrices) door $a \in \mathbb{Z}$ te sturen naar a keer de eenheidsmatrix. Bewijs dat f een homomorfisme is.

(e) Algemener: bewijs dat er voor iedere ring R een *uniek* homomorfisme $\mathbb{Z} \to R$ bestaat.

6. Voor deze opgave is Opgave V.1.5 vereist. Gegeven is een lichaam F. Bekijk het inversebeeld $c^{-1}(0)$ van de canonieke afbeelding $c : \mathbb{N} \to F$. Als dit inversebeeld een positief getal bevat, dan bevat het een kleinste positieve getal n. We zeggen dat F *karakteristiek* n heeft. Als er geen positief getal is, dan zeggen we dat F *karakteristiek* 0 heeft.

(a) Bewijs dat n een priemgetal moet zijn.

In Voorbeeld V.1.5 is voor een priemgetal p het eindig lichaam $\mathbb{F}_p$ met p elementen geïntroduceerd.

(b) Laat zien: er bestaat een homomorfisme $\mathbb{F}_p \to F$ als, en precies dan als, F karakteristiek p heeft.

(c) Laat zien: er bestaat een homomorfisme $\mathbb{Q} \to F$ als, en precies dan als, F karakteristiek 0 heeft.

(d) Toon aan dat de homomorfismes in de vorige twee onderdelen, als ze bestaan, uniek zijn en injectief.

(e) Stel F is een geordend lichaam. Laat zien dat F karakteristiek 0 heeft.

7. Bewijs Stelling V.1.6.

✍ **8.** Bewijs Stelling V.1.10.

9. Zij R een geordende ring met meer dan één element. We laten voor het gemak de index $_R$ uit de notatie weg. Bewijs de volgende uitspraken.

(a) $0 \leqslant 1$;

(b) $\forall_{a\in R}(0 \leqslant a \vee 0 \leqslant -a)$;

(c) $\forall_{a,b,c\in R}(a \leqslant b \wedge c \leqslant 0) \implies bc \leqslant ac$;

(d) $\forall_{a,b,c,d\in R}(a \leqslant b \wedge c \leqslant d) \implies a + c \leqslant b + d$;

(e) $\forall_{a\in R}(a \leqslant 0 \iff 0 \leqslant -a)$.

V.2 De ring van gehele getallen

We zullen in deze paragraaf de *verzameling van gehele getallen*

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

bestuderen, samen met de optel- en vermenigvuldigingsstructuur daarop. Een *constructie* stellen we uit tot paragraaf V.5.

Het systeem van gehele getallen is een commutatieve ring. De ring $\mathbb{Z}$ is zelfs de kleinste ring die $\mathbb{N}$ bevat. Dit is intuïtief duidelijk: ten opzichte van $\mathbb{N}$ zijn in $\mathbb{Z}$ immers alleen maar de inversen voor optelling toegevoegd. Maar wat betekent 'kleinste ring'? We zullen nu een stelling formuleren die dit precies formaliseert.

Uitbreiding van $\mathbb{N}$

Een ring R is een *uitbreiding* van $\mathbb{N}$ als $\mathbb{N} \subset R$ en de optellings- en vermenigvuldigingsstructuur verenigbaar is. Dit laatste betekent dat $0 = 0_R$, $1 = 1_R$ en dat $a +_R b = a + b$ en $a \cdot_R b = ab$ voor alle $a, b \in \mathbb{N}$.

V.2.1 Stelling. Er bestaat een commutatieve ring Z met de volgende eigenschap: voor iedere ring R is er een uniek homomorfisme $f : Z \to R$.

Bovendien geldt:

- Z is uniek op uniek isomorfisme na;
- Z kan zo gekozen worden dat het een uitbreiding van $\mathbb{N}$ is.

Het bewijs stellen we uit tot Paragraaf V.5. Zie ook Opgave V.1.5.

Geheel getal

We noemen een ring als in voorgaande stelling een *ring van gehele getallen*. We kiezen vanaf nu een zo'n ring $\mathbb{Z}$ die een uitbreiding is van $\mathbb{N}$ en omdat deze ring uniek is op uniek isomorfisme na, noemen we hem dé ring van gehele getallen. Zoals opgemerkt in de discussie na Definitie V.1.9 maakt een andere keuze alleen een administratief verschil, het unieke isomorfisme met de eerste keuze is een 'vertaling' tussen de twee keuzen.

V.2.2 Gevolg. i) Voor $a \in \mathbb{Z}$ geldt $a \in \mathbb{N}$ of $-a \in \mathbb{N}$.

ii) Voor iedere ring R die een uitbreiding is van $\mathbb{N}$, is er een injectief homomorfisme $\mathbb{Z} \to R$. (Dit maakt de uitspraak precies dat $\mathbb{Z}$ de kleinste uitbreiding van $\mathbb{N}$ is.)

Bewijs. We laten de details aan de lezer over en beperken ons tot de hoofdlijnen.

(i): Definieer een verzameling X door

$$X = \{a \in \mathbb{Z} : a \in \mathbb{N} \vee (-a) \in \mathbb{N}\}.$$

Deze deelverzameling van $\mathbb{Z}$ bevat 0 en 1 en is gesloten onder optelling en vermenigvuldiging en het nemen van de additieve inverse en vormt daarmee een ring. Volgens Stelling V.2.1 is er dus een homomorfisme $f : \mathbb{Z} \to X$. Stellen we deze samen met de inbedding $X \subset Z$, dan krijgen we een homomorfisme $\mathbb{Z} \to \mathbb{Z}$ van $\mathbb{Z}$ naar $\mathbb{Z}$. Volgens Stelling V.2.1 is zo'n homomorfisme uniek en dus moet de samenstelling de identiteit op $\mathbb{Z}$ zijn; maar dat kan alleen als $X = \mathbb{Z}$ en f de identiteit is.

(ii): Er is een homomorfisme $f : \mathbb{Z} \to R$. Dit homomorfisme is de identiteit op $\mathbb{N}$. Zij $a, b \in \mathbb{Z}$ waarvoor geldt $f(a) = f(b)$. Dan volgt $f(a-b) = 0$ en $f(b-a) = 0$. Omdat $a - b \in \mathbb{N}$ of $b - a \in \mathbb{N}$ volgt $a = b$. ■

De volgende elementaire eigenschap geldt niet voor elke ring (zie Opgave V.1.3). Deze eigenschap (veralgemeniseerd naar $\mathbb{R}$) speelt een belangrijke rol in de schoolwiskunde bij het oplossen van kwadratische vergelijkingen.

V.2.3 Stelling. Zij $a, b \in \mathbb{Z}$. Als $ab = 0$, dan $a = 0$ of $b = 0$.

Bewijs. Als $a, b \in \mathbb{N} \subset \mathbb{Z}$ dan is dit een eigenschap van natuurlijke getallen uit Opgave IV.2.2. Zo niet, dan stellen Gevolg V.2.2 en Stelling V.1.3 ons in staat te reduceren tot dit geval. Als voorbeeld bekijken we de situatie $a \in \mathbb{N}$, maar $b \notin \mathbb{N}$. Dan geldt

$$a \cdot (-b) = -(a \cdot b) = -0 = 0,$$

en omdat $-b \in \mathbb{N}$ volgt $a = 0$ of $b = 0$ (we weten natuurlijk dat het $a = 0$ moet zijn, maar dat is voor het bewijs niet relevant). ■

Ordening op $\mathbb{Z}$

In Hoofdstuk IV is een lineaire ordening $\leq$ op de natuurlijke getallen gedefinieerd. Deze definitie is makkelijk generaliseerbaar naar $n_1, n_2 \in \mathbb{Z}$:

$$n_1 \leq n_2 \quad \Leftrightarrow \quad \text{er is een } m \in \mathbb{N} \text{ met } n_1 + m = n_2.$$

De aldus gedefinieerde relatie $\leq$ geeft $\mathbb{Z}$ de structuur van een geordende ring (zie Opgave V.2.2).

Opgaven

✍ **1.** Een veelgebruikte regel zegt dat als $ab = ac$ met $a \neq 0$, dit impliceert dat $b = c$. Waarschijnlijk is je eerste neiging dit te bewijzen door links en rechts te delen door a. In een lichaam is dat een prima manier, maar met enkel $\mathbb{Z}$ gaat die methode niet op omdat er geen deeloperatie is. Geef een alternatief bewijs (zonder de inbedding $\mathbb{Z} \subset \mathbb{Q}$ te gebruiken).

2. Bewijs dat $(\mathbb{Z}, \leq)$ een geordende ring is. Je mag hierbij aannemen dat de relatie $\leq$ op $\mathbb{N}$ een lineaire ordening is. Als je ambitieus bent, dan kun je ook dat bewijzen.

V.3 Deelbaarheid

In de ring van gehele getallen kun je in het algemeen niet delen. Soms kan het echter wel — ieder even getal is bijvoorbeeld deelbaar door 2. In deze paragraaf bespreken we een aantal elementaire eigenschappen van deelbaarheid van gehele getallen. Deze eigenschappen worden bij het vak "Algebra/Getaltheorie" veel verder uitgediept.

V.3.1 Definitie. Gegeven $a, b \in \mathbb{Z}$. We zeggen dat b een *deler* is van a als er een $x \in \mathbb{Z}$ is zodat $a = bx$. Is b een deler van a, dan zeggen we b *deelt* a, en a *is deelbaar door* b, en a is een *veelvoud* van b; notatie: $b|a$.

Priemgetal

Een *priemgetal* is een natuurlijk getal dat precies vier delers heeft, of equivalent, precies twee positieve delers. Omdat ieder getal deelbaar is door 1 en door zichzelf, kun je het nog anders formuleren: een priemgetal is een geheel getal $p > 1$ met als enige delers ± 1 en $\pm p$.

V.3.2 Stelling. Ieder positief geheel getal is een product van priemgetallen. (We gebruiken hier de conventie dat een 'leeg product' gelijk is aan 1.)

Bewijs. Voor $n = 1$ is de uitspraak wegens de genoemde conventie triviaal. Zij $n \geqslant 2$ en stel dat voor alle gehele getallen $1 \leqslant k < n$ is bewezen dat het een product van priemgetallen is. We gaan bewijzen dat n dan ook een product van priemgetallen is. Met volledige inductie is daarmee de stelling dan bewezen.

Bekijk daartoe de verzameling

$$\{d \in \mathbb{N} : d > 1 \text{ en } d|n\}.$$

Deze verzameling is niet leeg, want n is bijvoorbeeld een element, en vanwege de welordeningsstelling (Stelling IV.2.4) heeft de verzameling dus een kleinste element p. We zullen bewijzen dat p een priemgetal is. Ten eerste geldt $p > 1$. Als p niet priem is, dan zou er een deler d met $1 < d < p$ moeten zijn. Deze d is dan ook een deler van n (zie Opgave V.3.3) die groter is dan 1 en dat kan niet omdat p al het kleinste element is met deze eigenschap.

Omdat $p|n$ bestaat er per definitie een $k \in \mathbb{Z}$ zodat $n = kp$. Er geldt $1 \leqslant k < n$ en dus zegt onze inductiehypothese dat k een product is van priemgetallen. Voegen we aan dit product de extra factor p toe, dan hebben we n dus ook uitgedrukt als product van priemgetallen. ∎

We willen ook graag bewijzen dat het product uit voorgaande stelling *uniek* is. Dat is nog verbazend lastig. We stellen het bewijs uit tot het einde van de paragaaf, omdat het handig is hiervoor theorie over de grootste gemene deler te gebruiken. Wat we al wel kunnen bewijzen, is de volgende stelling die een klassiek voorbeeld is van een bewijs met tegenspraak (zie Hoofdstuk II).

V.3.3 Stelling. (Euclides) Er zijn oneindig veel priemgetallen.

Bewijs. Laat P de verzameling priemgetallen zijn en veronderstel dat P *eindig* is. Definieer het getal

$$n = 1 + \prod_{p \in P} p;$$

hier is de productnotatie gebruikt: het product van alle elementen van P. Uit voorgaande stelling volgt dat n een product is van priemgetallen. Omdat $\prod_{p \in P} p \geqslant 1$, geldt $n > 1$. Dus is er een priemgetal p dat n deelt. Maar dat betekent $p \in P$ en dus $p|(n-1)$. Uit $p|n$ en $p|(n-1)$ volgt dat p ook een deler is van $n-(n-1) = 1$ en dus $p = 1$ (zie hiervoor Opgave V.3.3). Dat is een tegenspraak: 1 is per definitie geen priemgetal. Onze aanname dat de verzameling P eindig is, kan dus niet juist zijn. ∎

Delen met rest

V.3.4 Stelling. Voor alle $a, b \in \mathbb{Z}$ met $b \neq 0$ bestaan er unieke $q, r \in \mathbb{Z}$ waarvoor

$$a = qb + r \qquad \text{en} \qquad 0 \leqslant r < |b|.$$

Het getal r uit deze stelling noemen we de *rest* bij deling van a door b. Merk op dat de rest gelijk is aan 0 precies dan als $b|a$.

Bewijs. Zij $a, b \in \mathbb{Z}$ $(b \neq 0)$ gegeven. Definieer de verzameling

$$A = \{n \in \mathbb{N} \mid \exists_{q \in \mathbb{Z}}\ a = qb + n\}.$$

Dit is een deelverzameling van $\mathbb{N}$ die niet leeg is (zie Opgave V.3.2). Volgens de welordeningsstelling (Stelling IV.2.4) bevat A een kleinste element $r \in A$. Voor dit element geldt dus $0 \leqslant r$ en $a = qb + r$ voor een zekere $q \in \mathbb{Z}$. Bovendien geldt $r < |b|$; immers, als $r \geqslant |b|$ dan is ook $r - |b| \in A$ en dat is in tegenspraak met het geven dat r het kleinste element in A is.

Wat rest is de uniciteit van q en r te bewijzen. Stel daarom dat er ook $q', r' \in \mathbb{Z}$ zijn met $a = q'b + r'$ en $0 \leqslant r' < |b|$. Dan volgt uit $qb + r = q'b + r'$ dat

$$(q - q')b = r' - r.$$

Maar dat betekent dat b een deler is van $r' - r$. Omdat $-|b| < r' - r < |b|$ kan dat alleen als $r' = r$. Maar dan is ook $q = q'$. ∎

Grootste gemene deler

Noteer met D_n de verzameling delers van een geheel getal n. Merk op dat $1 \in D_n$; bovendien geldt voor $n \neq 0$ dat D_n een eindige verzameling is; voor een deler d van n geldt immers $-|n| \leqslant d \leqslant |n|$.

Laat nu twee gehele getallen a en b gegeven zijn. De doorsnede $D_a \cap D_b$ is de verzameling *gemeenschappelijke delers* van a en b. Ze is niet leeg en zolang a en b niet beide gelijk zijn aan 0 is de verzameling eindig en bevat het dus een grootste element. Dit grootste element noemen we de *grootste gemene deler* (ggd, 'gemeen' betekent hier 'gemeenschappelijk'); notatie: $\text{ggd}(a, b)$. We spreken af dat $\text{ggd}(0, 0) = 0$. Als $\text{ggd}(a, b) = 1$ dan noemen we a en b *relatief priem*.

V.3.5 Stelling. Zij $a, b \in \mathbb{Z}$. Er bestaan $m, n \in \mathbb{Z}$ zodat

$$\text{ggd}(a, b) = ma + nb.$$

Bewijs. Als a of b gelijk is aan 0, dan is de uitspraak triviaal; stel dus dat dit niet het geval is. Bekijk de verzameling

$$W = \{z \in \mathbb{N} \mid z \geqslant 1 \text{ en } z = ma + nb \text{ voor zekere } m, n \in \mathbb{Z}\}.$$

Omdat bijvoorbeeld $|a| + |b| \in W$ is $W \neq \varnothing$. Volgens de welordeningsstelling (Stelling IV.2.4) is er dus een kleinste element g in W. Ieder element van W heeft de vorm $am + bn$ en is dus deelbaar door $\text{ggd}(a, b)$. In het bijzonder is dus ook $g \in W$ deelbaar door $\text{ggd}(a, b)$. We zullen nu bewijzen dat omgekeerd $g \mid \text{ggd}(a, b)$; daaruit volgt dan dat g gelijk is aan de grootste gemene deler en daarmee is het bewijs voltooid.

We laten zien dat g een deler is van *ieder* element van W en dus in het bijzonder van $|a|$ en $|b|$; dan is g dus een gemeenschappelijke deler van a en b. Welnu: zij $z \in W$ gegeven. Voer een deling met rest uit: $z = qg + r$ met $0 \leqslant r < g$. Als $r = 0$ dan geldt inderdaad $g \mid z$. Stel dus dat $r \neq 0$. Schrijf $g = ma + nb$ en $z = m'a + n'b$. Dan blijkt uit

$$r = z - qg = m'a + n'b - q(ma + nb) = (m' - qm)a + (n' - qn)b$$

dat r óók een element is van W. Maar dan hebben we een element in W gevonden dat kleiner is dan g en dat kan niet; tegenspraak. Dus $r \neq 0$ zal niet gebeuren. ∎

Algoritme van Euclides

Er is een efficiënte methode om de grootste gemene deler van twee getallen te bepalen, net als de coëfficiënten m en n uit voorgaande stelling: het *euclidische algoritme*. We bespreken dit algoritme aan de hand van een voorbeeld. Het algoritme is gebaseerd op het volgende lemma.

V.3.6 Lemma. Zij $a, b \in \mathbb{N}$ met $a > b > 0$. Zij r de rest van deling van a door b. Dan geldt

$$\text{ggd}(a,b) = \text{ggd}(b,r).$$

Bewijs. Zie Opgave V.3.7. ∎

V.3.7 Voorbeeld. We willen de grootste gemene deler van 2520 en 1100 bepalen. Het euclidisch algoritme gaat als volgt[1]:

$$\begin{array}{rcll}
\text{ggd}(2520,1100) &=& \text{ggd}(1100,320), & \text{want } 2520-2\cdot 1100 = 320; \quad \text{(i)}\\
\text{ggd}(1100,320) &=& \text{ggd}(320,140), & \text{want } 1100-3\cdot 320 = 140; \quad \text{(ii)}\\
\text{ggd}(320,140) &=& \text{ggd}(140,40), & \text{want } 320-2\cdot 140 = 40; \quad \text{(iii)}\\
\text{ggd}(140,40) &=& \text{ggd}(40,20), & \text{want } 140-3\cdot 40 = 20; \quad \text{(iv)}\\
\text{ggd}(40,20) &=& \text{ggd}(20,0), & \text{want } 40-2\cdot 20 = 0; \quad \text{(v)}\\
\text{ggd}(20,0) &=& 20. &
\end{array}$$

We lezen hieruit af dat $\text{ggd}(2520,1100) = \cdots = \text{ggd}(40,20) = 20$.

In de linkerkolom staat de uitleg, rechts staat het feitelijke rekenwerk. Als je enkel het algoritme wilt uitvoeren en de uitleg wel gelooft, dan is het korter om alleen de vergelijkingen aan de rechterkant op te schrijven. Zie hier het patroon:

$$\begin{array}{rl}
\text{(i)} & 2520 - 2\cdot 1100 = 320\\
\text{(ii)} & 1100 - 3\cdot 320 = 140\\
\text{(iii)} & 320 - 2\cdot 140 = 40\\
\text{(iv)} & 140 - 3\cdot 40 = \boxed{20}\\
& 40 - 2\cdot 20 = 0
\end{array}$$

Omdat op de laatste regel de uitkomst 0 is, is de uitkomst één regel daarboven de ggd.

De rekenpartij uit het vorige voorbeeld levert meer op dan alleen de ggd. Loop dezelfde berekening nog eens door, maar nu van onder naar boven beginnend bij (iv).

$$\begin{array}{rr}
\text{(iv) is:} & 140-3\cdot 40 = 20\\
\text{gebruimakend van (iii):} & 140-3\cdot(320-2\cdot 140) = 20\\
& 7\cdot 140-3\cdot 320 = 20\\
\text{gebruimakend van (ii):} & 7\cdot(1100-3\cdot 320)-3\cdot 320 = 20\\
& 7\cdot 1100-24\cdot 320 = 20\\
\text{gebruikmakend van (i):} & 7\cdot 1100-24\cdot(2520-2\cdot 1100) = 20\\
& 55\cdot 1100-24\cdot 2520 = 20
\end{array}$$

Dit heet ook wel het *uitgebreide euclidische algoritme*. Het is een methode om de ggd van twee getallen te schrijven als lineaire combinatie, zoals in Stelling V.3.5. —∎

Unieke priemfactorisatie

Tot slot komen we terug op de uniciteit van de priemfactorisatie. We hebben inmiddels de technieken ontwikkeld om het volgende cruciale lemma te bewijzen.

V.3.8 Lemma. (Gauss) Zij $a, b \in \mathbb{Z}$ en zij p een priemgetal. Als $p|ab$, dan $p|a$ of $p|b$.

Bewijs. Stel $p|ab$ terwijl $p\not|a$. Omdat p een priemgetal is en $p\not|a$, geldt $\text{ggd}(p,a) = 1$. Volgens Stelling V.3.5 zijn er dan $m, n \in \mathbb{Z}$ zodat

$$mp + na = 1.$$

[1] Zie ook een uitwerking op YouTube: `http://youtu.be/7Es4j-0Gf_I` en `http://youtu.be/sEZQwLBEo48`.

Als we links en rechts met b vermenigvuldigen, krijgen we

$$mpb + nab = b.$$

Maar uit $p|ab$ volgt het bestaan van een getal t zodat $ab = tp$. Substitutie geeft

$$mpb + ntp = b$$

en vervolgens kunnen we aan de linkerkant p buiten haakjes halen:

$$p(mb + nt) = b;$$

maar uit deze laatste vergelijking volgt $p|b$. ■

V.3.9 Stelling. (Hoofdstelling van de rekenkunde) Voor ieder positief geheel getal n bestaan er een **unieke** rij priemgetallen $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$ $(r \in \mathbb{N})$ zodat

$$n = p_1 p_2 \ldots p_r.$$

Bewijs. Existentie is Stelling V.3.2. We bewijzen uniciteit met behulp van inductie. Voor $n = 1$ is dit triviaal: een leeg product is natuurlijk uniek en zodra een product van priemgetallen niet leeg is, is het groter dan 1. Stel nu dat voor alle k met $1 \leqslant k < n$ is bewezen dat de priemfactorisatie van k uniek is. Laat

$$n = p_1 p_2 \ldots p_r \qquad \text{met } p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r \text{ alle priem;}$$

$$n = q_1 q_2 \ldots q_s \qquad \text{met } q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s \text{ alle priem.}$$

Uit het voorgaande lemma volgt $p_1|q_1$ (en dus $p_1 = q_1$) of $p_1|q_2 \ldots q_s$. In het tweede geval volgt $q_2 \ldots q_s = p_1 \cdot k = p_1 \cdot k_1 \ldots k_t$, waarbij $k_1 \ldots k_t$ een priemfactorisatie van k is. Omdat volgens de inductiehypothese de priemfactorisatie van $q_2 \ldots q_s$ uniek is, volgt $p_1 = q_j$ voor zekere j met $2 \leqslant j \leqslant s$.

De conclusie is dus dat p_1 ook in de rij $q_1, q_2, \ldots, q_s$ voorkomt. Delen we deze factor weg, dan houden we twee priemfactorisaties van n/p_1 over die volgens de inductiehypothese identiek zijn. Maar dan zijn de oorspronkelijke factorisaties dus ook identiek. ■

V.3.10 Voorbeeld. De priemontbinding van 2520 is

$$2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 = 2^3 \cdot 3^2 \cdot 5 \cdot 7;$$

en die van 1100:

$$1100 = 2^2 \cdot 5^2 \cdot 11.$$

We lezen hieruit af dat de grootste gemene deler gelijk is aan $2^2 \cdot 5 = 20$, zoals we al hadden gezien. Het euclidische algoritme biedt echter een *efficiënte* manier om de ggd te bepalen, terwijl voor het vinden van de priemontbinding er in het algemeen geen snelle methode bestaat. Dit vormt de grondslag van de beveiliging van elektronisch bankieren, logins op websites, enzovoorts. Meer hierover vind je in het vak “Algebra/Getaltheorie”. ■

Opgaven

1. (a) Laat zien dat de relatie | (“is deler van”) géén lineaire ordeningsrelatie is.

(b) Laat zien dat het ook geen equivalentierelatie is.

2. (a) Bewijs dat de verzameling A uit het bewijs van Stelling V.3.4 niet leeg is.

(b) Waar wordt in het bewijs van de stelling (het gaat niet alleen over het gedeelte uit vraag a) gebruikt dat $b \neq 0$?

✍ **3.** Bewijs of weerleg:

(a) $\forall_{a\in\mathbb{Z}}\ -a|a$

(b) $\forall_{a,b\in\mathbb{Z}}\ a|b \implies a|-b$

(c) $\forall_{a,b\in\mathbb{Z}}\ a|b \implies -a|b$

(d) $\forall_{a\in\mathbb{Z}}\ a|0$

(e) $\exists_{a\in\mathbb{Z}}\ a|0$

(f) $\forall_{a\in\mathbb{Z}}\ 0|a$

(g) $\exists_{a\in\mathbb{Z}}\ 0|a$

(h) $\forall_{a\in\mathbb{Z}}\ a|1$

(i) $\forall_{a\in\mathbb{Z}}\ 1|a$

(j) $\forall_{a,b,c\in\mathbb{Z}}\ (a|b \wedge b|c) \implies a|c$

(k) $\forall_{a,b\in\mathbb{Z}}\ (a|b \wedge b|a) \implies a = b$

(l) $\forall_{a,b,c\in\mathbb{Z}}\ a|b \implies a|(bc)$

(m) $\forall_{a,b,c\in\mathbb{Z}}\ a|b \implies a|(b+c)$

(n) $\forall_{a,b,c\in\mathbb{Z}}\ (a|b \wedge a|c) \implies a|(bc)$

(o) $\forall_{a,b,c\in\mathbb{Z}}\ (a|b \wedge a|c) \implies a|(b+c)$

(p) $\forall_{a,b\in\mathbb{Z}}\ a|b \implies -|b| \leqslant a \leqslant |b|$

(q) $\forall_{a,b,c\in\mathbb{Z}}\ a|(bc) \implies (a|b \vee a|c)$

(r) $\forall_{a,b,c\in\mathbb{Z}}\ a|(b+c) \implies (a|b \vee a|c)$

✍ **4.** We gebruiken de notatie D_n voor de verzameling delers van n. Beargumenteer steeds per uitspraak of deze waar is:

(a) $-1 \in D_a$ voor alle $a \in \mathbb{Z}$.

(b) Er is een $a \in \mathbb{Z}$ waarvoor geldt dat $0 \in D_a$.

(c) $D_p \cap D_q = \{-1, 1\}$ als p en q priemgetallen zijn.

(d) Als $a|b$, dan $D_a \subset D_b$.

(Het is een goede oefening om een paar van de uitspraken uit Opgave V.3.3 te vertalen in de D_n-notatie.)

5. Bepaal steeds met behulp van het euclidische algoritme één paar gehele getallen m, n dat voldoet aan de gegeven vergelijking.

(a) $341n + 259m = 1$

(b) $503m + 401n = 1$

(c) $2849m + 791n = \text{ggd}(2849, 791)$

(d) $689m + 403n = 39$

6. Zij $a, b, c \in \mathbb{Z}$. We zijn geïnteresseerd in de oplossingen van de vergelijking

$$ax + by = c,$$

waarbij x en y gehele getallen zijn. (Dit is een voorbeeld van een *diophantische vergelijking*.)

(a) Onderzoek onder welke voorwaarde op a, b en c er een oplossing $(x, y) \in \mathbb{Z}^2$ is.

(b) Stel $(x_0, y_0) \in \mathbb{Z}^2$ is een oplossing, wat zijn dan *alle* oplossingen?

✍ **7.** Bewijs Lemma V.3.6.

8. De hoofdstelling (Stelling V.3.9) wordt ook wel eens als volgt geformuleerd. Noteer met $\mathscr{P}$ de verzameling priemgetallen. Voor ieder geheel getal $n \neq 0$ bestaat er een unieke functie $e : \mathscr{P} \to \mathbb{N}$ waarvoor geldt dat $e^{-1}(\mathbb{N} \setminus \{0\})$ eindig is en

$$n = \pm \prod_{p \in \mathscr{P}} p^{e(p)}.$$

Doorgrond deze formulering en leg uit waarom het equivalent is aan de hoofdstelling. Waarom wordt eindigheid geëist?

✍ **9.** Alle positieve delers van het getal 54 vind je terug in een vermenigvuldigingstabel:

×	3^0	3^1	3^2	3^3
2^0	1	3	9	27
2^1	2	6	18	54

(a) Leg uit waarom elke positieve deler van 54 in deze tabel moet staan.

(b) Maak een vergelijkbare tabel om alle positieve delers van 200 te bepalen.

(c) Hoeveel positieve delers heeft 19800?

(d) Bepaal het kleinste natuurlijke getal met precies 105 delers.

(e) Bepaal alle getallen tussen 0 en 200 die precies tien delers hebben.

✍ **10.**

(a) Bewijs dat alle priemgetallen in de ontbinding van een kwadraat een even aantal keer voorkomen.

(b) Algemener: hoe zit het met een n-de macht?

11. De rij van Fibonacci is een getallenrij. Je begint met tweemaal een 1 op te schrijven, en daarna bereken je elk volgend getal uit de rij als de som van zijn twee voorgangers. De rij begint dus als volgt:

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

Bewijs met volledige inductie dat twee opeenvolgende getallen in deze rij altijd ggd gelijk aan 1 hebben.

✍ **12.** Bereken de ggd van $3^{100} + 2^{100}$ en $3^{100} - 2^{100}$.

✍ **13.** In het tijdschrift *Pythagoras* staat een methode om de grootste gemeenschappelijke deler van meer dan twee getallen uit te rekenen. De methode wordt beschreven aan de hand van een voorbeeld:
Gevraagd: Bereken de ggd van 72–54–24–12 (de getallen zijn in volgorde van grootte gezet).
De verschillen zijn resp. 18–30–12.
We plaatsen nu de gevonden verschillen in de rij van de oorspronkelijke getallen, waarbij we de getallen maar eenmaal opschrijven:
72–54–30–24–18–12.
De verschillen zijn nu resp. 18–24–6–6–6. Het getal 6 is er dus nog bijgekomen. Dit geeft de rij
72–54–30–24–18–12–6.
Hiervan is de rij van verschillen 18–24–6–6–6–6.
Er komen nu geen nieuwe getallen meer bij. De ggd is dus 6.

Verklaar deze methode.

✍ **14.** In de film *Die Hard with a Vegeance* moeten de hoofdrolspelers Bruce Willis en Samuel L. Jackson een bom onschadelijk maken door op een weegschaal 4 gallon water te plaatsen. Helaas beschikken ze enkel over flessen van 3 en 5 gallon en een onuitputtelijk waterreservoir. Hoe lossen onze helden dit op? En wat heeft het met de theorie van dit hoofdstuk te maken?

✍ **15.**

(a) Formuleer zelf een definitie van '*kleinste gemene veelvoud*'.

(b) Waarom is de 'kleinste gemene deler' geen nuttig begrip?

(c) Waarom is het 'grootste gemene veelvoud' een onzinnig concept?

(d) Wat kun je zeggen over het product van de ggd en het kgv?

V.4 Het lichaam van rationale getallen

Uitbreiding van $\mathbb{Z}$

Een lichaam F heet een *uitbreiding* van $\mathbb{Z}$ als $\mathbb{Z} \subset F$ en als de corresponderende inbedding $\mathbb{Z} \to F$ een homomorfisme is.

V.4.1 Stelling. Er bestaat een lichaam Q met de volgende eigenschap: voor ieder lichaam F dat een uitbreiding is van $\mathbb{Z}$ is er een uniek homomorfisme $f : Q \to F$.
Bovendien geldt:

- Q is uniek op uniek isomorfisme na;
- Q kan zo gekozen worden dat het een uitbreiding van $\mathbb{Z}$ is.

Rationaal getal

Ook het bewijs van deze stelling stellen we uit tot Paragraaf V.5; zie Opgave V.5.3, maar ook Opgave V.1.6. Net als bij $\mathbb{Z}$ kiezen we één uitbreiding $\mathbb{Q}$ van $\mathbb{Z}$ als in de stelling die we *hét lichaam van rationale getallen* noemen.

V.4.2 Gevolg. i) Voor $a \in \mathbb{Q}$ zijn er $b \in \mathbb{Z}$ en $c \in \mathbb{Z} \setminus \{0\}$ zodat $a = \frac{b}{c}$.
ii) Het homomorfisme f uit de vorige stelling in injectief. (Dit maakt de uitspraak precies dat $\mathbb{Q}$ de kleinste uitbreiding van $\mathbb{Z}$ is.)

Bewijs. Onderdeel (i) wordt bewezen op eenzelfde manier als in Gevolg V.2.2. Onderdeel (ii) volgt uit een algemenere uitspraak: als een homomorfisme $f : F \to R$ van een lichaam naar een ring niet injectief is, dan geldt $0_R = 1_R$ (en dan $R = \{0\}$). Stel immers dat $f(a) = f(b)$, terwijl $a \neq b$. Dan geldt ook $f(a-b) = f(a) - f(b) = 0$ en omdat $a - b \neq 0$ kunnen we de inverse gebruiken:

$$1_R = f(1) = f((a-b)(a-b)^{-1}) = f(a-b)f((a-b)^{-1}) = 0_R.$$

■

Gedegenereerd

Onderdeel (i) van het gevolg zegt dat ieder rationaal getal te schrijven is als een breuk (het omgekeerde geldt natuurlijk ook). We verwijzen naar Stelling V.1.6 voor de rekenregels voor breuken. Merk in ieder geval op dat de breukvorm *gedegenereerd* is: ieder rationaal getal is op meerdere manieren te schrijven als een breuk.

Ordening op $\mathbb{Q}$

De lineaire ordening $\leq$ op $\mathbb{Z}$ laat zich uitbreiden tot een lineaire ordening op $\mathbb{Q}$ (zie Opgave V.4.3). Hiermee wordt $\mathbb{Q}$ een geordend lichaam.

Archimedische eigenschap

V.4.3 Stelling. (Archimedes/Eudoxus) Zij $a, b \in \mathbb{Q}_+$. Dan is er een $n \in \mathbb{N}$ zodat $a \leqslant nb$.

Opgaven

1. Bewijs dat er voor ieder rationaal getal $a \in \mathbb{Q}$ er unieke $b \in \mathbb{Z}$ en $c \in \mathbb{Z}_+$ zijn, zodat $\gcd(b,c) = 1$ en $a = \frac{b}{c}$.

2. We borduren voort op de notatie in Opgave V.3.8. Bewijs dat er voor ieder rationaal getal $a \neq 0$ een unieke functie $e\colon \mathscr{P} \to \mathbb{Z}$ bestaat waarvoor geldt dat $e^{-1}(\mathbb{Z} \setminus \{0\})$ eindig is en

$$a = \pm \prod_{p \in \mathscr{P}} p^{e(p)}.$$

3. In deze opgave gaan we de lineaire ordening $\leqslant$ op $\mathbb{Z}$ uitbreiden naar $\mathbb{Q}$. Laat $\frac{a}{c}$ en $\frac{b}{d}$ breuken zijn met c en d positief. Definieer

$$\frac{a}{c} \leqslant \frac{b}{d} \qquad \Longleftrightarrow \qquad ad \leqslant bc,$$

waarbij links de te defniëren ordening van rationale getallen en rechts de reeds gedefinieerde ordening in $\mathbb{Z}$ wordt gebruikt.

(a) Bewijs dat dit een goede definitie is van een relatie op $\mathbb{Q}$; met andere woorden: laat zien dat het niet afhangt van de gekozen breukrepresentatie van een rationaal getal.

(b) Bewijs dat $\mathbb{Q}$ een geordend lichaam is.

4. Het woord 'infinitesimaal' ben je waarschijnlijk wel eens in een natuurkundeboek of calculuscursus tegengekomen. Leg uit waarom de archimedische eigenschap van $\mathbb{Q}$ ook wel eens als volgt wordt geformuleerd: "er bestaan geen infinitesimale rationale getallen."

V.5 Constructie

Zoals beloofd, zullen we in deze paragraaf vanuit de natuurlijke getallen de gehele getallen en van daaruit (in een opgave) de rationale getallen construeren. Dit is een illustratie van de eerder gedane uitspraak dat heel de wiskunde kan worden opgebouwd uit verzamelingen (oftewel de ZFC-axioma's). Daarbij maken we gebruik van equivalentieklassen, een concept dat is ingevoerd in Hoofdstuk III.

V.5.1 Opmerking. Laten we eerst een intuïtief beeld geven van wat we gaan doen. We beginnen met de verzameling natuurlijke getallen en willen hier graag de verzameling gehele getallen mee definiëren. Nu zijn er, althans intuïtief, voor ieder natuurlijk getal $n \neq 0$ twee gehele getallen n en $-n$. Het ligt voor de hand om als definitie te kiezen

$$\mathbb{Z} = \mathbb{N} \cup \{-n : n \in \mathbb{N}\}.$$

Toch zijn er twee redenen waarom dit niet de handigste oplossing is. Ten eerste is '$-n$' een element dat we, *a priori* aan de definitie van $\mathbb{Z}$, nog niet kennen: in welke verzameling hoort het thuis? Hoewel het technisch niet zo ingewikkeld is dit met een trucje op te lossen, is er een belangrijker bezwaar: het is nogal een gedoe om de rekenoperaties op $\mathbb{Z}$ te definiëren en vervolgens eigenschappen te bewijzen, omdat we steeds een gevalsonderscheiding moeten maken tussen positieve en negatieve getallen. Er blijkt gelukkig een elegantere methode te zijn en hiervoor doen we inspiratie op uit de constructie van $\mathbb{Q}$ uit $\mathbb{Z}$, die we daarom nu eerst (nog steeds intuïtief) zullen bespreken.

We denken over $\mathbb{Q}$ als een verzameling breuken

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a \in \mathbb{Z} \wedge b \in \mathbb{Z} \setminus \{0\} \right\}.$$

Hier geldt nog steeds het eerste bezwaar van het onbekende element, maar dat lossen we op door $\frac{a}{b}$ te schrijven als een geordend paar $(a,b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Als we dat doen, dan moeten we ons wel realiseren dat de breuknotatie niet uniek is. Dat betekent dat we een *equivalentierelatie* moeten introduceren; de beoogde gelijkheid

$$\frac{a}{c} = \frac{b}{d} \qquad \Longleftrightarrow \qquad ad = bc$$

vormt de inspiratie voor de equivalentierelatie

$$(a,c) \sim (b,d) \qquad \Longleftrightarrow \qquad ad = bc.$$

Nu kunnen we $\mathbb{Q}$ *definiëren* als verzameling van equivalentieklassen:

$$\mathbb{Q} = \big(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\big)/\!\sim.$$

Dit lost het eerste bezwaar op. Het tweede bezwaar gaat niet op als we op $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ operaties optellen en vermenigvuldigen kunnen definiëren die compatibel zijn met $\sim$. We kunnen dan immers Stelling III.2.5 toepassen en krijgen operaties op $\mathbb{Q}$ 'cadeau'. Dit blijkt mogelijk, waarbij we ons in de definitie van de operaties natuurlijk laten inspireren door de rekenregels die in $\mathbb{Q}$ zouden moeten gelden.

Na deze excursie naar $\mathbb{Q}$ keren we weer terug naar de constructie van $\mathbb{Z}$. Ook hier kunnen we geordende paren gebruiken. We denken dan over $(a,b) \in \mathbb{N} \times \mathbb{N}$ na als het gehele getal '$a-b$'. De uitdaging is nu om een equivalentierelatie en operaties optellen en vermenigvuldigen op $\mathbb{N}\times\mathbb{N}$ te vinden. Dat gaan we nu formeel doen.

Constructie $\mathbb{Z}$

We definiëren twee operaties op $\mathbb{N} \times \mathbb{N}$:

$$(a,c) + (b,d) = (a+b, c+d)$$

en

$$(a,c) \cdot (b,d) = (ab+cd, ad+bc).$$

Voorts definiëren we een relatie op $\mathbb{N} \times \mathbb{N}$ door

$$(a,c) \sim (b,d) \qquad \Longleftrightarrow \qquad a+d = b+c.$$

V.5.2 Stelling. Beschouw voorgaande operaties en relatie op $\mathbb{N} \times \mathbb{N}$.

i) De operaties zijn beide associatief en commutatief. Voorts is $(0,0)$ een neutraal element voor optelling en is $(1,0)$ een neutraal element voor vermenigvuldiging.
ii) De relatie $\sim$ is een equivalentierelatie.
iii) Beide operaties zijn compatibel met $\sim$.

Bewijs. Dit vereist geen creatieve ideeën: gewoon de definities controleren aan de hand van een hoop zorgvuldig uitgevoerde algebra. Zie Opgave V.5.2. ■

V.5.3 Gevolg. De quotiëntverzameling $Z = (\mathbb{N} \times \mathbb{N})/\!\sim$ met de geïnduceerde operaties $+$ en $\cdot$ is een commutatieve ring.

Bewijs. Associativiteit en commutativiteit van optelling en vermenigvuldiging en het bestaan van eenheden voor deze operaties zijn directe gevolgen van voorgaande stelling in combinatie met Stelling III.2.5. Distributiviteit kun je controleren door definities te ontrafelen; dat gebeurt in Opgave V.5.5. Wat rest is te bewijzen dat ieder element $[(a,b)]$ een inverse heeft voor optelling. Dat is het element $[(b,a)]$; immers:

$$(a,b) + (b,a) = (a+b, b+a) \sim (0,0)$$

en dus geldt $[(a,b)] + [(b,a)] = [(0,0)]$. ■

We kunnen nu bewijzen dat Z een ring van gehele getallen is:

Bewijs. (van Stelling V.2.1) Zij R een ring en Z als in het bovenstaande gevolg. We laten in de equivalentieklassenotatie $[(a,b)]$ voor het gemak de binnenste haakjes voortaan weg.

Bekijk de canonieke functie $C\colon \mathbb{N} \to R$ gegeven door $C(n) = n1_R$ (zie Opgave V.1.5). Definieer een afbeelding $F\colon \mathbb{N}\times\mathbb{N} \to R$ door

$$F(a,c) = C(a) - C(c).$$

Als $(a,c) \sim (b,d)$, dan geldt $a+d = b+c$ en dus ook $C(a)+C(d) = C(b)+C(c)$, waaruit volgt $C(a-c) = C(b-d)$. De conclusie is dat F equivalente elementen op hetzelfde element afbeeldt. Er is dus een welgedefinieerde afbeelding $f : Z \to R$ gegeven door $f([a,c]) = F(a,c)$.

We moeten nu nagaan dat f een homomorfisme is. Dat is rechttoe-rechtaan:

- $f([a,c]+[b,d]) = f([a+b,c+d]) = C(a+b) - C(c+d)$
  $= C(a) - C(c) + C(b) - C(d) = f([a,c]) + f([b,d])$.
- $f([a,c]\cdot[b,d]) = f([ab+cd, ad+cb]) = C(ab+cd) - C(ad+cb)$
  $= C(a)C(b) + C(c)C(d) - C(a)C(d) - C(c)C(b) = (C(a)-C(c))\cdot(C(b)-C(d))$
  $= f([a,c])\cdot f([b,d])$.
- $f([1,0]) = C(1) - C(0) = C(1) = 1_R$.

Uniciteit van f bewijzen we als volgt. Stel dat $g\colon Z \to R$ óók een homomorfisme is. Omdat $f([1,0]) = 1_R = g([1,0])$ heeft ook ieder veelvoud van $[1,0]$ hetzelfde beeld. Omdat $[0,a] = -[a,0]$ en $g(-x) = -g(x)$ geldt hetzelfde voor ieder element van de vorm $[0,a]$. Maar ieder element uit Z heeft een representant van de vorm $(0,a)$ of $(a,0)$ en dus geldt $f = g$.

Nu bewijzen we dat Z uniek is op uniek isomorfisme na. Dit is een formaliteit: stel maar dat Z' óók een commutatieve ring is waarvoor geldt dat er voor iedere ring R een uniek homomorfisme $Z' \to R$ is. Dan zijn er in het bijzonder unieke homomorfismes $f\colon Z \to Z'$ en $g\colon Z' \to Z$. Samenstelling geeft een homomorfisme $g\circ f : Z \to Z$. Er is echter nóg een homomorfisme $Z \to Z$, namelijk de identiteit id_Z. Omdat een homomorfisme $Z \to Z$ uniek is, moet gelden $g\circ f = \mathrm{id}_Z$. Op dezelfde manier volgt $f\circ g = \mathrm{id}_{Z'}$. Dus is f een isomorfisme.

Tot slot willen we[2] een ring $\mathbb{Z}$ die isomorf is met Z, maar ook een uitbreiding is van $\mathbb{N}$. Vervang daartoe ieder element in Z van de vorm $[a,0]$ door $a \in \mathbb{N}$ en pas ook in de rekenoperaties deze 'vertaling' toe[3]. ∎

Opgaven

1. (a) Leg uit dat de equivalentierelatie $\sim$ op $\mathbb{N}\times\mathbb{N}$ inderdaad past bij de beoogde interpretatie van (a,b) als $a-b \in \mathbb{Z}$.

(b) Controleer ook dat de operaties optellen en vermenigvuldigen op $\mathbb{N}\times\mathbb{N}$ passen bij de beoogde interpretatie.

[2] Deze 'wens' leidt, zoals je hier ziet, tot een lelijk argument. Daarom zijn er ook wiskundigen die $\mathbb{N} \to \mathbb{Z}$ helemaal niet als een inclusie willen zien — en idem voor $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$. Dat wijkt wel veel af van intuïtie en schoolpraktijk. Anderzijds: in computerimplementaties van getallen is er ook geen sprake van injecties: natuurlijke getallen worden anders gerepresenteerd dan gehele, en die weer anders dan 'floating point'. Bovendien: we zijn in de wiskunde alleen geïnteresseerd in de structuur van getalssystemen en niet in specifieke constructies, dus eigenlijk zou je niet over 'de ring' van gehele getallen maar over 'een ring' moeten praten en dan is het weglaten van inclusies noodzakelijk geworden.

[3] Er is hier een vervelend technisch detail, namelijk dat we wel zeker moeten weten dat $\mathbb{N}$ en Z disjunct zijn. Voor een concrete constructie van $\mathbb{N}$, zoals in de appendix, kun je dat expliciet nagaan: de elementen van $\mathbb{N}$ zijn in onze constructie eindige verzamelingen en de elementen van Z zijn oneindig. Een alternatief is om het regulariteitsaxioma te gebruiken en ieder element $a \in Z$ eerst te vervangen door $(\mathbb{N}, a)$. We laten de details hier achterwege.

✍ **2.** Bewijs Stelling V.5.2.

3. In deze paragraaf is gedetailleerd beschreven hoe $\mathbb{Z}$ kan worden geconstrueerd uit $\mathbb{N}$. Ook is in de opmerking een globaal programma beschreven hoe $\mathbb{Q}$ kan worden geconstrueerd uit $\mathbb{Z}$. Voer dit programma in detail uit.

4. Voor negatieve getallen gebruiken we niet de notatie $a - c$, maar schrijven we gewoon $-d$. Het voordeel van deze laatste notatie is dat deze niet gedegeneerd is. De breuknotatie $\frac{a}{c}$ voor rationale getallen is daarentegen wél gedegeneerd. Is er hier niet ook een alternatieve, niet gedegeneerde notatie? En waarom gebruiken we die niet gewoon?

✍ **5.** Bewijs dat vermenigvuldigen distributief is over optellen in $\mathbb{N}\times\mathbb{N}/\sim$ (zie het bewijs van Gevolg V.5.3).

V.6 Lichaamsuitbreidingen

Het lichaam $\mathbb{Q}$ van rationale getallen is nog een vrij beperkt getalssysteem. We zagen in Hoofdstuk II al dat veel wortels (Voorbeeld II.3.4, Opgave II.3.2) en logartimen (Opgave II.3.3) niet rationaal zijn; en we zullen in het volgende hoofdstuk zien dat ook veel limieten in $\mathbb{Q}$ niet bestaan. Om die reden zullen we in het volgende hoofdstuk de reële getallen $\mathbb{R}$ en zelfs de complexe getallen $\mathbb{C}$ bestuderen. Er is echter een andere klasse van lichamen F, die uitbreidingen zijn van $\mathbb{Q}$ maar bevat zijn in $\mathbb{C}$, die nog passen in de context van dit specifieke hoofdstuk: de *algebraïsche uitbreidingen*.

V.6.1 Opmerking. De theorie in deze paragraaf behandelen we wat globaler dan hiervoor — met veel doorverwijzingen naar literatuur. We concentreren ons op algebraïsche eigenschappen die voor de schoolwiskunde relevant zijn. Voor details, generalisaties en met name voor veel rijkere theorie verwijzen we naar een algebraboek of naar de cursus “Algebra/Getaltheorie”.

Zij $K \subseteq F$ met K en F lichamen. Als de inbedding $K \to F$, $x \mapsto x$ een homomorfisme is, dan noemen we K een *deellichaam* van F en, omgekeerd, F een *lichaamsuitbreiding* van K.

Polynoom

Zij K een lichaam. We noteren met $K[X]$ de verzameling[4] *polynomen met coëfficiënten in* K. Deze verzameling bestaat dus uit de polynomen

$$f(X) = \sum_{i\in\mathbb{N}} f_i X^i, \qquad \text{waarin } f_i \in K \text{ en } f_i = 0 \text{ voor alle } i \text{ op eindig veel na.}$$

Twee polynomen zijn gelijk als alle coëfficiënten met dezelfde index gelijk zijn. De *graad* van een polynoom is de hoogste index i waarvoor $f_i \neq 0$; voor het nulpolynoom is de graad niet gedefinieerd. Twee polynomen kun je zoals gebruikelijk optellen en vermenigvuldigen en met deze operaties vormt $K[X]$ een commutatieve ring.

In de ring van polynomen $K[X]$ kun je naar analogie van de ring van gehele getallen een aantal concepten introduceren, waarvan we er hier twee noemen:

- Een polynoom $g(X)$ is een *deler* van een polynoom $f(X)$ als er een polynoom $h(X)$ bestaat zodat $f(X) = g(X)\cdot h(X)$.
- Een polynoom $f(X)$ van positieve graad is *irreducibel* als er geen polynomen van positieve graad $g(X)$ en $h(X)$ bestaan zodat $f(X) = g(X)\cdot h(X)$.

[4] Voor een verzamelingstheoretische constructie van zo'n verzameling, uitgaande van de ZFC-axioma's, verwijzen we naar een algebraboek.

Is nu $f(X)$ een element van $K[X]$, dan kunnen we een equivalentierelatie definiëren door

$$g(X) \sim h(X) \qquad \Longleftrightarrow \qquad f(X) \text{ is een deler van } (g(X) - h(X)).$$

We noteren de ring van equivalentieklassen onder deze equivalentierelatie met $K[X]/(f(X))$. Als $f(X)$ graad $\geqslant 1$ heeft, dan is de natuurlijke afbeelding $K \to K[X]/f(X)$ injectief en kunnen we K beschouwen als deelring van $K[X]/(f(X))$. Kern van deze paragraaf is de volgende stelling.

V.6.2 Stelling. Zij K een lichaam en zij $f(X) \in K[X]$ een irreducibel polynoom van graad $n \geqslant 1$. Dan is $K[X]/f(X)$ een lichaamuitbreiding van K. Ieder element van $K[X]/(f(X))$ heeft een unieke representant van de vorm

$$a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} \qquad (a_i \in K \text{ voor } 0 \leqslant i < n).$$

Het bewijs van deze stelling is niet ingewikkeld, maar wel wat werk. In plaats van een bewijs geven we enig vertrouwen en inzicht in de stelling aan de hand van enkele voorbeelden.

V.6.3 Voorbeelden. Bekijk het polynoom $f(x) = x^2 - 2$ in $\mathbb{Q}[X]$. Dit polynoom is irreducibel in $\mathbb{Q}[X]$. Noteer $F = \mathbb{Q}[X]/(f(X))$. Voor de equivalentieklasse $[X] \in F$ geldt $[X]\cdot[X] = [X^2] = [2]$ en daarom noteren we die equivalentieklasse met $\sqrt{2}$. De stelling zegt dat F een lichaam is en dat ieder element van F van de vorm $a + b\sqrt{2}$ is, met $a, b \in \mathbb{Q}$. We maken dit aannemelijk met een paar berekeningen:

- optellen en aftrekken behoudt de vorm: $(a+b\sqrt{2}) \pm (c+d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2}$;
- idem voor vermenigvuldiging: $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$;
- delen vereist een trucje:

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}.$$

In de literatuur wordt F vaak genoteerd met $\mathbb{Q}(\sqrt{2})$. De notatie '$\sqrt{2}$' is hier enigszins onvoorzichtig gekozen. Er zijn namelijk twee inbeddingen $\mathbb{Q}(\sqrt{2}) \subset \mathbb{C}$: de een beeldt $[X]$ af op $\sqrt{2}$, de ander op $-\sqrt{2}$. Eenzelfde opmerking geldt voor de volgende voorbeelden.

Bekijk het irreducibele polynoom $g(x) = x^2 + 1$ in $\mathbb{R}[X]$ en noteer $\mathbb{R}(i) = \mathbb{R}[X]/(f(X))$. Omdat voor de equivalentieklasse $[X]$ geldt $[X]^2 = -1$, noteren we deze met i. Elementen van $\mathbb{R}(i)$ hebben de vorm $a + bi$ met $a, b \in \mathbb{R}$. Uitwerking van de rekenoperaties, analoog aan hiervoor, geeft de bekende rekenregels voor complexe getallen - zie Opgave V.6.1.

Hetzelfde polynoom, $g(x) = x^2 + 1$, is ook een element van $\mathbb{Q}[X]$. Dit leidt tot een lichaam $\mathbb{Q}(i)$ met elementen van de vorm $a + bi$ met $a, b \in \mathbb{Q}$.

Omgekeerd is $f(x) = x^2 - 2$ natuurlijk ook een element van $\mathbb{R}[X]$, maar in deze ring is $f(X)$ niet irreducibel. Je kunt dus niet 'nog een wortel uit 2' aan $\mathbb{R}$ toevoegen.

Het polynoom $g(x) = x^2 + 1$ is ook irreducibel in $\mathbb{Q}(\sqrt{2})[X]$. Dat leidt tot een lichaam dat een uitbreiding is van $\mathbb{Q}(\sqrt{2})$ en dat genoteerd wordt met $\mathbb{Q}(\sqrt{2}, i)$. Elementen hebben de vorm $a + b\sqrt{2} + ci + di\sqrt{2}$ met $a, b, c, d \in \mathbb{Q}$.

Algebraïsche uitbreiding

V.6.4 Definitie. Zij F een lichaamsuitbreiding van K. Een element $x \in F$ heet *algebraïsch over* K als x een nulpunt is van een polynoom $f(X) \neq 0$ met coëfficiënten in K. Als ieder element $x \in F$ algebraïsch over K is, dan heet F een *algebraïsche uitbreiding* van K. Een lichaamsuitbreiding die niet algebraïsch is, heet *transcendent*.

Je kunt bewijzen dat ieder lichaam $K[X]/(f(X))$ als in Stelling V.6.2 een algebraïsche uitbreiding van K is.

V.6.5 Voorbeeld. Het element $\sqrt{2} \in \mathbb{R}$ is algebraïsch over $\mathbb{Q}$, omdat het een nulpunt is van bijvoorbeeld het polynoom $f(X) = x^2 - 2$. De elementen π, e en $\log_2 3$ in $\mathbb{R}$ zijn niet algebraïsch over $\mathbb{Q}$, al is het bewijs daarvan best ingewikkeld. Dat betekent dat $\mathbb{R}$ *geen* algebraïsche uitbreiding is van $\mathbb{Q}$. (We zullen hieronder nog een argument geven hiervoor.) Een element $x \in \mathbb{C}$ dat algebraïsch is over $\mathbb{Q}$, noem je een *algebraïsch getal*. ∎

Algebraïsch gesloten

V.6.6 Definitie. Een lichaam K heet *algebraïsch gesloten* als K geen algebraïsche lichaamsuitbreidingen heeft ongelijk aan K zelf.

Uit Stelling V.6.2 volgt:

V.6.7 Stelling. In een algebraïsch gesloten lichaam K is ieder polynoom in $K[X]$ van graad $\geqslant 1$ een product van polynomen in $K[X]$ van graad 1. Gevolg is dat ieder polynoom van graad $\geqslant 1$ een nulpunt heeft in K.

V.6.8 Voorbeelden. Het lichaam $\mathbb{C}$ is algebraïsch gesloten, zoals we in het volgende hoofdstuk zullen zien. Deze eigenschap heet (om historische redenen) de *hoofdstelling van de algebra*.

Je kunt bewijzen dat ieder lichaam een uitbreiding heeft die algebraïsch gesloten is. Voor $\mathbb{Q}$ is $\mathbb{C}$ hier een voorbeeld van. Maar er geldt een sterker resultaat: ieder lichaam heeft een *algebraïsche* uitbreiding die algebraïsch gesloten is. Voor $\mathbb{Q}$ noteren we dit lichaam met $\overline{\mathbb{Q}}$; het bestaat uit alle algebraïsche getallen in $\mathbb{C}$. Omdat de verzameling polynomen met rationale coëfficiënten aftelbaar (Hoofdstuk I) is, is $\overline{\mathbb{Q}}$ ook aftelbaar. Dit is nog een argument waarom $\mathbb{R}$ en $\mathbb{C}$ geen algebraïsche uitbreiding zijn van $\mathbb{Q}$: deze verzamelingen zijn immers overaftelbaar.

Opgaven

1. (a) Werk de rekenregels voor elementen uit $\mathbb{R}(i)$ uit zoals in Voorbeeld V.6.3.
(b) Doe hetzelfde voor $\mathbb{Q}(\sqrt{2}, i)$.
(c) Doe hetzelfde voor $\mathbb{Q}[X]/(X^3 - 2)$.
(d) Doe hetzelfde voor $\mathbb{Q}[X]/(X^2 + 3X + 1)$.

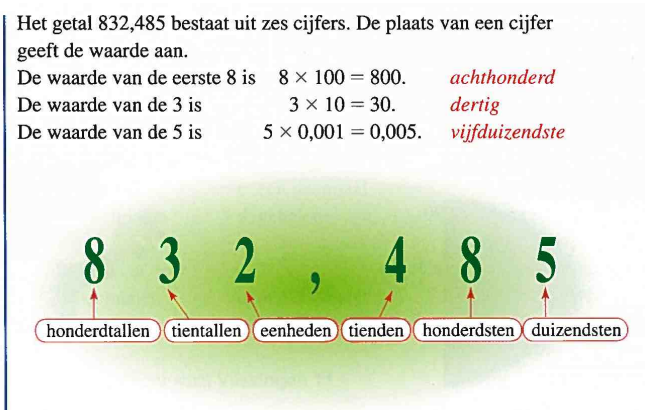
2. Bewijs of weerleg:
(a) $i \in \mathbb{C}$ is algebraïsch over $\mathbb{R}$;
(b) $i \in \mathbb{C}$ is algebraïsch over $\mathbb{Q}$;
(c) $\mathbb{C}$ is een algebraïsche uitbreiding van $\mathbb{R}$;
(d) $\mathbb{C}$ is een algebraïsche uitbreiding van $\mathbb{Q}$.

VI REËLE EN COMPLEXE GETALLEN, RIJEN EN FUNCTIES

Het programma dat we in de vorige twee hoofdstukken hebben ingezet om de bekende getalsystemen axiomatisch te beschrijven en te construeren, zetten we in dit hoofdstuk voort. Nu zijn de getalsystemen van reële en complexe getallen aan de beurt. De reële getallen modelleren de complete getallenlijn, waar in het bijzonder geen 'gaten' in zitten zoals bij $\mathbb{Q}$ het geval is. We zullen deze vage omschrijving op meerdere manieren precies maken: in de eerste paragraaf met de notie van supremum en in de daaropvolgende paragrafen met behulp van verschillende convergentiecriteria. We treden hier uit het domein van de algebra en betreden het domein van de analyse.

Als intermezzo's staan we stil bij de kommanotatie voor reële getallen en gaan we in op continuïteit van functies. Na al het werk dat we in de reële getallen zullen stoppen, zal blijken dat de complexe getallen als een eenvoudig 'toegift' verschijnen. We hebben een groot deel van het voorwerk al in het voorgaande hoofdstuk gedaan!

VI.0.9 Voorbeeld. In de schoolwiskunde wordt veel gebruikt gemaakt van de decimale kommanotatie — zoals in Figuur 6.1. Sommige getallen kun je in decimale



Figuur 6.1 – De introductie van de kommanotatie in *Getal & ruimte* (vwo 2).

kommanotatie schrijven, zoals $\frac{1}{2} = \frac{5}{10} = 0{,}5$ en $\frac{7}{5} = \frac{14}{10} = 1{,}4$. Bij de meeste getallen lukt dat echter niet. We kunnen alleen een 'beginnetje' opschrijven:

$$\tfrac{1}{6} = 0{,}166666666666666666666666666666666666666666666666666666\ldots$$
$$\pi = 3{,}14159265358979323846264338327950288419716939937510582\ldots$$

De puntjes aan de rechterkant geven aan dat we nog niet klaar zijn—en dat zal ook nooit gebeuren, hoe groot het papier ook is. Wat hier staat is slechts het begin

van de *decimale ontwikkeling* van $\frac{1}{6}$ en π. Natuurlijk weten we bij $\frac{1}{6}$ wel hoe de decimale ontwikkeling verder gaat. In de decimale ontwikkeling van π valt geen enkele regelmaat te herkennen (al is dat niet heel eenvoudig te bewijzen).

Rekenen met decimale ontwikkelingen is lastig. Volgens de elementaire rekenalgoritmes kun je twee getallen optellen of vermenigvuldigen door ze onder elkaar te schrijven en van rechts naar links de cijfers af te werken. Maar in decimale ontwikkelingen is er geen rechts!

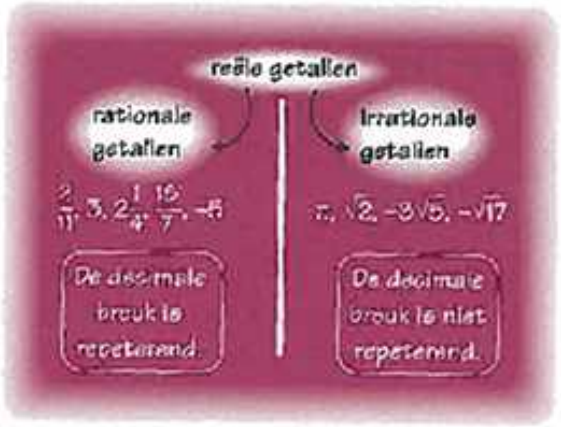
Een ander vervelend technisch detail is dat de decimale ontwikkeling niet altijd uniek is. Zo geldt bijvoorbeeld $1 = 0{,}\overline{9}$, waarbij de streepjesnotatie per definitie staat voor $0{,}99999999\ldots$. Wat zou $1 - 0{,}\overline{9}$ anders moeten zijn dan nul? Dat is niet alleen gevoelsmatig vervelend, maar het maakt ook dat je moet uitkijken hoe je je uitdrukt. Zo staat in *Getal & ruimte* (vwo 1, maar andere schoolboeken bevatten soortgelijke uitspraken) bijvoorbeeld:

> **Bij het afronden op twee decimalen kijk je naar de derde decimaal.**
> **Derde decimaal 5 of meer? Rond af naar boven.**
> **Derde decimaal minder dan 5? Rond af naar beneden.**

Deze regel geeft niet altijd een uniek antwoord!

Een laatste nadeel van de notatie is dat het geen *instrinsieke* beschrijving van reële getallen geeft. De *basis*, in dit geval de cijfers nul tot en met negen, lijken immers een bijzondere rol te spelen. Je kunt je afvragen of het gebruik van een ander talstelsel, bijvoorbeeld het binaire, tot andere getalstypen zou leiden. Dat is niet zo — maar dat is niet meteen duidelijk. (En pas je een kleine perspectiefwisseling toe die leidt to zogenaamde p-adische getallen, dan maakt de basiskeuze wel degelijk uit.) ∎

VI.0.10 Voorbeeld. Reële getallen komen in de schoolwiskunde veel voor, zowel in de onderbouw bij bijvoorbeeld wortels als in de bovenbouw bij logaritmen, continuïteit, et cetera. Bij Wiskunde D op vwo (en soms ook op havo) kiezen veel docenten ervoor complexe getallen te behandelen. ∎



Figuur 6.2 – Verschillende soorten reële getallen, als beschreven in *Getal & ruimte* (vwo 2).

VI.1 Supremum

In Voorbeeld VI.0.9 is gemotiveerd dat de decimale kommanotatie niet de mooiste manier is om het getalssystemen van reële getallen te definiëren. We kiezen hier

voor een andere benadering, die gebaseerd is op de intuïtie dat de reële getallen gemodelleerd worden door de getallenlijn en dat (anders dan bij bijvoorbeeld $\mathbb{Q}$) er geen 'gaten' zijn. Het volgende voorbeeld maakt deze intuïtie wat concreter en is bovendien een opstapje naar de definitie van supremum hieronder.

VI.1.1 Voorbeeld. Bekijk de verzameling van alle rationale getallen met de eigenschap dat ze negatief zijn of dat hun kwadraat niet groter dan 2 is:

$$A = \{x \in \mathbb{Q} : x < 0\} \cup \{x \in \mathbb{Q} : x \geqslant 0 \text{ en } x^2 \leqslant 2\}.$$

Blijkbaar is elk rationaal getal $q < \sqrt{2}$ een element van A en het is ook niet moeilijk in te zien dat geen getal groter dan $\sqrt{2}$ element van A is. Het getal $\sqrt{2}$ markeert de overgang van A naar zijn complement $\mathbb{Q} \setminus A$: alle elementen van A liggen op de reële rechte *links* van $\sqrt{2}$, en alle elementen van $\mathbb{Q} \setminus A$ bevinden zich *rechts* van $\sqrt{2}$. Het 'grensgetal' $\sqrt{2}$ is echter *géén* rationaal getal — zie Voorbeeld II.3.4. We zouden kunnen zeggen dat de verzameling $\mathbb{Q}$ 'gaten' bevat. ∎

We hebben in Paragraaf III.2 gedefinieerd wat een *lineaire ordening* $\leqslant$ op een verzameling R is.

VI.1.2 Definitie. Zij $(R, \leqslant)$ een verzameling met een lineaire ordening en zij $A \subseteq R$ een deelverzameling.

1. A is *naar boven begrensd* (voor de relatie $\leqslant$) als er een $x \in R$ is zodat $a \leqslant x$ voor alle $a \in A$. Het element x heet een *bovengrens* van A.
2. Een element $x \in R$ is een *supremum* van A als x de kleinste bovengrens is. Dat wil zeggen:
   - x is een bovengrens van A, en
   - als y een bovengrens is van A, dan is $x \leqslant y$;
3. Een supremum x van A is een *maximum* als $x \in A$.

Op analoge wijze kunnen de begrippen *naar onder begrensd*, *ondergrens* en *infimum* worden gedefinieerd, maar die hebben we in dit hoofdstuk niet nodig.

Begrensd, supremum

Als een supremum van een verzameling A bestaat, dan is deze uniek en noteren we het met $\sup(A)$. Immers, stel x en y zijn beide suprema van A. Dan zijn x en y beide bovengrenzen van A en ook geldt $x \leqslant y$ en $y \leqslant x$; dus $x = y$.

VI.1.3 Voorbeeld. De verzameling $A \subset \mathbb{Q}$ uit Voorbeeld VI.1.1 is naar boven begrensd (voor de gebruikelijke ordening op $\mathbb{Q}$): 3 is bijvoorbeeld een bovengrens, omdat

$$x < 0 \implies x \leqslant 3 \qquad \text{en} \qquad x \geqslant 0 \text{ en } x^2 \leqslant 2 \implies x \leqslant 3.$$

Als deelverzameling van $\mathbb{Q}$ heeft A echter geen supremum. Stel immers dat $y \in \mathbb{Q}$ een supremum is. We weten al (Voorbeeld II.3.4) dat $y^2 \neq 2$; dus $y^2 < 2$ of $y^2 > 2$. We laten zien dat $y^2 > 2$ tot een tegenspraak leidt; het geval $y^2 < 2$ gaat analoog en is Opgave VI.1.2. Definieer daartoe $\epsilon = y^2 - 2$ en $y' = y - \frac{\epsilon}{2y}$. Dan geldt

$$(y')^2 - 2 = y^2 - \epsilon + \frac{\epsilon^2}{4y^2} - 2 = \frac{\epsilon^2}{4y^2} > 0$$

en bovendien

$$0 < y' < y,$$

waarbij we hebben gebruikt $\epsilon, y > 0$ en $2y^2 > \epsilon$, hetgeen je met een grove schatting kunt aantonen. De conclusie is dat y' óók een bovengrens is van A, die bovendien kleiner is dan het supremum y — tegenspraak. ∎

VI.1.4 Voorbeeld. Bekijk het interval $(1,2)$ in $\mathbb{R}$. Dit interval is naar boven begrensd. Een bovengrens is bijvoorbeeld 2, maar 3, π en 5213 zijn dat net zo goed. Een van deze bovengrenzen is de kleinste: 2 is het supremum van $(1,2)$.

Merk op dat $2 \notin (1,2)$. Dat is anders bij het interval $A = (1,2]$. Het getal 2 is ook een supremum van dit interval, maar bovendien geldt $\sup(A) \in A$; het is dus een maximum. ∎

Kanonieke inbedding

Zij $(R, \leqslant)$ een geordend lichaam. Uit Opgave V.1.6 volgt dat er een uniek injectief homomorfisme $\mathbb{Q} \to R$ is. We herhalen voor het gemak de definitie en verwijzen voor details naar de genoemde opgave. Begin, via recursie, met een afbeelding $i : \mathbb{N} \to R$ die $n \in \mathbb{N}$ afbeeldt op de som $1_R + 1_R + \cdots + 1_R$ (n termen). Breid deze afbeelding uit naar $\mathbb{Z}$ door $-n$ te sturen naar de inverse van $i(n)$ in R. Breid hem vervolgens uit naar $\mathbb{Q}$ door $\frac{a}{b}$ te sturen naar $i(a)i(b)^{-1}$. In deze laatste stap moet je natuurlijk wel twee dingen controleren: (1) dat de definitie niet afhangt van de keuze van teller en noemer (de breuknotatie is immers gedegenereerd) — dat is eenvoudig na te gaan; (2) dat $i(b) \neq 0$ — hier gebruik je dat R geordend is en dat daarom $i(1 + \cdots + 1) > 0$.

We zullen vanaf nu voor het gemak aannemen dat $\mathbb{Q} \subseteq R$. Merk op dat de ordeningen in $\mathbb{Q}$ en R compatibel zijn.

VI.1.5 Stelling. Zij R een geordend lichaam waarin iedere niet lege naar boven begrensde deelverzameling een supremum heeft. Dan geldt:

R is archimedisch

i) R is archimedisch (ter herinnering: dat wil zeggen dat voor alle $a, b \in R_{>0}$ er een $n \in \mathbb{N}$ is zodat $na > b$).

$\mathbb{Q}$ ligt dicht

ii) Tussen ieder tweetal $a, b \in R$ met $a < b$ is er een $c \in \mathbb{Q}$ zodat $a < c < b$.

Bewijs. (i) Zij

$$A = \{a \in R : a > 0 \wedge \forall_{n \in \mathbb{N}}\, an \leqslant 1\}.$$

We gaan bewijzen dat A leeg is en daaruit volgt eenvoudig de archimedische eigenschap.

Stel daarom $A \neq \varnothing$. Omdat A naar boven begrensd is, bijvoorbeeld door 1, is er een supremum $x = \sup(A)$. We doen nu twee observaties:

- $2x \notin A$ omdat $x < 2x$ en x de kleinste bovengrens is. Dus is er een $N \in \mathbb{N}$ zodat $2xN > 1$.
- $\frac{1}{2}x \in A$. Immers: als dat niet zo is, dan is er een $m \in \mathbb{N}$ met $\frac{1}{2}xm > 1$; omdat $\frac{1}{2}x < x$ en x de kleinste bovengrens is, is er een $a \in A$ met $\frac{1}{2}x < a \leqslant x$; maar dan volgt $am > 1$ en dat is een tegenspraak. Dus voor alle $n \in \mathbb{N}$ geldt $\frac{1}{2}xn \leqslant 1$.

Substitueren we in de laatste ongelijkheid $n = 4N$, dan krijgen we $2xN \leqslant 1$, in tegenspraak met $2xN > 1$.

(ii) We kunnen aannemen dat $0 \leqslant a < b$, want als a en b beide niet positief zijn voldoet $-c$ voor een $c \in \mathbb{Q}$ waarvoor geldt $|a| < c < |b|$ en als $a < 0$ en $b > 0$ dan voldoet $c = 0$.

Volgens de archimedische eigenschap (onderdeel i) is er een $n \in \mathbb{N}$ zodat $n > \frac{1}{b-a}$. Bekijk de verzameling

$$B = \{x \in \mathbb{N} : a < \frac{x}{n}\}.$$

Deze verzameling is niet leeg en heeft dus een kleinste element $t \in \mathbb{N}$. Voor dit element geldt per definitie $\frac{t-1}{n} \leqslant a < \frac{t}{n}$. We zijn klaar als we kunnen bewijzen dat $\frac{t}{n} < b$. Dat gaat als volgt:

$$\frac{t}{n} \leqslant a + \frac{1}{n} < a + (b - a) = b.$$

∎

VI.1.6 Definitie. Een *dedekindsnede* is een deelverzameling $A \subset \mathbb{Q}$ waarvoor geldt:

- $A \neq \varnothing$ en $A \neq \mathbb{Q}$;
- voor alle $a \in A$ en $b \in \mathbb{Q} \setminus A$ geldt $a < b$;
- A heeft geen maximum.

dedekind-snede

Merk op dat A naar boven begrensd is (ieder element van $\mathbb{Q} \setminus A$ is een bovengrens en $\mathbb{Q} \setminus A$ is niet leeg).

VI.1.7 Stelling. Zij D de verzameling dedekindsneden en zij R een geordend lichaam waarin iedere naar boven begrensde deelverzameling een supremum heeft. De afbeelding

$$D \to R \qquad A \mapsto \sup(A)$$

is bijectief.

Bewijs. Noteer met f de afbeelding $D \to R$. We beschouwen $\mathbb{Q}$ als deelverzameling van R; in het bijzonder is daarmee iedere dedekindsnede een deelverzameling van R. We zullen nu een inverse $g : R \to D$ definiëren door $r \in R$ te sturen naar

$$A = \mathbb{Q} \cap \{x \in R : x < r\}.$$

Merk eerst op dat A inderdaad een dedekindsnede is. Alleen de eis dat A geen maximum heeft, behoeft toelichting: stel dat er wél een maximum $s \in A$ is. Dan geldt $s < r$ en volgens Stelling VI.1.5 is er dus een $t \in \mathbb{Q}$ zodat $s < t < r$. Maar dan ook $t \in A$; tegenspraak.

In Opgave VI.1.4 ga je bewijzen dat g ook echt een inverse van f is. ■

VI.1.8 Voorbeelden. De verzameling $B = \{x \in \mathbb{Q} : x < \frac{1}{2}\}$ is een dedekindsnede die we volgens bovenstaande afbeelding $D \to \mathbb{R}$ associëren met het element $\frac{1}{2}$. Er is nóg een linker deel van de rationale getallenlijn met supremum $\frac{1}{2}$, namelijk $C = \{x \in \mathbb{Q} : x \leqslant \frac{1}{2}\}$ — om te zorgen dat er in voorgaande stelling sprake is van een bijectie, is de eis van het ontbreken van een maximum in de definitie van dedekindsnede opgenomen; C is géén dedekindsnede.

De verzameling A uit Voorbeeld VI.1.3 is een dedekindsnede. We associëren deze met het element $\sqrt{2} \in \mathbb{R}$.

reële getallen definitie!

De vorige stelling suggereert nu een methode om het lichaam van reële getallen te *definiëren*: het is de verzameling van dedekindsneden D. Daartoe moet D nog wel worden voorzien van een optelling en vermenigvuldiging. Dat kan op een voor de hand liggende manier (Opgave VI.1.3) en die manier geeft bovendien dat de bijectie uit voorgaande stelling een isomorfisme is. Dit leidt tot het volgende gevolg.

VI.1.9 Gevolg. Er bestaat een geordend lichaam waarin iedere naar boven begrensde deelverzameling een supremum heeft. Dit lichaam is uniek, op een uniek isomorfisme na.

Vanwege de uniciteit spreken we over *hét lichaam van reële getallen*, hetgeen we noteren met $\mathbb{R}$.

Opgaven

1. Definieer, naar analogie met de definitie van supremum, de notie van een *infimum* van een deelverzameling van een geordende verzameling.

2. Leidt in Voorbeeld VI.1.3 uit $y^2 < 2$ een tegenspraak af.

3. Zij D de verzameling dedekindsneden.

(a) Laat zien dat voor $A, B \in D$

$$A + B = \{x \in \mathbb{Q} : \exists_{a \in A, b \in B}\ x = a + b\}$$

een operatie op D definieert die commutatief en associatief is en waarvoor er een identiteit en bij ieder element een inverse is.

(b) Definieer zelf een vermenigvuldiging. Houd er daarbij rekening mee dat het product van twee negatieve getallen positief is!

(c) Laat zien dat D met de voorgaande twee operaties een lichaam is.

(d) Laat ten slotte zien dat de afbeelding uit Stelling VI.1.7 een homomorfisme van lichamen is. (Hint: gebruik Stelling VI.1.5.)

✍ **4.** Bewijs dat de afbeelding g uit het bewijs van Stelling VI.1.7 inderdaad een inverse is van f. Je moet dus laten zien dat $f \circ g = \mathrm{id}_R$ en $g \circ f = \mathrm{id}_D$.

VI.2 Rijen

VI.2.1 Definitie. Zij A een verzameling. Een *rij* in A is een functie $a : \mathbb{N} \to A$. In plaats van $a(n)$ schrijven we meestal a_n en in plaats van $a : \mathbb{N} \to A$ schrijven we vaak $(a_n)_{n \geqslant 0}$ of $(a_n)_{n \in \mathbb{N}}$. De getallen a_n heten de *termen* van $(a_n)_{n \geqslant 0}$. Als $A = \mathbb{R}$ dan noemen we zo'n rij ook wel een *reële rij*.

Rijen van reële getallen

In dit verband noemen we $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ de *indexverzameling* van de rij. Het is soms handiger om een andere indexverzameling te gebruiken, bijvoorbeeld $\{1, 2, 3, \ldots\}$; in dat geval noteren we de rij als $(a_n)_{n \geqslant 1}$.

Vaak is de rij door een expliciete formule voor de n-de term gegeven, zoals $a_n = 1/n$, $b_n = 2^{-n}$, $c_n = \sin n$ enzovoort. Deze rijen kunnen we dan noteren als $(1/n)_{n \geqslant 1}$, $(2^{-n})_{n \geqslant 0}$ en $(\sin n)_{n \geqslant 0}$. Minder formeel kunnen we een rij geven door een aantal termen uit te schrijven (indien de formule voor a_n duidelijk is); bijvoorbeeld: met $1, 1/3, 1/5, 1/7, \ldots$ bedoelen we de rij $(1/(2n+1))_{n \geqslant 0}$.

Convergentie, limiet

VI.2.2 Definitie. Een reële rij $(a_n)_{n \geqslant 0}$ heet *convergent* wanneer er een $a \in \mathbb{R}$ bestaat met de volgende eigenschap: voor iedere $\varepsilon \in \mathbb{R}$ met $\varepsilon > 0$ bestaat een $N \in \mathbb{N}$ zodanig dat

$$\text{voor alle } n \geq N : \quad |a_n - a| < \varepsilon.$$

We noemen a een *limiet* van de rij $(a_n)_{n \geqslant 0}$. Notatie:

$$\lim_{n \to \infty} a_n = a.$$

Een rij die niet convergent is heet *divergent*.

VI.2.3 Voorbeeld.

De rij $(1/n)_{n \geqslant 1}$

(a) We zullen aan de hand van bovenstaande definitie laten zien dat de rij $(1/n)_{n \geqslant 1}$ convergent is met limiet 0. Laat $\varepsilon > 0$. Uit de Archimedische eigenschap van $\mathbb{R}$ volgt het bestaan van een $N \in \mathbb{N}$ met $N \geqslant 1$ en $1/N < \varepsilon$. Dan geldt voor alle $n \geq N$:

$$\left| \frac{1}{n} - 0 \right| = \frac{1}{n} \leqslant \frac{1}{N} < \varepsilon.$$

(b) Constante rijen zijn convergent, zie Opgave VI.2.6.

(c) De rij $((-1)^n)_{n\geq 0}$ is divergent want geen enkel getal a voldoet aan de eisen uit Definitie VI.2.2. Neem maar eens aan dat er wel zo'n a was en neem $\varepsilon = 1/2$. Laat $N \in \mathbb{N}$ zó dat $\left|(-1)^n - a\right| < 1/2$ voor alle $n \geqslant N$. Neem een even $n > N$, dan volgt dat $\left|1-a\right| < 1/2$, Neem een oneven $n > N$, dan volgt dat $\left|-1-a\right| < 1/2$. Maar dat kan niet want hier zou uit volgen dat

$$2 = \left|(1-a)-(-1-a)\right| \leq |1-a|+|-1-a| < 1.$$

We gebruiken hier de *driehoeksongelijkheid* die zegt dat voor alle $a, b \in \mathbb{R}$ geldt $|a+b| \leqslant |a|+|b|$ (en dus ook $|a-b| \leqslant |a|+|b|$ — waarom?). In Paragraaf VI.4 komen we hier in grotere algemeenheid op terug.

■

VI.2.4 Opmerking. Een reële rij $(a_n)_{n\geqslant 0}$ kan maximaal één limiet hebben. Stel maar eens dat $\lim\limits_{n\to\infty} a_n = a$ en $\lim\limits_{n\to\infty} a_n = b$ met $a \neq b$. Dan geldt $|a-b| > 0$. We leiden een tegenspraak af. Kies $\varepsilon = \frac{1}{2}|a-b|$. Uit $\lim\limits_{n\to\infty} a_n = a$ volgt dat er een $N_1 \in \mathbb{N}$ bestaat zó dat voor alle $n \geq N_1$ geldt $|a_n - a| < \varepsilon$. Uit $\lim\limits_{n\to\infty} a_n = b$ volgt dat er een $N_2 \in \mathbb{N}$ bestaat zó dat voor alle $n \geq N_2$ geldt $|a_n - b| < \varepsilon$. Kies een $n \geq \max\{N_1, N_2\}$. Dan geldt dat

$$|a-b| = |(a-a_n)+(a_n-b)| \leq |a-a_n|+|a_n-b| < \varepsilon+\varepsilon = |a-b|.$$

Ofwel $|a-b| < |a-b|$ en dat is onzin.

VI.2.5 Definitie. Zij $(x_n)_{n\geqslant 0}$ een reële rij. We zeggen dat $(x_n)_{n\geqslant 0}$ een *begrensde rij* is als een reëel getal $M \geq 0$ bestaat zó dat voor elke $n \in \mathbb{N}$ geldt $|x_n| \leqslant M$.

Analoog definiëren we naar boven en naar beneden begrensdheid.
Het volgende hulpresultaat is vaak handig.

VI.2.6 Propositie. Iedere convergente rij in $\mathbb{R}$ is begrensd.

Bewijs. Zij $(x_n)_{n\geqslant 0}$ een convergente rij in $\mathbb{R}$ met limiet x. We moeten laten zien dat er een $M \geq 0$ bestaat met $|x_n| \leqslant M$ voor alle $n \geqslant 0$. Kies een $N \in \mathbb{N}$ zodanig dat $|x_n - x| < 1$ voor alle $n \geqslant N$. Zij $m = \max\{|x_k| : k = 0, \ldots, N-1\}$ en $M = \max\{m, |x|+1\}$. Het is duidelijk dat $|x_n| \leqslant m \leqslant M$ voor alle $0 \leqslant n \leqslant N-1$. Voor $n \geqslant N$ geldt

$$|x_n| = \left|x+(x_n-x)\right| \leqslant |x|+|x_n-x| \leqslant |x|+1 \leqslant M.$$

■

VI.2.7 Voorbeeld. Beschouw de rij $(a_n)_{n\geq 0}$ gedefinieerd door $a_n = 2n$. De rij is niet begrensd en dus divergent. Om in te zien dat $(a_n)_{n\geqslant 0}$ niet begrensd is, laat $M \geq 0$ willekeurig. Kies $n \in \mathbb{N}$ zó dat $n > M/2$. Dan geldt $|a_n| = 2n > M$. ■

Het is handig om ook een notatie in te voeren die beschrijft in welke zin een rij zoals $(2n)_{n\geq 0}$ divergeert.

VI.2.8 Definitie. We zeggen dat een rij $(x_n)_{n\geqslant 0}$ in $\mathbb{R}$ *naar* ∞ *divergeert*, notatie:

$$\lim_{n\to\infty} x_n = \infty,$$

als er voor iedere $\xi \in \mathbb{R}$ een $N \in \mathbb{N}$ bestaat zodanig dat voor alle $n \geq N$: $x_n \geqslant \xi$.

Divergentie naar $-\infty$ wordt analoog gedefinieerd.
Het is wel gevaarlijk om te rekenen met divergentie naar ∞ en $-\infty$. Bedenk goed dat ∞ en $-\infty$ alleen symbolen zijn. Het zijn dus *geen* getallen.

VI.2.9 Voorbeeld. (a) Zij $a_n = 2n$ met $n \geq 0$. Laat $\xi \in \mathbb{R}$. Volgens de Archimedische eigenschap is er een $N \in \mathbb{N}$ met $N \geqslant \xi$. Voor alle $n \geqslant N$ geldt dan $2n \geqslant 2N \geqslant N \geqslant \xi$. We hebben bewezen dat $\lim_{n\to\infty} 2n = \infty$.

(b) Zij $a_n = n$, $b_n = -n$ en $c_n = -n+1$ met $n \geq 0$. Dan is $\lim_{n\to\infty} a_n = \infty$, $\lim_{n\to\infty} b_n = -\infty$ en $\lim_{n\to\infty} c_n = -\infty$. Verder geldt dat de rij $(a_n + b_n)_{n\geq 0}$ is convergent met limiet 0. De rij $(a_n + c_n)_{n\geq 0}$ is convergent met limiet 1.

(c) Zij $a_n = n$, en $b_n = -n + (-1)^n$ met $n \geq 0$. Dan geldt $\lim_{n\to\infty} a_n = \infty$ en $\lim_{n\to\infty} b_n = -\infty$ $(a_n + b_n)_{n\geq 0}$ is divergent. Immers $a_n + b_n = (-1)^n$.

Blijkbaar kun je dus beter niet rekenen met ∞. ∎

Monotone-convergentie

We hebben gezien (Propositie VI.2.6) dat iedere convergente rij begrensd is. We zullen nu een criterium geven waaronder een begrensde rij convergeert.

VI.2.10 Definitie. Een rij $(x_n)_{n\geqslant 0}$ in $\mathbb{R}$ heet *stijgend* als $x_0 \leqslant x_1 \leqslant x_2 \leqslant \cdots$. Een rij heet *dalend* als $x_0 \geqslant x_1 \geqslant x_2 \geqslant \cdots$.

VI.2.11 Stelling (Monotoneconvergentiestelling)**.** Zij $(x_n)_{n\geq 0}$ een stijgende en begrensde rij in $\mathbb{R}$. Dan geldt: $(x_n)_{n\in\mathbb{N}}$ is convergent en de limiet van deze rij is het supremum van de verzameling $V = \{x_n : n \in \mathbb{N}\}$.

Evenzo geldt dat een dalende en begrensde rij convergent is.

Bewijs. Vanwege de aannames is V niet-leeg en naar boven begrensd. Wegens Gevolg VI.1.9 bestaat het supremum $x = \sup V$. Laat $\varepsilon > 0$. Omdat $x - \varepsilon$ geen bovengrens voor V is, bestaat een $v \in V$ met $x - \varepsilon < v$. Er geldt $v = x_N$ voor een zekere $N \in \mathbb{N}$. Voor alle $n \geqslant N$ geldt dan $x - \varepsilon < x_N \leqslant x_n \leqslant x$, waarbij we gebruiken dat de rij stijgt en dat x een bovengrens is. Uit deze ongelijkheden volgt dat

$$|x_n - x| = x - x_n < \varepsilon \quad \text{voor alle } n \geqslant N.$$

Voor het tweede deel van de stelling bekijken we een begrensde, dalende rij $(y_n)_{n\geqslant 0}$. We kunnen nu het voorgaande toepassen op de rij $(-y_n)_{n\geqslant 0}$, die begrensd en stijgend is. ∎

Opgaven

1. Schrijf een paar termen van $(a_n)_{n\geqslant 0}$ op om een mogelijke limiet a af te leiden. Probeer vervolgens in elk geval hieronder een natuurlijk getal N te vinden zó dat $|a_n - a| < 1/2$ voor alle $n \geq N$, als gegeven wordt

(a) $a_n = \dfrac{1}{2n+1}$;

(b) $a_n = \dfrac{n}{n+1}$;

(c) $a_n = \dfrac{(-1)^n}{n+1}$;

2. Beschouw dezelfde rijen als in de voorafgaande opgave.

(a) Vind voor elke $\varepsilon \in \{10^{-1}, 10^{-2}, 10^{-3}\}$ een $N \in \mathbb{N}$ zó dat voor alle $n \geq N$: $|a_n - a| < \varepsilon$.

✍ (b) Herzie indien nodig je keuze van a, en bewijs dat elke rij naar de gevonden waarde a convergeert.

3. (a) Definieer de rij $(a_n)_{n\geq 0}$ door $a_n = \frac{1}{\sqrt{n+1}}$. Toon met behulp van de definitie aan dat $\lim_{n\to\infty} a_n = 0$.

(b) Definieer de rij $(a_n)_{n\geq 0}$ door $a_n = \sqrt{n}$. Toon met behulp van de definitie aan dat $\lim_{n\to\infty} a_n = \infty$.

4. Beschouw de rij $(a_n)_{n\geqslant 0}$, waarbij $a_n = (4^n + 5^n)/(2^n + 3^n)$ voor elke $n \in \mathbb{N}$.

(a) Vind een $N \in \mathbb{N}$ zó dat voor alle $n \geqslant N$ geldt $a_n > 1000$.

(b) Bewijs dat $\lim_{n\to\infty} a_n = \infty$.

✍ **5.** Beschouw $(a_n)_{n\geqslant 0}$ gedefinieerd voor elke $n \in \mathbb{N}$ als volgt: $a_{2n} = 2^{-n}$ en $a_{2n+1} = 0$. Bewijs met behulp van Definitie VI.2.2 dat de rij convergent is of laat zien dat de rij divergent is.

6. Bewijs dat een constante rij in $\mathbb{R}$ convergent is.

7. Wat kan men zeggen over een rij $(a_n)_{n\geqslant 0}$ als gegeven is dat de rij convergent is en elke a_n een geheel getal is? Vind eerst een paar voorbeelden.

8. Toon aan:

(a) Voor alle $k \in \mathbb{N}$ met $k \geq 1$ geldt $\lim_{n\to\infty} 1/n^k = 0$.

(b) Voor alle $n \geq 2$ geldt $\lim_{k\to\infty} 1/n^k = 0$.

✍ **9.** Van een reële rij $a_0, a_1, a_2, \ldots$ is gegeven

$$a_0 = 0 \quad \text{en voor } n \in \mathbb{N} \quad a_n + a_{n+1} = 2n - 1.$$

Vind en bewijs een algemene formule voor a_n.

✍ **10.** Zij $(x_n)_{n\geqslant 0}$ een convergente rij in $\mathbb{R}$ met limiet x. Laat a en b in $\mathbb{R}$ met $a \leqslant b$.

(a) Toon aan: als $a \leqslant x_n \leqslant b$ voor alle n, dan geldt ook $a \leqslant x \leqslant b$.

(b) Geef een voorbeeld waaruit blijkt dat de volgende bewering niet juist is: als $a < x_n < b$ voor alle n, dan geldt ook $a < x < b$.

✍ **11.** Zij $(x_n)_{n\geqslant 0}$ een rij zó dat $(x_{2n})_{n\geq 0}$ en $(x_{2n+1})_{n\geq 0}$ convergeren naar dezelfde limiet x. Toon aan dat $(x_n)_{n\geqslant 0}$ convergeert en $\lim_{n\to\infty} x_n = x$.

12. Zij $x \in \mathbb{R}$. bewijs:

✍ (a) Als $|x| > 1$ dan is de rij $(x^n)_{n\geqslant 0}$ divergent.

(b) Als $|x| < 1$ dan $\lim_{n\to\infty} x^n = 0$.

(c) Als $x = 1$ dan $\lim_{n\to\infty} x^n = 1$.

(d) Als $x = -1$ dan is de rij $(x^n)_{n\geqslant 0}$ divergent.

VI.3 De kommanotatie voor reële getallen

Nu we het begrip convergente rij gedefinieerd hebben, kunnen we een korte excursie maken naar onze gebruikelijke notatie voor reële getallen, die we overigens aan de Nederlandse wiskundige Simon Stevin (1548–1620) te danken hebben. De volgende stelling laat zien dat de decimale notatie nog best complex is.

basis

Zij $b \geqslant 2$ een geheel getal. Een *cijfer in de basis* b is een natuurlijk getal c waarvoor geldt $0 \leqslant c < b$. Wij zijn gewend als basis 10 te gebruiken en spreken dan van *decimalen*.

VI.3.1 Stelling.

i) Voor iedere rij cijfers $(c_i)_{i\geqslant 1}$ in basis b is de rij $(x_n)_{n\geqslant 1}$ gegeven door

$$x_n = \sum_{i=1}^{n} c_i b^{-i}$$

convergent.

ii) Voor ieder reëel getal $x \in [0,1]$ bestaat er een rij cijfers $(c_i)_{i\geqslant 1}$ zodat voorgaande rij $(x_n)_{n\geqslant 1}$ convergeert naar x.

iii) Voor ieder reëel getal $x \in [0,1)$ dat niet gelijk is aan $x = \frac{t}{b^k}$ voor zekere $t,k \in \mathbb{N}\setminus\{0\}$, is de rij cijfers uniek.

iv) In het andere geval zijn er precies twee rijen die met $x = \frac{t}{b^k}$ zijn geassocieerd, en hiervoor geldt $c_i = 0$ respectievelijk $c_i = b-1$ voor i boven een bepaalde grens $N \in \mathbb{N}$.

We herkennen hier voor $b = 10$ de *decimale ontwikkeling*, die we noteren als

$$0{,}c_1c_2c_3\ldots,$$

of

$$\sum_{i=1}^{\infty} c_i b^{-i}.$$

We beperken ons in deze stelling voor het gemak tot reële getallen in $[0,1)$. De stelling laat zich makkelijk uitbreiden naar alle reële getallen. Merk op dat geen enkel geheel getal een unieke ontwikkeling heeft, *behalve* het getal 0.

Bewijs. (i) Dit volgt uit direct uit de monotoneconvergentiestelling (Stelling VI.2.11).

(ii) Zij $x \in [0,1]$ gegeven. Definieer c_i $(i \geqslant 1)$ met recursie, waarbij we voor het gemak de 'extra' term $c_0 = 0$ gebruiken: stel c_i gelijk aan dat geheel getal a met $0 \leqslant a < b$ waarvoor geldt

$$x \in \left[ab^{-i} + \sum_{j=0}^{i-1} c_j b^{-j}, (a+1)b^{-i} + \sum_{j=0}^{i-1} c_j b^{-j} \right).$$

We laten zien dat de rij (x_n) die door deze c_i's wordt gedefinieerd naar x convergeert. Zij daarom $\varepsilon > 0$ gegeven. Kies $N \in \mathbb{N}$ zó, dat $10^{-N} < \varepsilon$. Zij $n \geqslant N$. Dan geldt

$$0 \leqslant \sum_{i=1}^{n} c_i b^{-i} - x \leqslant 10^{-N} < \varepsilon.$$

(iii), (iv) Laat $(c_i)_{i\geqslant 1}$ en $(d_i)_{i\geqslant 1}$ twee verschillende rijen cijfers zijn zodat

$$x_n = \sum_{i=1}^{n} c_i b^{-i} \qquad \text{en} \qquad y_n = \sum_{i=1}^{n} d_i b^{-i}$$

beide naar hetzelfde getal convergeren. Bekijk

$$x_n - y_n = \sum_{i=1}^{n} (c_i - d_i) b^{-i}.$$

Zij j de kleinste index waarvoor $c_j \neq d_j$. Dan volgt voor $n > j$:

$$x_n - y_n = b^{-i} \cdot (c_j - d_j) + b^{-i} \cdot z_n, \quad \text{waarbij } z_n = \sum_{i=1}^{n-j} (c_{i+j} - d_{i+j}) b^{-i}.$$

Nu convergeert $x_n - y_n$ naar 0 en is $c_j - d_j$ een geheel getal, dus moet z_n ook naar een geheel getal convergeren. We zullen laten zien dat de enige mogelijke limieten 0, 1 en -1 zijn en dat in het geval ± 1 geldt $\{c_k, d_k\} = \{0, b-1\}$ voor alle $k > j$. Een eenvoudige berekening laat dan zien dat x van de vorm $\frac{t}{b^k}$ is.

Het komt erop neer dat we moeten onderzoeken wanneer de rij

$$\sum_{i=1}^{n} q_i b^{-i}, \qquad 0 \leqslant q_i < b \text{ en } q_i \in \mathbb{N}$$

convergeert naar een geheel getal. Als $q_i = 0$ voor alle i is dat natuurlijk het geval en zodra een $q_i \neq 0$ is de limiet in ieder geval positief. Stel dat er een i is waarvoor $q_i < b - 1$. Dan volgt uit

$$\sum_{i=1}^{n} (b-1)b^{-i} - \sum_{i=1}^{n} q_i b^{-i} = \sum_{i=1}^{n} (b - 1 - q_i)b^{-i}$$

dat deze rij convergeert naar een positief getal. Wat dus rest is aan te tonen dat de limiet van de rij

$$\sum_{i=1}^{n} (b-1)b^{-i} = (b-1)\sum_{i=1}^{n} (b^{-1})^i$$

gelijk is aan 1. Dit volgt uit Voorbeeld IV.2.2 en de constatering dat $\lim_{i\to\infty}(b^{-1})^i = 0$ omdat $b > 1$. ∎

Repeterende ontwikkeling

Een rij $(c_i)_{i\geqslant 1}$ heet *repeterend* als er een $N \in \mathbb{N}$ en een $d \geqslant 1$ bestaan zodat $c_i = c_{i+d}$ voor alle $i > N$.

VI.3.2 Stelling. Zij $x \in \mathbb{R}$, met een bijbehorende rij cijfers $(c_i)_{i\geqslant 1}$. De volgende uitspraken zijn equivalent:

i) de rij (c_i) is repeterend;
ii) x is rationaal.

We laten een precies bewijs van deze stelling achterwege, maar zullen aan de hand van een voorbeeld het bewijsidee schetsen. Het leuke is namelijk dat er een *constructief* bewijs te geven is!

VI.3.3 Voorbeeld. We nemen als basis $b = 10$ en laten zien hoe je bij de breuk $\frac{1}{7}$ de decimale ontwikkeling bepaalt. Dat kun je doen door een staartdeling uit te voeren:

$$\begin{array}{l} 7\,/\,1{,}0000000\,\backslash\,0{,}14285714\ldots \\ \quad\underline{7} \\ \quad\;30 \\ \quad\;\underline{28} \\ \quad\;\;20 \\ \quad\;\;\underline{14} \\ \quad\;\;\;60 \\ \quad\;\;\;\underline{56} \\ \quad\;\;\;\;40 \\ \quad\;\;\;\;\underline{35} \\ \quad\;\;\;\;\;50 \\ \quad\;\;\;\;\;\underline{49} \\ \quad\;\;\;\;\;\;10** \\ \quad\;\;\;\;\;\;\underline{7} \\ \quad\;\;\;\;\;\;30 \\ \quad\;\;\;\;\;\;28 \\ \quad\;\;\;\;\;\;\ldots \end{array}$$

Het lijkt erop dat geldt $\frac{1}{7} = 0{,}142857\ldots$, waarbij de ontwikkeling zich vanaf de puntjes gaat herhalen. Maar weten we dit zeker? Waarom zou na de laatste vier rechts in de staartdeling niet een heel ander getal kunnen komen? De reden is dat vanaf $***$ het algoritme zichzelf gaat herhalen. De rest 10 die bij de sterretjes staat, staat ook linksboven. We zijn dus dus in een lus terecht gekomen.

Maar dit is slechts een voorbeeld. De vraag is nu: treedt de herhaling ook bij andere breuken op? Het antwoord is 'ja' en wel om de volgende reden: Als je deelt door n, dan is in de staartdeling de rest per definitie altijd kleiner dan n. Er is dus maar een eindig aantal mogelijkheden voor de rest, namelijk $0, 1, \ldots, n-1$. Maar dat betekent dat als je maar lang genoeg doorgaat met staartdelen, je altijd een moment zult krijgen dat er een rest optreedt die al eerder is voorgekomen. Op dat moment treedt de herhaling op. (Een dergelijk argument is een toepassing van het *pigeon hole*-principe.)

Nu het tweede deel van de stelling (voor basis 10): **Als** de decimale ontwikkeling van x repeterend is, **dan** is het een breuk. Wederom doen we een voorbeeld: welke breuk is $x = 0{,}1\overline{234} = 0{,}1234234234\ldots$? Om deze vraag te beantwoorden, is er de volgende truc:

$$\begin{array}{rcl} 1000x & = & 123{,}4234234234234234\ldots \\ x & = & \quad 0{,}1234234234234234\ldots \quad - \\ \hline 999x & = & 123{,}3 \end{array}$$

De onderste vergelijking heeft als oplossing $x = 123{,}3999 = \frac{1233}{9990}$. ∎

$\mathbb{Q} \neq \mathbb{R}$

VI.3.4 Opmerking. We kunnen voorgaande stelling gebruiken om opnieuw te bewijzen dat niet ieder reëel getal als breuk te schrijven is. Niet iedere rij is immers repeterend! Neem maar

$$x = 0{,}101001000100001\ldots.$$

Opgaven

1. (a) Bewijs: Ieder positief, geheel getal x is op een unieke manier te schrijven als

$$x = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_0 \cdot 10^0,$$

met $c_i \in \{0, \ldots, 9\}$ en $c_k \neq 0$.

(b) Verklaar de '*negen-truc*': een positief, geheel getal is deelbaar door 9 precies dan als de som van de cijfers deelbaar is door 9. (Er is ook een drie-truc.)

(c) Veralgemeniseer voorgaande naar een willekeurige basis.

✍ **2.** Bepaal (zonder rekenmachine) de decimale ontwikkeling van de volgende breuken:

(a) $\frac{3}{11}$

(b) $\frac{3}{13}$

(c) $\frac{313}{495}$

(d) $\frac{15}{3}$

✍ **3.** Schrijf de volgende repeterende decimale ontwikkelingen als breuk:

(a) $0{,}4234231 = 0{,}4234231\overline{0}$

(b) $0{,}\overline{3211}$

(c) $2{,}12\overline{1}$

4. Geef een formeel bewijs (en dus niet enkel een voorbeeld) van de uitspraak 'Iedere repeterende decimale ontwikkeling definieert een breuk.'

VI.4 Compleetheid

Metriek

In de lijn, het vlak en de ruimte kunnen we spreken over de afstand $\mathrm{d}(P,Q)$ tussen twee punten P en Q. We zullen in de volgende een aantal eigenschappen van de intuïtieve notie van afstand extraheren.

VI.4.1 Definitie. Zij A een verzameling. Een *metriek* op A is een functie

$$\mathrm{d}\colon A \times A \to \mathbb{R}$$

die voldoet aan de volgende eigenschappen:

i) $\forall_{a,b\in A}\, \mathrm{d}(a,b) \geqslant 0$;
ii) $\forall_{a,b\in A}(\mathrm{d}(a,b) = 0 \iff a = b)$;
iii) $\forall_{a,b\in A}\, \mathrm{d}(a,b) = \mathrm{d}(b,a)$;
iv) $\forall_{a,b,c\in A}\, \mathrm{d}(a,c) \leqslant \mathrm{d}(a,b) + \mathrm{d}(b,c)$.

Een verzameling met een metriek noemen we een *metrische ruimte*.

Metrische ruimte, driehoeksongelijkheid

De laatste voorwaarde (iv) wordt de *driehoeksongelijkheid* genoemd — teken maar een driehoek met hoekpunten a, b en c om te zien waar deze naam vandaan komt. In woorden: om van a naar c te gaan via b is minstens even lang als rechtstreeks. De ongelijkheid in het volgende lemma heet de *omgekeerde driehoeksongelijkheid*. In woorden zegt deze ongelijkheid: de afstand van a naar b is minstens het verschil van de afstanden van a naar c en van b naar c.

VI.4.2 Lemma. Laat (A,d) een metrische ruimte zijn. Dan geldt voor alle a, b en c in A dat:

$$\mathrm{d}(a,b) \geq |\,\mathrm{d}(a,c) - \mathrm{d}(b,c)|.$$

Bewijs. Laat a, b en c in A. De driehoeksongelijkheid geeft $\mathrm{d}(a,c) \leqslant \mathrm{d}(a,b) + \mathrm{d}(b,c)$. Aan beide kanten $\mathrm{d}(b,c)$ aftrekken geeft: $\mathrm{d}(a,c) - \mathrm{d}(b,c) \leqslant \mathrm{d}(a,b)$. Verwisselen van de rollen van a en b geeft dat $\mathrm{d}(b,c) - \mathrm{d}(a,c) \leqslant \mathrm{d}(a,b)$. Samen geven deze ongelijkheden het gevraagde. ∎

VI.4.3 Stelling. De functie $d\colon \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ gegeven door $d(a,b) = |a-b|$ is een metriek op $\mathbb{R}$. Is $V \subset \mathbb{R}$, dan geeft beperking hiervan tot $V \times V$ een metriek op V.

Bewijs. Zie Opgave VI.4.1 voor het eerste deel. Het tweede deel is een algemene eigenschap van metrieken: in de definitie komt enkele de universele kwantor voor en niet de existentie-kwantor. ∎

VI.4.4 Gevolg. Voor alle a, b en c in $\mathbb{R}$ geldt: $|a-b| \geqslant ||a| - |b||$.

Bewijs. Pas de omgekeerde driehoeksongelijkheid toe met a, b en 0. ∎

VI.4.5 Voorbeeld. Pythagoras geeft in $\mathbb{R}^2$ een metriek:

$$\mathrm{d}\big((x_1,y_1),(x_2,y_2)\big) = \sqrt{(x_1-x_2)^2 + (y_1-y_2)^2}.$$

Deze *euclidische metriek* is niet de enige metriek op $\mathbb{R}^2$. Een ander voorbeeld is de zogenaamde *manhattanmetriek*, genoemd naar het stratenpatroon van New York:

$$\mathrm{d}_m\big((x_1,y_1),(x_2,y_2)\big) = |x_1-x_2| + |y_1-y_2|.$$

Deze voorbeelden laten zich generaliseren naar $\mathbb{R}^n$ voor $n \in \mathbb{N}$. Merk op dat ze voor $n = 1$ gelijk zijn en identiek aan de metriek uit stelling VI.4.3. ∎

Opnieuw convergentie

We kunnen nu algemener definiëren wat convergentie van rijen is.

VI.4.6 Definitie. Zij A een metrische ruimte. Een rij $(a_n)_{n\geqslant 0}$ in A heet *convergent* wanneer er een $a \in A$ bestaat met de volgende eigenschap: voor iedere $\varepsilon > 0$ bestaat een $N \in \mathbb{N}$ zodanig dat

$$\text{voor alle } n \geq N: \quad \mathrm{d}(a_n, a) < \varepsilon.$$

We noemen a een *limiet* van de rij $(a_n)_{n\geqslant 0}$. Notatie:

$$\lim_{n\to\infty} a_n = a.$$

Een rij die niet convergent is heet *divergent*.

Cauchy-rij

We zullen nader kijken naar criteria waaronder een rij convergeert. Nadeel van voorgaande definitie is dat de limiet a bekend moet zijn om na te gaan of een rij convergeert. De definitie die we nu invoeren, verwijst enkel naar de bekende termen van de rij $(x_n)_{n\geqslant 0}$ en niet naar de mogelijke limiet.

VI.4.7 Definitie. Zij A een metrische ruimte. Een rij $(x_n)_{n\geqslant 0}$ in A heet een *cauchy-rij* als er voor iedere $\varepsilon > 0$ een $N \in \mathbb{N}$ bestaat met de volgende eigenschap:

$$\text{voor alle } m, n \geq N: \quad \mathrm{d}(x_n, x_m) < \varepsilon.$$

VI.4.8 Voorbeelden. We geven twee voorbeelden voor reële rijen.

(a) De rij $(1/(n+1))_{n\geq 0}$ is een cauchy-rij. Immers, zij $\varepsilon > 0$. Kies $N \in \mathbb{N}$ met $N + 1 > 2/\varepsilon$ dan is $1/(N+1) < \varepsilon/2$. Hieruit volgt dat voor elke $m, n \geqslant N$ geldt:

$$\Big|\frac{1}{n+1} - \frac{1}{m+1}\Big| \leqslant \frac{1}{n+1} + \frac{1}{m+1} \leqslant \frac{2}{N+1} < \varepsilon.$$

(b) De rij $((-1)^n)_{n\geq 0}$ is geen cauchy-rij want voor $\varepsilon = 1$ bestaat geen $N > 0$ zó dat *voor alle* $n \geqslant N$ geldt $|(-1)^n - (-1)^m| < 1$: zij $N > 0$ en neem $n = N + 1$ en $m = N$ dan geldt $|(-1)^n - (-1)^m| = |(-1)^{N+1} - (-1)^N| = 2 \not< 1$.

VI.4.9 Stelling. Iedere convergente rij in A is een cauchy-rij.

Bewijs. Zie Opgave VI.4.4. ∎

compleet

Het omgekeerde van Stelling VI.4.9 is niet altijd waar.

VI.4.10 Definitie. Zij A een verzameling met een metriek. De verzameling A is *compleet* voor de metriek d als iedere cauchy-rij convergeert.

VI.4.11 Stelling. $\mathbb{R}$ (met de standaardmetriek) is compleet.

Bewijs. Zij $(x_n)_{n\geqslant 0}$ een Cauchy-rij in $\mathbb{R}$. Definieer voor iedere $n \in \mathbb{N}$ de deelverzameling

$$S_n = \{x_m : m \geqslant n\} \subset \mathbb{R}.$$

Merk op dat $S_n \subseteq S_{n'}$ als $n \geqslant n'$. Merk ook op dat $S_{n'} \setminus S_n$ een eindige verzameling is; in het bijzonder geldt dat iedere S_n begrensd is zodra we dat voor één index n hebben vastgesteld, hetgeen we hieronder zullen doen.

Voor iedere $\varepsilon > 0$ bestaan er $N \in \mathbb{N}$ en $g \in \mathbb{R}$, zodat S_N bevat is in het interval

$$(g - \tfrac{1}{2}\varepsilon, g + \tfrac{1}{2}\varepsilon).$$

Immers, aangezien $(x_n)_{n\geqslant 0}$ cauchy is, bestaat er een $N \in \mathbb{N}$ zodat $|x_m - x_n| < \frac{1}{2}\varepsilon$ voor alle $n, m \geqslant N$; nemen we nu $g = x_N$, dan volgt $|g - x| < \frac{1}{2}\varepsilon$ voor alle $x \in S_N$.

In het bijzonder is iedere S_n begrensd en niet leeg en dus bestaat het supremum $\sup S_n$, dat we met s_n zullen noteren. Uit het voorgaande volgt bovendien dat er voor iedere $\varepsilon > 0$ een grens $N \in \mathbb{N}$ bestaat zodat voor alle $m, n \geqslant N$ geldt $|s_n - x_m| \leqslant \varepsilon$.

De rij $(s_n)_{n \geqslant 0}$ is begrensd en dalend. Volgens de monotoneconvergentiestelling (Stelling VI.2.11) heeft de rij dus een limiet $s \in \mathbb{R}$.

Zij nu $\varepsilon > 0$ gegeven. Omdat s een limiet is, bestaat er een $N_1 \in \mathbb{N}$ zodat $|s - s_n| < \frac{1}{2}\varepsilon$ voor alle $n \geqslant N_1$. We hebben ook geconstateerd dat er een $N_2 \in \mathbb{N}$ is zodat $|s_n - x_n| \leqslant \frac{1}{2}\varepsilon$ voor alle $n \geqslant N_2$. Stel nu $N = \max(N_1, N_2)$. Dan geeft de driehoeksongelijkheid dat voor alle $n \geqslant N$ geldt:

$$|s - x_n| \leqslant |s - s_n| + |s_n - x_n| < \frac{1}{2}\varepsilon + \frac{1}{2}\varepsilon = \varepsilon.$$

Dus is s per definitie een limiet van de rij $(x_n)_{n \geqslant 0}$, waarmee is aangetoond dat de rij convergent is. ∎

VI.4.12 Voorbeelden.

- $\mathbb{Q}$ met de standaardmetriek is niet compleet. Neem maar een (de) decimale ontwikkeling van $\sqrt{2}$:

  $$\sqrt{2} = 1 + \sum_{i=1}^{\infty} c_i 10^{-i} \qquad \text{met } c_i \in \{0, 1, \ldots, 9\}.$$

  Het is makkelijk te zien dat de rij $(a_n)_{n \geqslant 0}$ gegeven door $a_0 = 1$ en

  $$a_n = 1 + \sum_{i=1}^{n} c_i 10^{=i} \qquad (n \geqslant 1)$$

  een cauchy-rij in $\mathbb{Q}$ is (dit volgt uit Stelling VI.4.9 met $A = \mathbb{R}$). Deze rij convergeert echter niet in $\mathbb{Q}$.
- Ieder niet leeg begrensd open interval (a, b) in $\mathbb{R}$ is niet compleet. Het argument gaat analoog als hiervoor: construeer een cauchy-rij die in $\mathbb{R}$ limiet b heeft.

VI.4.13 Stelling. $\mathbb{R}^k$ (met $k \geqslant 1$) met de euclidische metriek is compleet.

Bewijs. Zij $(x_n)_{n \geqslant 0}$ een cauchy-rij in $\mathbb{R}^k$. Noteer met $x_{n,i}$ de i-de coördinaat van x_n. Zij $\varepsilon > 0$ gegeven. Volgens de definitie van cauchyrij is er een $N \in \mathbb{N}$ zodat voor alle $n, m \geqslant N$:

$$d(x_n, x_m) = \sqrt{\sum_{i=1}^{k} (x_{n,i} - x_{m,i})^2} < \varepsilon.$$

Daaruit volgt dat voor iedere $1 \leqslant i \leqslant k$ dan ook geldt

$$|x_{n,i} - x_{m,i}| < \varepsilon.$$

Bijgevolg is voor iedere $1 \leqslant i \leqslant k$ de rij $(x_{n,i})_{n \geqslant 0}$ een cauchy-rij en dus bestaat er volgens Stelling VI.4.11 een limiet $p_i \in \mathbb{R}$. Definieer $p = (p_1, p_2, \ldots, p_k) \in \mathbb{R}^k$; we zullen laten zien dat de rij $(x_n)_{n \geqslant 0}$ naar p convergeert, waarmee het bewijs van de stelling dan voltooid is.

Zij wederom $\varepsilon > 0$ gegeven. Omdat p_i een limiet is van $(x_{n,i})_{n \geqslant 0}$, bestaat er een $N_i \in \mathbb{N}$ zodat voor alle $n \geqslant N_i$ geldt

$$|x_{n,i} - p_i| < \frac{\varepsilon}{\sqrt{k}}.$$

Dan geldt voor alle $n \geqslant \max(N_1, N_2, \ldots, N_k)$:

$$d(x_n, p)^2 = \sum_{i=1}^{k} (x_{n,i} - p_i)^2 < \sum_{i=1}^{k} \left(\frac{\varepsilon}{\sqrt{k}}\right)^2 = \varepsilon^2$$

en dus $d(x_n, p) < \varepsilon$. ∎

deelrij

Laat $(a_n)_{n\geqslant 0}$ en $(a'_n)_{n\geqslant 0}$ rijen zijn in een verzameling A. Per definitie zijn dit afbeeldingen $a, a' : \mathbb{N} \to A$. We noemen $(a'_n)_{n\geqslant 0}$ een *deelrij* van $(a_n)_{n\geqslant 0}$ als $a' = a \circ r$ voor een functie $r : \mathbb{N} \to \mathbb{N}$ waarvoor $r(n) > r(m)$ als $n > m$. Minder formeel gezegd: een deelrij van een rij $(a_n)_{n\geqslant 0}$ ontstaat door uit de rij $a_0, a_1, a_2, \ldots$ termen weg te laten (mogelijk geen) zodat er nog oneindig veel termen overblijven. Voorbeeld: de rij niet-negatieve even getallen is een deelrij van de telrij $0, 1, 2, 3, \ldots$.

rijcompact

VI.4.14 Definitie. Een metrische ruimte heet *rijcompact* als iedere rij een convergente deelrij heeft.

Een deelverzameling W van een metrische ruimte V is op een natuurlijke manier weer een metrische ruimte door beperking van de metriek $\mathrm{d} : V \times V \to \mathbb{R}$ tot $W \times W$. Het volgende is belangrijk om te beseffen: als V rijcompact is, dan heeft in het bijzondere iedere rij in W een deelrij die convergeert *naar een element in* V. Dat impliceert niet dat W rijcompact is — dat is pas het geval als iedere rij een deelrij heeft die convergeert naar een element *dat bevat is in* W. Dit motiveert de volgende definitie.

Open,
Gesloten

VI.4.15 Definitie. Een deelverzameling $Z \subseteq \mathbb{R}^n$ heet *gesloten* als voor iedere convergente rij $(a_n)_{n\geqslant 0}$ in $\mathbb{R}^n$ met limiet $a \in \mathbb{R}^n$ geldt:

$$\left(\forall_{n\in\mathbb{N}} a_n \in Z\right) \quad \Longrightarrow \quad a \in \mathbb{Z}.$$

Een deelverzameling $U \subseteq \mathbb{R}^n$ heet *open* als $R^n \setminus U$ gesloten is.

Gezien de discussie voorafgaand aan de definitie geldt dat iedere gesloten deelverzameling van een rijcompacte verzameling rijcompact is. Ook geldt vanwege Stelling VI.4.9 dat een deelverzameling Z van een complete metrische ruimte gesloten is precies dan als iedere cauchy-rij in Z een limiet in Z heeft.

We zullen nu onze aandacht weer richten op $\mathbb{R}^n$. Doel is om te komen tot een noodzakelijke en voldoende voorwaarde waaronder een deelverzameling van $\mathbb{R}^n$ rijcompact is, zonder dat we daarvoor naar convergentie van rijen hoeven te verwijzen. De eerste stap is dat we een andere beschrijving geven van open en gesloten deelverzamelingen van $\mathbb{R}^n$ aan de hand van het begrip 'bol'.

Bol

VI.4.16 Definitie. De *bol in* $\mathbb{R}^n$ *met middelpunt* $x \in \mathbb{R}^n$ *en straal* $\varepsilon > 0$ is de deelverzameling

$$B_{x,\varepsilon} = \{x \in \mathbb{R}^n : \mathrm{d}(y, x) < \epsilon\}.$$

De bol $B_{x,\varepsilon}$ wordt ook een *bolomgeving* van x genoemd.

VI.4.17 Stelling. Een deelverzameling $U \subseteq \mathbb{R}^n$ is open precies dan als iedere $x \in U$ een bolomgeving B heeft, zodat $B \subseteq U$.

In Opgave VI.4.8 zul je uit deze stelling afleiden dat de 'open' intervallen $(\leftarrow, b)$, (a, b) en $(a, \rightarrow)$ inderdaad open zijn volgens onze definitie; en dat analoog de intervallen $(\leftarrow, b]$, $[a, b]$ en $[a, \rightarrow)$ gesloten zijn.

Bewijs. (van Stelling VI.4.17) Zij $U \subset \mathbb{R}^n$ en noteer $Z = \mathbb{R}^n \setminus U$.

'$\Rightarrow$': Stel U is open; dan is Z dus gesloten. Zij $x \in U$. Stel dat $B_{x,\varepsilon} \not\subseteq U$ voor alle $\varepsilon > 0$; dan geldt dus voor alle $\varepsilon > 0$ dat $B_{x,\varepsilon} \cap Z \neq \varnothing$. Kies voor iedere $n \in \mathbb{Z}$ een element $x_n \in B_{x,\frac{1}{n+1}} \cap Z$. Dit definieert een rij $(x_n)_{n\geqslant 0}$ in Z die convergeert naar x. Omdat Z gesloten is, geldt $x \in Z$; tegenspraak.

'$\Leftarrow$': Stel dat voor iedere $x \in U$ er een $\varepsilon > 0$ is zodat $B_{x,\epsilon} \subseteq U$. Laat $(a_n)_{n\geqslant 0}$ een rij zijn in Z die in $\mathbb{R}^n$ convergeert naar $a \in \mathbb{R}^n$. We zullen laten zien dat $a \in Z$; daarmee is dan aangetoond dat Z gesloten is en U dus open.

Stel $a \notin Z$. Dat $a \in U$. Er is dus een $\varepsilon > 0$ zodat $B_{a,\varepsilon} \subseteq U$. Maar uit de definitie van limiet volgt dat er een $N \in \mathbb{N}$ is zodat $\mathrm{d}(a_n, a) < \varepsilon$ voor alle $n \geqslant N$. Hieruit volgt $a_N \in U$ en dus $a_N \notin Z$; tegenspraak. ∎

Begrensd

Een deelverzameling V van een metrische ruimte A is *begrensd* als het beeld onder de metriek $\mathrm{d}(V \times V) \subseteq \mathbb{R}$ begrensd is. Equivalent: V is begrensd precies dan als er $a \in A$ en $r \in \mathbb{R}$ zijn met $V \subseteq B_{a,r}$. Een rij $(a_n)_{n\geqslant 0}$ in een metrische ruimte A heet begrensd als $\{a_n : n \in \mathbb{N}\} \subseteq A$ begrensd is.

Bolzano-Weierstrass

De volgende stelling staat, althans voor het geval $n = 1$, bekend als de *Stelling van Bolzano-Weierstrass*. Ze zal leiden tot de gewenste beschrijving van rijcompacte deelverzamelingen van $\mathbb{R}^n$ in Gevolg VI.4.20. We beginnen met een elementair lemma.

VI.4.18 Lemma. Zij V een begrensde deelverzameling van $\mathbb{R}^n$ en zij $\varepsilon > 0$. Dan is V bevat in de vereniging van een eindig aantal deelverzamelingen $V_1, V_2, \ldots, V_r$ die zo gekozen kunnen worden dat voor alle i en alle $x, y \in V_i$ geldt $\mathrm{d}(x, y) < \varepsilon$.

Bewijs. Het idee is om $\mathbb{R}^n$ te bedekken met (niet noodzakelijk disjuncte) 'hyperkubusjes' met ribben kleiner dan ε (denk bijvoorbeeld aan het roosterpapier waarmee je het vlak in vierkantjes verdeelt) op zo'n manier dat maar eindig veel van deze kubusjes een niet lege doorsnede heeft met V. Voor details verwijzen we naar Opgave VI.4.10. ∎

VI.4.19 Stelling. Iedere begrensde rij in $\mathbb{R}^n$ heeft een convergente deelrij.

Bewijs. Zij $(a_n)_{n\geqslant 0}$ zo'n begrensde rij. We zullen een rij deelverzamelingen

$$\cdots \subset I_{n+1} \subset I_n \subset \cdots \subset I_2 \subset I_1 \subset I_0 = \mathbb{N}$$

definiëren waarbij voor iedere $n \geqslant 1$ geldt:

i) I_n bestaat uit oneindig veel elementen;
ii) het kleinste element van I_{n+1} (dat bestaat volgens welordening) is niet het kleinste element van I_n;
iii) voor alle $n > 0$ en alle $i, j \in I_n$ geldt $\mathrm{d}(a_i, a_j) < \frac{1}{n}$.

Daartoe gebruiken we recursie. We weten al $I_0 = \mathbb{N}$. Stel nu dat I_n gedefinieerd is voor een bepaald $n \in \mathbb{N}$. Herinner je dat de rij in feite een afbeelding $a : \mathbb{N} \to \mathbb{R}^n$ is. Volgens Lemma VI.4.18 kan het beeld $a(I_n)$ overdekt worden met eindig veel deelverzamelingen $V_1, V_2, \ldots, V_r$ waarvan de elementen afstand kleiner dan $\frac{1}{n+1}$ hebben. Dan geldt

$$I_n \subset a^{-1}(V_1) \cup a^{-1}(V_2) \cup \cdots \cup a^{-1}(V_r)$$

en omdat I_n oneindig veel elementen heeft, moet er een index i zijn zodat ook $J = I_n \cap a^{-1}(V_i)$ oneindig is. Laat nu I_{n+1} gelijk zijn aan J met daaruit weggelaten het kleinste element van I_n. Hiermee is de rij deelverzamelingen gedefinieerd.

Definieer nu $r : \mathbb{N} \to \mathbb{N}$ door $r(n) = \min I_n$ en bekijk de rij $a \circ r$ — anders gezegd, de rij $(a_{r(n)})_{n\geqslant 0}$. Dit is een deelrij van de rij $(a_n)_{n\geqslant 0}$, en deze deelrij is per constructie een cauchy-rij. Bijgevolg is de deelrij convergent. ∎

VI.4.20 Gevolg. Een deelverzameling $Z \subset \mathbb{R}^n$ is rijcompact precies dan als Z begrensd en gesloten is.

Bewijs. '⇒': Stel Z is rijcompact. Zij $(a_n)_{n\geqslant 0}$ een convergente rij in $\mathbb{R}^n$ zodat $a_n \in Z$ voor alle $n \in \mathbb{N}$; zij $a \in \mathbb{R}^n$ de limiet. Iedere deelrij van $(a_n)_{n\geqslant 0}$ convergeert naar limiet a (Opgave VI.4.3). Omdat er volgens rijcompactheid een deelrij is die naar een limiet in Z convergeert, volgt dus $a \in Z$. Dus Z is gesloten.

Stel nu dat Z niet begrensd zou zijn. We definiëren nu een rij $(a_n)_{n\geqslant 0}$ in Z. Laat $a_0 \in Z$ willekeurig (omdat Z niet begrensd is, is het in het bijzonder niet leeg). Kies $a_n \in Z$ voor $n \geqslant 1$ zo, dat $\mathrm{d}(a_0, a_n) > n$; zo'n element bestaat, omdat anders voor alle $z, y \in Z$ zou gelden

$$\mathrm{d}(z, y) \leqslant \mathrm{d}(x, a_0) + \mathrm{d}(a_0, y) \leqslant 2n$$

en dat is in tegenspraak met onbegrensdheid. Volgens rijcompactheid is er een deelrij $(a_{r(n)})_{n\geqslant 0}$ die convergent is en dus (Stelling VI.4.9) cauchy. Voor ieder $\varepsilon > 0$ is er dus een $N \in \mathbb{N}$ zodat $\mathrm{d}(a_{r(N)}, a_{r(m)}) < \varepsilon)$ voor alle $m > N$. Maar dan geldt voor al deze m:

$$\mathrm{d}(a_0, a_{r(m)}) \leqslant \mathrm{d}(a_0, a_{r(N)}) + \mathrm{d}(a_{r(N)}, a_{r(m)}) < \mathrm{d}(a_0, a_{r(N)}) + \varepsilon.$$

Het rechterlid van deze ongelijkheid is constant, terwijl het linkerlid variabel is en groter is dan $r(m)$; tegenspraak.

'$\Leftarrow$': Stel Z is begrensd en gesloten. Zij $(a_n)_{n\geqslant 0}$ een rij in Z. Dan is $(a_n)_{n\geqslant 0}$ een begrensde rij en dus geldt volgens Stelling VI.4.19 dat er een deelrij is die convergeert naar een element $a \in \mathbb{R}^n$. Maar omdat deze deelrij ook een rij in Z is, volgt uit geslotenheid van Z dat $a \in Z$. Dus is Z rijcompact. ■

Opgaven

1. Bewijs het eerste deel van Stelling VI.4.3.

2. Bekijk Voorbeeld VI.4.5.

(a) Bewijs dat de 'euclidische metriek' inderdaad een metriek is op $\mathbb{R}^2$.

(b) Bewijs dat de 'manhattanmetriek' inderdaad een metriek is op $\mathbb{R}^2$.

(c) Doe hetzelfde voor $\mathbb{R}^n$ met $n > 2$.

3. Zij A een verzameling met een metriek en zij $(a_n)_{n\geqslant 0}$ een convergente rij in A.

(a) Bewijs dat de limiet van de rij uniek is.

(b) Bewijs dat iedere deelrij convergent is met dezelfde limiet als de volledige rij.

✍ **4.** Bewijs Stelling VI.4.9.

5. Bewijs dat $\mathbb{R}^n$ (met $n \geqslant 1$) voorzien van de manhattanmetriek (zie Voorbeeld VI.4.5) compleet is. Hint: dit kan op dezelfde manier als het bewijs van Stelling VI.4.13.

6. Bewijs: Iedere bol in $\mathbb{R}^n$ is open.

7. Bewijs dat $\mathbb{R}^n$ en $\varnothing$ zowel open als gesloten zijn. Geef ook een voorbeeld van een deelverzameling van $\mathbb{R}^n$ die open noch gesloten is.

8. Bewijs dat voor alle $a, b \in \mathbb{R}$ geldt:

(a) de intervallen $(\leftarrow, b]$, $[a, b]$ en $[a, \rightarrow)$ zijn gesloten;

(b) de intervallen $(\leftarrow, b)$, (a, b) en $(a, \rightarrow)$ zijn open.

[Hint: gebruik Stelling VI.4.17.]

9. In deze opgave kijken we naar deelverzamelingen van $\mathbb{R}^n$.

(a) Bewijs dat een vereniging van eindig veel gesloten verzamelingen gesloten is.

(b) Bewijs dat een doorsnede van een willekeurige collectie gesloten verzamelingen gesloten is.

(c) Formuleer analoge uitspraken voor open verzamelingen.

10. Bewijs Lemma VI.4.18.

VI.5 Limieten en continuïteit van functies

We beperken ons tot functies van een deelverzameling van $\mathbb{R}^n$ naar $\mathbb{R}^m$. Doel is te laten zien hoe in lijn met de voorgaande paragraaf limieten en continuïteit precies kunnen worden gedefinieerd. Uiteraard vormt dit slechts een bescheiden basis van een onderwerp dat in een analyse- of calculuscursus veel meer aandacht krijgt.

De volgende definitie van continuïteit maakt de intuïtie precies dat 'een kleine variatie in x leidt tot een kleine variatie in $f(x)$'.[1]

Continu

VI.5.1 Definitie. Zij $V \subseteq \mathbb{R}^n$ en zij $f : V \to \mathbb{R}^m$ een functie. De functie f is *continu in een punt* $a \in V$ als er voor iedere bolomgeving $B_{f(a)}$ van $f(a)$ een bolomgeving B_a van a is, zodat

$$f(B_a \cap V) \subseteq B_{f(a)}.$$

De functie heet *continu* als f continu is voor alle $a \in V$.

Er is een andere veelgebruikte manier om continuïteit te definiëren, die aansluit bij de intuïtie dat de grafiek van een continue functie geen 'sprongen maakt'. Hiervoor hebben we de notie van limiet van een functie nodig, die we daarom nu introduceren.

VI.5.2 Definitie. Zij $f : V \to \mathbb{R}^n$ met $V \subseteq \mathbb{R}^m$ een functie en zij $a \in \mathbb{R}^m$ en $b \in \mathbb{R}^n$. We zeggen dat $f(x)$ *limiet* b *heeft als* x *naar* a *nadert* en noteren

$$\lim_{x \to a} f(x) = b,$$

als geldt: voor iedere bolomgeving B_b van b is er een bolomgeving B_a van a zodat

$$f(B_a \cap V \setminus \{a\}) \subseteq B_b.$$

Merk op dat a geen element van het domein van f hoeft te zijn. Zie ook Opgave VI.5.1. De volgende stelling is nu gewoon een herformulering van de definitie:

VI.5.3 Stelling. Een functie $f : V \to \mathbb{R}^n$ (met $V \subseteq \mathbb{R}^m$) is continu in $a \in V$ precies dan als

$$\lim_{x \to a} f(x) = f(a).$$

VI.5.4 Opmerking. De definiërende voorwaarde van $\lim_{x \to a} f(x) = b$ wordt vaak als volgt geformuleerd:

$$\forall_{\varepsilon > 0} \exists_{\delta > 0} \forall_{x \in V} \big(0 < \mathrm{d}(x,a) < \delta \implies \mathrm{d}(f(x), b) < \varepsilon\big).$$

Dat leidt tot de volgende definitie van continuïteit van f in a:

$$\forall_{\varepsilon > 0} \exists_{\delta > 0} \forall_{x \in V} \big(\mathrm{d}(x,a) < \delta \implies \mathrm{d}(f(x), f(a)) < \varepsilon\big).$$

Dit staat in de wandelgangen bekend als 'de epsilon-delta-definities'.

[1] Het zou nuttig zijn als bijvoorbeeld belastingwetten voldeden aan de eis dat de te betalen belasting continu is als functie van de input. Helaas wordt er bij het schrijven van dit soort wetten liever taal dan formules gebruikt.

VI.5.5 Voorbeeld. De functie $f:\mathbb{R}\to\mathbb{R}$ gegeven door $f(x)=|x|$ is continu in elke $c\in\mathbb{R}$. We zoeken voor elke $\varepsilon>0$ een $\delta>0$ zó dat voor elke $x\in\mathbb{R}$ met $|x-c|<\delta$ geldt $\big||x|-|c|\big|<\varepsilon$. We gaan hiervoor de omgekeerde driehoeksongelijkheid $\big||x|-|c|\big|\leqslant|x-c|$ gebruiken (zie Gevolg VI.4.4).

Zij $\varepsilon>0$ willekeurig. Kies $\delta=\varepsilon$. Neem aan dat $x,c\in\mathbb{R}$ en $|x-c|<\delta$. Er volgt

$$|f(x)-f(c)|=\big||x|-|c|\big|\leqslant|x-c|<\varepsilon.$$

Dus f is continu. ∎

VI.5.6 Voorbeeld. De functie $f:(-1,0)\cup(0,1)\to\mathbb{R}$ gedefinieerd door

$$f(x)=\begin{cases}0, & x\in(-1,0)\\ 1, & x\in(0,1)\end{cases}$$

is continu, want het volgt onmiddellijk uit de definitie dat f continu is in ieder punt van $(-1,0)$ en $(0,1)$.

Daarentegen is de functie $f:(-1,1)\to\mathbb{R}$ gedefinieerd door

$$f(x)=\begin{cases}0, & x\in(-1,0]\\ 1, & x\in(0,1)\end{cases}$$

niet continu, want f is niet continu in het punt 0. Inderdaad, neem bijvoorbeeld $\varepsilon=1/2$. Kies $\delta>0$ willekeurig. Neem $x\delta/2$. Dan geldt $|x-0|=|x|<\delta$ en

$$\big|f(x)-f(0)\big|=|f(x)|=1\geqslant\frac{1}{2}.$$

∎

VI.5.7 Voorbeeld. Laat $f:\mathbb{R}\setminus\{1\}\to\mathbb{R}$, gegeven zijn door $f(x)=\frac{x^2-1}{x-1}$. We tonen aan dat $\lim\limits_{x\to1}f(x)=2$. Merk op dat

$$f(x)=(x+1)(x-1)/(x-1)=x+1,\quad x\in\mathbb{R}\setminus\{-1\}.$$

Het is eenvoudig om te zien dat $\lim\limits_{x\to1}(x+1)=2$. Hieruit volgt het gevraagde. ∎

VI.5.8 Voorbeeld. Laat $f:\mathbb{R}\setminus\{0\}\to\mathbb{R}$ gegeven zijn door $f(x)=1/x$. Neem eens aan dat er een $L\in\mathbb{R}$ is met $\lim\limits_{x\to0}f(x)=L$. Zij $\varepsilon=1$. Volgens de definitie van de limiet is er een $\delta>0$ zó dat voor alle $x\in\mathbb{R}$ geldt: als $0<|x|<\delta$ dan $|f(x)-L|<\varepsilon$. We nemen zo'n δ. Dan geldt, voor $x\in(0,\delta)$, dat $f(x)\in(L-1,L+1)$. Maar $f[(0,\delta)]=(1/\delta,\infty)$. Dit is een tegenspraak. Dus heeft f geen limiet in 0. ∎

We geven nu een belangrijke toepassing van de theorie over rijcompactheid uit de vorige paragraaf.

VI.5.9 Stelling. Zij $Z:\mathbb{R}^m$ begrensd, gesloten en niet leeg en zij $f:Z\to\mathbb{R}$ een continue functie. Dan heeft f een maximum. (Met andere woorden: er is een $z\in Z$ zodat voor alle $x\in Z$ geldt $f(z)\geqslant f(x)$.)

Bewijs. Volgens Gevolg VI.4.20 is Z rijcompact: iedere rij in Z heeft een convergente deelrij.

Bekijk het beeld $f(Z)$ van Z. We zullen eerst bewijzen dat het beeld een begrensde deelverzameling van $\mathbb{R}$ is. Stel namelijk dat dit niet het geval is. Dan is er voor iedere $n\in\mathbb{N}$ een $a_n\in Z$ zodat $f(a_n)>n$. De aldus gedefinieerde rij $(a_n)_{n\geqslant0}$ heeft een convergente deelrij $(a_{r(n)})_{n\geqslant0}$ met limiet $a\in Z$. Kies een bolomgeving $B_{f(a)}$ van $f(a)$. Aangezien f continu is, bestaat er een bolomgeving B_a van a zodat

$f(B_a \cap Z) \subseteq B_{f(a)}$. Vanwege de limieteigenschap bestaat er een $N \in \mathbb{N}$ zodat voor alle $n \geqslant N$ geldt $a_{r(n)} \in B_a$. Bijgevolg geldt $f(a_{r(n)}) \in B_{f(a)}$, terwijl ook geldt

$$|f(a_{r(n)})| \leqslant |f(a_{r(n)}) - f(a)| + |f(a)|$$

en dus is $f(a_{r(n)})$ begrensd, terwijl we weten dat $|f(a_{r(n)})| > r(n)$; tegenspraak. Dus is $f(Z)$ begrensd en niet leeg, dus heeft $f(Z)$ een supremum.

Noteer $m = \sup f(Z)$. We zullen laten zien dat $m \in f(Z)$ en daarmee is de stelling bewezen. Zij $n \in \mathbb{N}$ en bekijk het interval $(m - \frac{1}{n+1}, m]$. Dit interval is niet disjunct met $f(Z)$, omdat m het supremum is. Bijgevolg kunnen we een element $a_n \in Z$ kiezen zodat $|m - f(a_n)| < \frac{1}{n+1}$. Dit definieert een rij $(a_n)_{n\geqslant 0}$ in Z die een convergente deelrij $(a_{r(n)})_{n\geqslant 0}$ heeft met limiet $a \in Z$. We claimen dat de rij $(f(a_{r(n)}))_{n\geqslant 0}$ convergent is met limiet $f(a)$. Voor iedere $\varepsilon > 0$ is er vanwege continuïteit van f in a een $\delta > 0$ zodat voor alle $x \in Z$ met $\mathrm{d}(x,a) < \delta$ geldt dat $|f(x) - f(a)| < \varepsilon$. Laat nu $N \in \mathbb{N}$ zodat $1/N < \delta$. Dan geldt voor alle $n \geq N$ dat $|a_{r(n)} - a| < 1/N < \delta$ en dus $|f(a_{r(n)}) - f(a)| < \varepsilon$. Dus is $f(a)$ een limiet van de deelrij $(f(a_{r(n)}))_{n\geqslant 0}$ van $(f(a_n))_{n\geqslant 0}$. Tegelijkertijd is m een limiet van de volledige rij. Dus $m = f(a)$. ■

Opgaven

1. Zij $f : V \to \mathbb{R}^n$ een functie met $V \subseteq \mathbb{R}^m$ gesloten. Stel dat $a \in \mathbb{R}^m$ maar $a \notin V$. Bewijs dat voor alle $b \in \mathbb{R}^n$ geldt

$$\lim_{x\to a} f(x) = b.$$

Geef ook een voorbeeld waaruit duidelijk wordt dat de eis dat V gesloten is noodzakelijk is.

2. Laat $D \subseteq \mathbb{R}$, $f, g : D \to \mathbb{R}$, en $a \in \mathbb{R}$. Neem aan dat $\lim_{x\to a} f(x) = L$ en $\lim_{x\to a} g(x) = M$. Dan

(a) $\lim_{x\to a}(f(x) + g(x)) = L + M$.

(b) $\lim_{x\to a}(\alpha \cdot f(x)) = \alpha \cdot M$ voor $\alpha \in \mathbb{R}$.

(c) $\lim_{x\to a}(f(x) \cdot g(x)) = L \cdot M$.

(d) Als $M \neq 0$, dan $\lim_{x\to a} 1/g(x) = 1/M$.

(e) $\lim_{x\to a} |f(x)| = |L|$.

3. Bewijs aan de hand van de definitie van continuïteit dat de functie $f : \mathbb{R} \to \mathbb{R}$ gedefinieerd door $f(x) = x^2$ continu is:

(a) in het punt 0;

(b) in het punt -1;

✍ (c) op $\mathbb{R}$.

4. Toon aan dat de functie $f : \mathbb{R} \to \mathbb{R}$, gegeven door

$$f(x) = x^2 + \frac{1}{1+x^2}$$

continu is. Gebruik de 'rekenregels' voor continuïteit.

✍ **5.** Is de functie $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ gedefinieerd door

$$f(x) = 1/x$$

continu?

6. Bewijs met behulp van de definitie van de continuïteit dat de functie $f : [0,\infty) \to \mathbb{R}$ gegeven door $f(x) = \sqrt{x}$ continu is.

✍ **7.** Zij $D \subseteq \mathbb{R}$ en $c \in D$, en laat $f : D \to \mathbb{R}$ functie zijn die continu is in c. Bewijs of weerleg;

(a) Als $f(c) > 0$, dan bestaat er een $\delta > 0$ zó dat voor alle $x \in D$ met $|x - c| < \delta$ geldt dat $f(x) \geq 0$

(b) Als $f(c) \geq 0$, dan bestaat er een $\delta > 0$ zó dat voor alle $x \in D$ met $|x - c| < \delta$ geldt dat $f(x) \geq 0$

Rekenregels voor continuïteit

8. Zij $V \subseteq \mathbb{R}$. Als $f : V \to \mathbb{R}$ en $g : V \to \mathbb{R}$ twee functies zijn die continu zijn in het punt $c \in V$, en $\alpha \in \mathbb{R}$ is een reëel getal. Bewijs:

(a) αf is continu in c.

(b) $f + g$ is continu in c.

(c) fg is continu in c.

(d) Als $f(x) \neq 0$ voor alle $x \in D$, dan is $1/f$, $x \mapsto 1/f(x)$ continu in c.

(e) $|f|$ is continu in c.

9. Bewijs dat de samenstelling van continue functies weer continu is.

10. Bewijs: een functie $f : V \to \mathbb{R}^n$ (met $V \subseteq \mathbb{R}^m$) is continu in $a \in V$ precies dan als voor iedere convergente rij $(a_n)_{n \geqslant 0}$ in V met limiet $a \in V$ geldt dat $(f(a_n))_{n \geqslant 0}$ convergeert met limiet $f(a)$.

11. Bewijs met behulp van de definitie dat $\lim_{x \to a} f(x)$ bestaat als

(a) $a = -1$, en $f : \mathbb{R} \setminus \{-1\} \to \mathbb{R}$ gegeven door $f(x) = (x^2 - 1)/(x + 1)$;

(b) $a = 2$, en $f : \mathbb{R} \setminus \{1, 2\} \to \mathbb{R}$ gegeven door $f(x) = (x^3 - 3x - 2)/(x^2 - 3x + 2)$;

(c) $a = 0$, en $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ gegeven door $f(x) = (x^2 + x)/x$.

✍ **12.** Definieer $f : (-1, 1) \to \mathbb{R}$ door

$$f(x) = \begin{cases} 0, & x \neq 0; \\ 1, & x = 0. \end{cases}$$

(a) Bestaat $\lim_{x \to 0} f(x)$? Zo ja, wat is de waarde van de limiet? Zo nee, waarom niet?

(b) Is f continu in 0?

✍ **13.** Laat $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, $x \mapsto 1/x$. Bewijs dat $\lim_{x \to 0} f(x)$ niet bestaat met behulp van Opgave VI.5.10.

14. Laat $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, $x \mapsto x/|x|$. Bepaal of de $\lim_{x \to 0} f(x)$ bestaat.

✍ **15.** Je bent uit de analyse waarschijnlijk bekend met eenzijdige limieten

$$\lim_{x \uparrow a} f(x) \qquad \text{en} \qquad \lim_{x \downarrow a} f(x).$$

Geef hier een 'epsilon-delta-definitie' van.

VI.6 Het getalsysteem van complexe getallen

Ter herinnering: een lichaam F is algebraïsch gesloten als ieder polynoom van positieve graad met coëfficiënten in F een nulpunt heeft. Het lichaam $\mathbb{R}$ is niet algebraïsch gesloten: $x^2+1=0$ heeft bijvoorbeeld geen oplossing $x \in \mathbb{R}$.

We hebben in Hoofdstuk V de opmerking gemaakt dat ieder lichaam een uitbreiding heeft die algebraïsch gesloten is. Voor $\mathbb{R}$ kennen we die algebraïsche afsluiting: het lichaam van complexe getallen $\mathbb{C}$. Het bijzondere is dat $\mathbb{C}$ bovendien ook nog eens compleet is onder de standaardmetriek $|a+bi| = \sqrt{a^2+b^2}$ — als metrische ruimte is $\mathbb{C}$ immers gewoon $\mathbb{R}^2$.

We hebben de constructie van $\mathbb{C}$ in feite al in hoofdstuk V uitgevoerd:

$$\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[X]/(X^2+1).$$

Wat rest is te bewijzen dat $\mathbb{C}$ algebraïsch gesloten is. Een formeel bewijs valt buiten het bestek van deze tekst, maar we zullen er nu een vrij gedetailleerde opmerking over maken.

VI.6.1 Opmerking. We moeten bewijzen: iedere veelterm van positieve graad

$$f(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 \qquad (\text{met } a_n \neq 0 \text{ en } n \geqslant 1)$$

met complexe coëfficiënten $(a_0, a_1, \ldots, a_n \in \mathbb{C})$ heeft een nulpunt.

Bewijsschets. We mogen aannemen dat $a_n = 1$. Bekijk de familie van cirkels

$$C_r = \{z \in \mathbb{C} : |z| = r\}.$$

met straal $r \geqslant 0$ om de oorsprong in het complexe vlak.

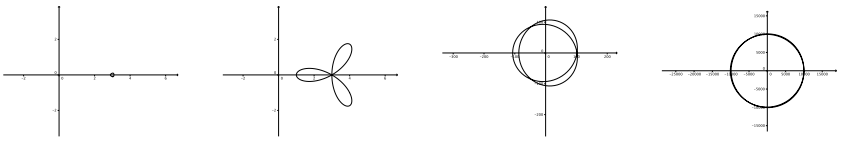
- Als $r = 0$ dan is deze 'cirkel' een punt; het beeld $f(C_r)$ is dus ook een punt A in het complexe vlak. Als $A = 0$ dan zijn we klaar. Neem vanaf nu dus aan dat $A \neq 0$.
- Voor een complex getalen z dat ver van de oorsprong ligt, geldt $f(z) \approx z^n$ (preciezer: $f(z) = z^n + \mathcal{O}(z^{n-1})$). Als de straal r heel groot is, is het beeld dus bij benadering een cirkel om de oorsprong (met een gigantische straal).

Bekijk nu het beeld van C_r als r gestaag toeneemt van 0 tot ∞. Je begint met een klein figuurtje bij punt A dat geleidelijk uitdijt tot je iets krijgt wat er bij benadering uitziet als een steeds groter wordende cirkel om de oorsprong. Omdat A buiten de oorsprong ligt, zal het beeld op een bepaald moment *door de oorsprong moeten gaan*.

Er is dus een straal r zodat $0 \in f(C_r)$. Maar voor een punt z op C_r geldt dan dus $f(z) = 0$. Dit is het gezochte nulpunt.

Hier staan de beelden van de cirkels met aangeven straal r voor een specifieke keuze van f. Let op de verandering van de schaal!

$r = 0{,}1$ $\qquad$ $r = 1$ $\qquad$ $r = 10$ $\qquad$ $r = 100$



VII LINEAIRE ALGEBRA

In dit hoofdstuk behandelen we de basis-resultaten van de lineaire algebra. We gaan ervan uit dat de lezer ervaring heeft met de reële vectorruimten $\mathbb{R}^n$ en lineaire afbeeldingen, met inproducten en afstanden in $\mathbb{R}^n$, met matrices met reële coëfficiënten, en met het oplossen van stelsels lineaire vergelijkingen door 'vegen', ook wel Gauss-eliminatie genoemd. Het gaat in dit hoofdstuk om de onderliggende theorie, nodig als voorkennis voor de andere lerarencolleges van Mastermath, denk aan algebra, getaltheorie en meetkunde. Maar ook aan analyse, waar het essentieel is om verzamelingen van $\mathbb{R}$-waardige functies te bekijken als vectorruimte over $\mathbb{R}$, en vervolgens eigenschappen van lineaire afbeeldingen te gebruiken. Dit soort vectorruimten zijn meestal oneindig-dimensionaal, en hebben niet een bij voorbaat gegeven basis. Ook de oplossingsruimte van een systeem lineaire vergelijkingen (bijvoorbeeld $\{(x,y) \in \mathbb{R}^2 : x + y = 0\}$) heeft geen gegeven basis. Hierom, en omdat het bij het kiezen van een basis belangrijk is om die geschikt te kiezen voor de vragen die moeten worden beantwoord, is het belangrijk om de theorie op te bouwen voor abstracte vectorruimten. Dat is ook natuurlijker en het vergroot de toepasbaarheid omdat alle resultaten uit een klein aantal axioma's worden afgeleid.

We kiezen er dan ook meteen voor om de theorie te formuleren voor vectorruimten over willekeurige lichamen. Het begrip 'lichaam' is ingevoerd in hoofdstuk V in Definitie V.1.4. Dit maakt het mogelijk om de theorie toe te passen over $\mathbb{F}_2$, op de welbekende 'lights out' puzzel.

VII.1 Vectorruimten over lichamen

Vectoren kan men optellen en vermenigvuldigen met scalairen. Deze scalairen komen uit een lichaam dat daarom gespecificeerd moet worden. De term 'vectorruimte' zonder meer is zinloos, en iemand die die term toch gebruikt dient direct de vraag te krijgen "Over welk lichaam?" Voor dit lichaam gebruiken we hier bij voorkeur de letter 'F', omdat 'lichaam' in het Engels 'field' is. In Vlaanderen is de gebruikte term 'veld'.

Definitie vectorruimte

VII.1.1 Definitie. Laat $(F, 0, 1, +, \cdot)$ een lichaam zijn. Een *vectorruimte over F*, of ook *F-vectorruimte*, is een systeem $(V, 0, +, \cdot)$, met $0 \in V$, $+ : V \times V \to V$, $(v, w) \mapsto v + w$, $\cdot : F \times V \to V$, $(\lambda, v) \mapsto \lambda \cdot v$, dat voldoet aan de volgende axioma's

V0 $\forall v, w \in V,\ v + w = w + v$ (optelling is commutatief);
V1 $\forall v, w, x \in V,\ (v + w) + x = v + (w + x)$ (optelling is associatief);

V2 $\forall v \in V,\ v + 0 = v$ (0 is neutraal voor de optelling);
V3 $\forall v \in V,\ \exists w \in V,\ v + w = 0$ (bestaan van additieve inverse);
V4 $\forall \lambda, \mu \in F,\ \forall v \in V,\ \lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v$ (associativiteit van vermenigvuldiging);
V5 $\forall v \in V,\ 1 \cdot v = v$ (vermenigvuldiging met 1 is de identiteit);
V6 $\forall \lambda \in F,\ \forall v, w \in V,\ \lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$ (distributiviteit in 2e variabele);
V7 $\forall \lambda, \mu \in F,\ \forall v \in V,\ (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ (distributiviteit in 1e variabele).

Voorbeeld F^n

VII.1.2 Voorbeeld. De simpelste voorbeelden zijn de F-vectorruimten F^n, waar n een natuurlijk getal is. De verzameling vectoren is F^n, de verzameling van n-tupels $v = (v_1, \ldots, v_n)$ met de v_i in F. Het nul-element is $(0, \ldots, 0)$. De optelling is coordinaatsgewijs:

$$(v_1, \ldots, v_n) + (w_1, \ldots, w_n) = (v_1 + w_1, \ldots, v_n + w_n).$$

De scalairvermenigvuldiging is ook coordinaatsgewijs:

$$\lambda \cdot (v_1, \ldots, v_n) = (\lambda v_1, \ldots, \lambda v_n).$$

De lichaamseigenschappen van F impliceren direct dat aan V0–V7 is voldaan. Iedere $(v_1, \ldots, v_n)$ heeft een unieke additieve inverse, namelijk $(-v_1, \ldots, -v_n)$. ∎

VII.1.3 Opmerking. Het kan verwarrend zijn dat de nul-elementen van F en V beide als 0 worden genoteerd. Om onderscheid te maken noteren we ze als 0_F en 0_V als we dat nodig vinden. Hetzelfde geldt voor de optelling in F en in V: $+_F$ en $+_V$. De scalairvermenigvuldiging noteren we ook als $(\lambda, v) \mapsto \lambda v$.

De axioma's V0–V4 betekenen dat $(V, 0, +)$ een additief genoteerde *commutatieve groep* is. Wie deze term nog niet kent kan het als definitie nemen.

Meestal zullen we $(V, 0, +, \cdot)$ als V noteren, als het duidelijk is wat de rest is.

Voorbeeld functieruimte

VII.1.4 Voorbeeld. Laat F een lichaam zijn, X een verzameling, en V de verzameling van alle functies $f : X \to F$. Dan kunnen elementen van V *puntsgewijs* worden opgeteld: we definiëren $+ : V \times V \to V$ door voor f en g in V te definiëren dat, voor alle $x \in X$, $(f+g)(x) = f(x) + g(x)$. Verder definiëren we $\cdot : F \times V \to V$ door $(\lambda, f) \mapsto \lambda \cdot f$ door puntsgewijs te vermenigvuldigen: $\forall x \in X$, $(\lambda \cdot f)(x) = \lambda f(x)$, waarbij de laatste vermenigvuldiging die van λ en $f(x)$ in F is. De nulfunctie $0 : X \to F$, $x \mapsto 0$ is neutraal voor de optelling. Men gaat eenvoudig na dat $(V, 0, +, \cdot)$ een F-vectorruimte is (Opgave VII.1.1).

Als $n \in \mathbb{N}$ en we voor X een verzameling $\{1, 2, \ldots, n\}$ nemen, dan hebben we de bijectie

$$\varphi : V \to F^n, \quad f \mapsto (f(1), f(2), \ldots, f(n)).$$

Deze bijectie φ is compatibel met de optelling: voor alle f en g in V geldt dat $\varphi(f + g) = \varphi(f) + \varphi(g)$, en met de scalairvermenigvuldiging: voor alle $\lambda \in F$ en alle $f \in V$ geldt $\varphi(\lambda f) = \lambda \varphi(f)$ (bewijs: Opgave VII.1.2). We zien dus dat het verschil tussen V en F^n slechts 'administratief' is (de vertaling in notatie wordt gedaan door φ).

De notatie Y^X voor $\{f : X \to Y\}$

Een les die we hieruit kunnen leren is dat het handig kan zijn om n-tupels van elementen in een willekeurige verzameling F te definiëren als functies van $\{1, 2, \ldots, n\}$ naar F, en dat het handig kan zijn om deze verzameling te noteren als $F^{\{1,2,\ldots,n\}}$. Sterker, het is handig om voor willekeurige verzamelingen X en Y de verzameling van functies $f : X \to Y$ te noteren als Y^X. ∎

Rekenregels

Alle rekenregels voor F-vectorruimten volgen uit de axioma's. We geven er een paar.

VII.1.5 Stelling. Laat F een lichaam zijn, en $(V, 0, +, \cdot)$ een F-vectorruimte. Dan gelden de volgende uitspraken.

1. Het nulelement is het unieke element van V dat neutraal is voor de optelling: als $0' \in V$ en $\forall v \in V,\ v + 0' = v$ dan $0' = 0$.
2. Additieve inversen zijn uniek: voor iedere $v \in V$ is er een unieke $w \in V$ met $v + w = 0$; we noteren deze w als $-v$.
3. Voor alle v in V: $-v = (-1)\cdot v$.
4. Voor alle $v \in V$: $0 \cdot v = 0$.
5. Voor alle $\lambda \in F$: $\lambda \cdot 0 = 0$.
6. Voor alle $\lambda \in F$ met $\lambda \neq 0$ en voor alle $v \in V$: $\lambda^{-1} \cdot (\lambda \cdot v) = v$.

Bewijs. Dat is Opgave VII.1.4. ∎

Deelruimten

Laat F een lichaam zijn, en V een F-vectorruimte.

VII.1.6 Definitie. Een *deelruimte*, of, precieser, *deel-F-vectorruimte* van V is een deelverzameling W van V met de eigenschap dat beperken van de optelling tot $W \times W$ en de scalairvermenigvuldiging tot $F \times W$ een F-vectorruimte structuur op W geeft met nulement dat van V.

VII.1.7 Stelling. Laat W een deelverzameling van V zijn. De volgende uitspraken zijn equivalent:

(a) W is een deel-F-vectorruimte;
(b) $0 \in W$ en $(\forall w_1, w_2 \in W,\ w_1 + w_2 \in W)$ en $(\forall \lambda \in F,\ \forall w \in W,\ \lambda w \in W)$.

Bewijs. We bewijzen dat '(b) impliceert (a)'. De aanname zegt dat $+|_{W\times W}$ en $\cdot|_{F\times W}$ afbeeldingen naar W geven. Aan alle eisen V0–V7 behalve misschien V3 is voldaan omdat die voor V gelden. Aan V3 is is voldaan omdat voor $w \in W$ de additieve inverse in V gelijk is aan $(-1)\cdot w$ en dus in W zit.

Dat '(a) impliceert (b)' is triviaal. ∎

Doorsnede deelruimten

VII.1.8 Stelling. Laat I een verzameling zijn, en voor iedere $i \in I$ laat W_i een deel-F-vectorruimte van V zijn. Dan is $\cap_{i\in I} W_i$ een deel-F-vectorruimte van V.

Bewijs. Opgave VII.1.6. ∎

Deelruimte voortgebracht door S

VII.1.9 Stelling. Laat S een deelverzameling van V, en laat

$$W = \{v \in V : \exists n \in \mathbb{N}, \exists v_1, \ldots, v_n \in S, \exists \lambda_1, \ldots, \lambda_n \in F, \lambda_1 v_1 + \cdots + \lambda_n v_n = v\}.$$

(a) W is een deel-F-vectorruimte van V, en $S \subseteq W$.
(b) W is de kleinste deel-F-vectorruimte van V die S bevat: als U een deel-F-vectorruimte van V is met $S \subseteq U$, dan $W \subseteq U$.
(c) W is de doorsnede van alle deel-F-vectorruimten van V die S bevatten.

Deze deelruimte W noemen we de *deelruimte voortgebracht door S*, en we noteren haar $\langle S \rangle$.

Bewijs. Opgave VII.1.7. ∎

Opgaven

✍ **1.** Laat F en $(V,0,+,\cdot)$ gedefiniëerd zijn als in Voorbeeld VII.1.4.

(a) Laat zien dat $(V,0,+,\cdot)$ een F-vectorruimte is.

(b) Bepaal voor f in V de additieve inverse.

(c) Stel dat we de scalairvermenigvuldiging definiëren als $(\lambda\cdot f)(x)=0$. Is $(V,0,+,\cdot)$ dan een F-vectorruimte?

(d) Wat is V als $X=\varnothing$?

(e) Kan een F-vectorruimte leeg zijn?

2. Bewijs de uitspraken over φ in Voorbeeld VII.1.4. Dit is vooral een oefening in notatie, er 'gebeurt' eigenlijk niets.

3. (a) Laat zien dat $(\mathbb{R},0,+)$ samen met de beperking van z'n vermenigvuldiging tot $\mathbb{Q}\times\mathbb{R}\to\mathbb{R}$ een $\mathbb{Q}$-vectorruimte vormt.

(b) Analoog voor $\mathbb{C}$ en $\mathbb{R}$.

4. Bewijs alle uitspraken in Stelling VII.1.5.

✍ **5.** We definiëren $V=\mathbb{R}$ met $+_V: V\times V\to V$, $(v,w)\mapsto v+_w -1$ en met $\cdot_V:\mathbb{R}\times V\to V$, $(\lambda,v)\mapsto \lambda x-\lambda+1$.

(a) Is er een $0_V\in V$ zodat $(V,0_V,+_V,\cdot_V)$ een $\mathbb{R}$-vectorruimte is? En wat is dan 0_V?

(b) Waarom is dit een 'flauw' voorbeeld? Kun je er nog wel meer verzinnen?

6. Bewijs Stelling VII.1.8.

7. Bewijs Stelling VII.1.9.

8. Laat V de verzameling zijn van alle functies $f:\mathbb{R}\to\mathbb{R}$, voorzien van puntsgewijze optelling en scalairvermenigvuldiging als in Voorbeeld VII.1.4 (met $F=\mathbb{R}$ en $V=\mathbb{R}$). Laat zien dat de deelverzameling D van V bestaand uit de differentiëerbare functies een deel-F-vectorruimte is.

VII.2 Lineaire afbeeldingen

Laat F een lichaam zijn. Omdat er in deze sectie alleen F-vectorruimten voorkomen noemen we F-vectorruimten gewoon vectorruimten.

Definitie lineaire afbeelding, $\mathrm{Hom}(V,W)$

VII.2.1 Definitie. Laat V en W vectorrruimten, en $f:V\to W$ een afbeelding. Dan noemen we f *lineair* als gelden:

(L0) $\forall v_1,v_2\in V,\ f(v_1+v_2)=f(v_1)+f(v_2)$;
(L1) $\forall\lambda\in F,\ \forall v\in V,\ f(\lambda v)=\lambda f(v)$.

De *verzameling* van lineaire afbeeldingen van V naar W noteren we $\mathrm{Hom}(V,W)$.

VII.2.2 Opmerking. In L0 is de eerste '+' die in V, en de tweede die in W. In L1 is de eerste scalairvermenigvuldiging die in V en de tweede die in W.

Voor $f:V\to W$ lineair geldt $f(0)=f(0\cdot 0)=0\cdot f(0)=0$ (waarin 0 achtereenvolgens in V, F, V, F, V en W zit).

In het onderwijs heten functies $f:\mathbb{R}\to\mathbb{R}$ van de vorm $x\mapsto ax+b$ lineaire functies. Merk op dat met de definitie hierboven alleen de $x\mapsto ax$ lineair zijn. De functies van de vorm $x\mapsto ax+b$ noemen we *affiene functies*.

Lineair belangrijk

Lineaire afbeeldingen zijn zo belangrijk omdat ze veel voorkomen (altijd als het 'gevolg' van een proces lineair afhangt van de 'oorzaak') en bovendien zo eenvoudig zijn dat er veel over te zeggen is. Zelfs als afbeeldingen niet lineair zijn kijkt men vaak naar benaderingen die dat wel zijn (denk aan differentiëren).

Primitiveren is lineair

VII.2.3 Voorbeeld. We nemen $F = \mathbb{R}$ en $X = \mathbb{R}$ in Voorbeeld VII.1.4. Dat geeft ons de $\mathbb{R}$-vectorruimte van alle functies $f : \mathbb{R} \to \mathbb{R}$. We laten $D \subseteq V$ de deelruimte zijn van alle differentiëerbare functies, en net zo C de deelruimte van alle continue functies. Dan blijken enige gebruikelijke operaties in de analyse lineaire afbeeldingen te zijn (bewijs: Opgave VII.2.1).

1. De afbeelding 'differentiëer', $d : D \to V$, $f \mapsto f'$ is lineair.
2. De afbeelding 'primitiveer', $p : C \to D$, $(p(f))(x) = \int_0^x f(t)\,dt$ is p lineair.
3. Voor iedere $a \in \mathbb{R}$ is de afbeelding 'verschuif a naar links', $v_a : V \to V$, gegeven door $(v_a(f))(x) = f(x+a)$ lineair.

∎

We gaan nu over op een eenvoudiger soort voorbeeld: lineaire afbeeldingen van F^m naar een vectorruimte W, en lineaire afbeeldingen van F^m naar F^n. In dit voorbeeld introduceren we ook wat terminologie en komen we vanzelf op het begrip 'matrix' en op de vermenigvuldiging van matrices. We beginnen met een 'laagdimensionaal' voorbeeld.

Lineaire $f : F^3 \to F^2$

VII.2.4 Voorbeeld. Laat $f : F^3 \to F^2$ een lineaire afbeelding zijn. We schrijven

$$f(1,0,0) = (f_{1,1}, f_{2,1}), \quad f(0,1,0) = (f_{1,2}, f_{2,2}), \quad f(0,0,1) = (f_{1,3}, f_{2,3}).$$

Voor alle (x_1, x_2, x_3) in F^3 geldt dan

$$\begin{aligned} f(x_1,x_2,x_3) &= f((x_1,0,0)+(0,x_2,0)+(0,0,x_3)) \\ &= f(x_1\cdot(1,0,0)+x_2\cdot(0,1,0)+x_3\cdot(0,0,1)) \\ &= x_1\cdot f(1,0,0)+x_2\cdot f(0,1,0)+x_3\cdot f(0,0,1) \\ &= x_1\cdot(f_{1,1},f_{2,1})+x_2\cdot(f_{1,2},f_{2,2})+x_3\cdot(f_{1,3},f_{2,3}) \\ &= (f_{1,1}x_1+f_{1,2}x_2+f_{1,3}x_3, f_{2,1}x_1+f_{2,2}x_2+f_{2,3}x_3). \end{aligned}$$

Kennelijk is iedere lineaire $f : F^3 \to F^2$ van deze eenvoudige vorm. Het omgekeerde geldt ook. Voor $(a_{1,1}, a_{2,1}, a_{1,2}, a_{2,2}, a_{1,3}, a_{2,3})$ in F^6 is de afbeelding

$$f_a : F^3 \to F^2, \quad (x_1,x_2,x_3) \mapsto (a_{1,1}x_1+a_{1,2}x_2+a_{1,3}x_3, a_{2,1}x_1+a_{2,2}x_2+a_{2,3}x_3)$$

lineair: er is voldaan aan L0 en L1. We hebben een bijectieve afbeelding gevonden van $\mathrm{Hom}(F^3, F^2)$ naar F^6.

Om formules als hierboven overzichtelijker te presenteren/visualiseren wordt het begrip matrix ingevoerd: het is beter de $f_{i,j}$ tezamen in een rechthoek van 2 bij 3 te zetten dan in een 6-tupel (waarvan voor de volgorde dan een keuze moet worden afgesproken). De afbeelding f_a komt er dan als volgt uit te zien:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} a_{1,1}x_1+a_{1,2}x_2+a_{1,3}x_3 \\ a_{2,1}x_1+a_{2,2}x_2+a_{2,3}x_3 \end{pmatrix}.$$

De punt tussen de 2 bij 3 matrix en de kolomvector staat voor de nog te definiëren vermenigvuldiging van matrices. Merk op dat de kolommen van de matrix de beelden zijn van de vectoren $(1,0,0)$, $(0,1,0)$ en $(0,0,1)$. ∎

Matrix, rijen, kolommen $0_{m,n}$ en 1_n

VII.2.5 Definitie. Laat $m,n \in \mathbb{N}$. Een *m-bij-n matrix met coëfficiënten in F is een functie* $a\colon \{1,\dots,m\}\times\{1,\dots,n\} \to F$, $(i,j)\mapsto a_{i,j}$, ook wel genoteerd als

$$a = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix}.$$

De verzameling van m-bij-n matrices met coëfficiënten in F noteren we $\mathrm{M}_{m,n}(F)$, en als $n=m$ ook als $\mathrm{M}_n(F)$.

Een element a in $\mathrm{M}_{m,n}(F)$ heeft m *rijen*, die we al naar gelang het ons uitkomt kunnen opvatten als 1-bij-n matrices (ook wel *rijvectoren* genoemd) of elementen van F^n, en n *kolommen*, die we kunnen opvatten als m-bij-1 matrices (ook wel *kolomvectoren* genoemd) of elementen van F^m.

We definiëren het element $0_{m,n} \in \mathrm{M}_{m,n}(F)$ als de matrix waarvan alle coëfficiënten 0 zijn. Als $n=m$ definiëren we $1_n \in \mathrm{M}_n(F)$ door: $\forall (i,j)\in\{1,\dots,n\}\times\{1,\dots,m\}$, $(1_n)_{i,j} = 1$ als $i=j$ en 0 anders.

Coördinaten in F^n

Laat nu $n\in\mathbb{N}$. Voor v in F^n schrijven we de $i$de coordinaat v_i, dus dan geldt:

$$v = (v_1,\dots,v_n).$$

Dan geldt voor iedere v in F^n dat

$$\begin{aligned} v = (v_1,\dots,v_n) &= (v_1,0,\dots,0)+\dots+(0,\dots,0,v_n) \\ &= v_1\cdot(1,0,\dots,0)+\dots+v_n\cdot(0,\dots,0,1). \end{aligned}$$

Om dit soort uitdrukkingen makkelijker op te schrijven noteren we voor $i\in\{1,\dots,n\}$ met $e_i = (e_{i,1},\dots,e_{i,n})$ het element van F^n met

$$\begin{aligned} e_{i,j} &= 1 \quad \text{als } i=j, \\ e_{i,j} &= 0 \quad \text{als } i\neq j. \end{aligned} \tag{VII.1}$$

Coördinaten en standaardbasis $e_1,\dots,e_n$ in F^n

Deze elementen $e_i \in F^n$ heten de *standaard basisvectoren in F^n*. De definitie van basis van een vectorruimte wordt gegeven in Definitie VII.3.6; hier hebben we die nog niet nodig. Met deze notatie geldt dan

$$\forall v\in F^n,\quad v = v_1e_1+\dots+v_ne_n = \sum_{i=1}^{n} v_ie_i. \tag{VII.2}$$

De matrix $\mathrm{mat}_{\mathrm{st}}(f)$ van een lineaire $f\colon F^n\to F^m$

VII.2.6 Definitie. Laat $m,n\in\mathbb{N}$ en $f\colon F^n\to F^m$ lineair. Dan definiëren we $\mathrm{mat}_{\mathrm{st}}(f)$ in $\mathrm{M}_{m,n}(F)$ door:

$$\forall (i,j)\in\{1,\dots,m\}\times\{1,\dots,n\}, \mathrm{mat}_{\mathrm{st}}(f)_{i,j} = f(e_j)_i.$$

In woorden: de (i,j)-coëfficiënt van $\mathrm{mat}_{\mathrm{st}}(f)$ is de i-de coördinaat van het beeld onder f van het j-de element van de standaardbasis van F^n; de j-de kolom van $\mathrm{mat}_{\mathrm{st}}(f)$ is $f(e_j)$. We noemen $\mathrm{mat}_{\mathrm{st}}(f)$ de *matrix van f ten opzichte van de standaardbases van F^n en F^m*.

Bijectie tussen $\mathrm{Hom}(F^n,W)$ en W^n

VII.2.7 Propositie. Laat $n\in\mathbb{N}$ en laat W een vectorruimte zijn. Dan is de afbeelding

$$\mathrm{Hom}(F^n,W)\to W^n,\quad f\mapsto (f(e_1),\dots,f(e_n))$$

een bijectie.

Bewijs. We laten zien dat er voor iedere $w = (w_1, \ldots, w_n) \in W^n$ een unieke lineaire afbeelding $f : F^n \to W$ is zodat voor alle j in $\{1, \ldots, n\}$ geldt dat $f(e_j) = w_j$.

Laat $w = w \in W^n$. Laat $f : F^n \to W$ de afbeelding zijn die gegeven is door het voorschrift

$$f(v) = \sum_{j=1}^{n} v_j w_j.$$

We bewijzen dat f lineair is. Volgens Opgave VII.2.3 is het voldoende te bewijzen dat voor alle v en v' in V en voor alle λ in F geldt dat $f(v + \lambda v') = f(v) + \lambda f(v')$. Laat $v, v' \in V$ en $\lambda \in F$. Dan geldt

$$\begin{aligned}
f(v + \lambda v') &= f((v_1, \ldots, v_n) + \lambda(v'_1, \ldots, v'_n)) \\
&= f((v_1, \ldots, v_n) + (\lambda v'_1, \ldots, \lambda v'_n)) \\
&= f((v_1 + \lambda v'_1, \ldots, v_n + \lambda v'_n)) \\
&= (v_1 + \lambda v'_1)w_1 + \cdots + (v_n + \lambda v'_n)w_n \\
&= v_1 w_1 + \lambda v'_1 w_1 + \cdots + v_n w_n + \lambda v'_n w_n \\
&= v_1 w_1 + \cdots v_n w_n + \lambda v'_1 w_1 + \cdots + \lambda v'_n w_n \\
&= v_1 w_1 + \cdots v_n w_n + \lambda(v'_1 w_1 + \cdots + v'_n w_n) \\
&= f(v) + \lambda f(v').
\end{aligned}$$

De afbeelding f is dus inderdaad lineair. Voor iedere $j \in \{1, \ldots, n\}$ geldt dat $f(e_j) = w_j$.

Neem nu aan dat $g : F^n \to W$ lineair is met $\forall j \in \{1, \ldots, n\}, g(e_j) = w_j$. Dan geldt voor iedere $v \in F^n$

$$g(v) = g\left(\sum_{j=1}^{n} v_j e_j\right) = \sum_{j=1}^{n} v_j g(e_j) = \sum_{j=1}^{n} v_j w_j = f(v).$$

Dus $g = f$. ∎

Bijectie tussen $\mathrm{Hom}(F^n, F^m)$ en $\mathrm{M}_{m,n}(F)$

VII.2.8 Propositie. Laat $m, n \in \mathbb{N}$. Dan is de afbeelding

$$\mathrm{mat}_{\mathrm{st}} : \mathrm{Hom}(F^n, F^m) \to \mathrm{M}_{m,n}(F), \quad f \mapsto \mathrm{mat}_{\mathrm{st}}(f)$$

een bijectie.

Bewijs. Dit volgt uit Propositie VII.2.7 toegepast met $W = F^m$. ∎

Operaties op lineaire afbeeldingen

We hebben nu gezien dat m-bij-n matrices met coëfficiënten in F corresponderen met lineaire afbeeldingen $F^n \to F^m$. Daaruit volgt dan dat operaties op lineaire afbeeldingen leiden tot operaties op matrices. Om hiervan te profiteren voeren we nu een aantal operaties op lineaire afbeeldingen in. Daarna bekijken we wat de corresponderende operaties op matrices zijn, en leiden we eigenschappen van die operaties af.

VII.2.9 Stelling.
1. Laat V, W en U vectorruimten zijn, en $f : V \to W$ en $g : W \to U$ lineaire afbeeldingen. Dan is $g \circ f : V \to U$ lineair.
2. Laat V en W vectorruimten zijn, en $f : V \to W$ een lineaire afbeelding die bijectief is. Dan is $f^{-1} : W \to V$ lineair.
3. Laat V en W vectorruimten zijn, f en g lineaire afbeeldingen van V naar W. Dan is voor elke $\lambda \in F$ de afbeelding $f + \lambda g : V \to W$, $v \mapsto f(v) + \lambda g(v)$ lineair.
4. Laat V en W vectorruimten zijn. Dan is de verzameling $\mathrm{Hom}(V, W)$ van lineaire afbeeldingen van V naar W, met de puntsgewijze optelling en scalairvermenigvuldiging als in onderdeel 3 een vectorruimte.
5. Laat V, W en U vectorruimten zijn, $f, g : V \to W$, $h : W \to U$, en $\lambda \in F$. Dan geldt $h \circ (f + \lambda g) = h \circ f + \lambda(h \circ g)$.

6. Laat V, W en U vectorruimten zijn, $h: V \to W$, $f, g: W \to U$, en $\lambda \in F$. Dan geldt $(f + \lambda g) \circ h = f \circ h + \lambda(g \circ h)$.

Bewijs. We bewijzen alleen 2, de andere onderdelen zijn Opgave VII.2.4. We hebben dus de afbeelding $f^{-1}: W \to V$, waarvan we willen bewijzen dat-ie lineair is. We geven twee bewijzen, het 2e wat formeler dan het 1e.

Bewijs 1. Laat $w_1, w_2 \in W$, en $\lambda \in F$. Omdat f bijectief is zijn er unieke v_1 en v_2 in V met $w_1 = f(v_1)$ en $w_2 = f(v_2)$: dit zijn $f^{-1}(w_1)$ en $f^{-1}(w_2)$. Dan geldt

$$w_1 + \lambda w_2 = f(v_1) + \lambda f(v_2) = f(v_1 + \lambda v_2),$$

waar de 2e gelijkheid volgt uit de lineariteit van f. Dan zijn ook de beelden onder f^{-1} van $w_1 + \lambda w_2$ en $f(v_1 + \lambda v_2)$ gelijk:

$$f^{-1}(w_1 + \lambda w_2) = f^{-1}(f(v_1 + \lambda v_2)) = v_1 + \lambda v_2 = f^{-1}(w_1) + \lambda f^{-1}(w_2).$$

Bewijs 2. Laat $w_1, w_2 \in W$, en $\lambda \in F$. Dan geldt

$$\begin{aligned}
w_1 = f(f^{-1}(w_1)) \wedge w_2 = f(f^{-1}(w_2)) &\quad \text{definitie inverse functie} \\
w_1 + \lambda w_2 = f(f^{-1}(w_1)) + \lambda f(f^{-1}(w_2)) &\quad \text{volgt uit regel 1} \\
f(f^{-1}(w_1)) + \lambda f(f^{-1}(w_2)) = f\left(f^{-1}(w_1) + \lambda f^{-1}(w_2)\right) &\quad \text{lineariteit van } f \\
w_1 + \lambda w_2 = f\left(f^{-1}(w_1) + \lambda f^{-1}(w_2)\right) &\quad \text{regels 2 en 3} \\
f^{-1}(w_1 + \lambda w_2) = f^{-1}\left(f\left(f^{-1}(w_1) + \lambda f^{-1}(w_2)\right)\right) &\quad f^{-1} \text{ op regel 4} \\
f^{-1}\left(f\left(f^{-1}(w_1) + \lambda f^{-1}(w_2)\right)\right) = f^{-1}(w_1) + \lambda f^{-1}(w_2) &\quad \text{definitie inverse functie} \\
f^{-1}(w_1 + \lambda w_2) = f^{-1}(w_1) + \lambda f^{-1}(w_2) &\quad \text{regels 5 en 6}
\end{aligned}$$

■

Matrix-vermenigvuldiging

Laat $n, m, l \in \mathbb{N}$, $a \in \mathrm{M}_{l,m}(F)$ en $b \in \mathrm{M}_{m,n}(F)$. Vanwege Propositie VII.2.8 is er een unieke $f_a: F^m \to F^l$ met $\mathrm{mat}_{\mathrm{st}}(f_a) = a$, en is er een unieke $f_b: F^n \to F^m$ met $\mathrm{mat}_{\mathrm{st}}(f_b) = b$. Dan is er vanwege Stelling VII.2.9 en Propositie VII.2.8 ook een unieke $c \in \mathrm{M}_{n,l}(F)$ met $c = \mathrm{mat}_{\mathrm{st}}(f_a \circ f_b)$. Deze c noemen we *het product van a met b*, en we noteren het als ab. De afbeelding

$$\mathrm{M}_{l,m}(F) \times \mathrm{M}_{m,n}(F) \to \mathrm{M}_{l,n}(F), \quad (a, b) \mapsto ab$$

heet *matrixvermenigvuldiging*.

VII.2.10 Propositie. In de notatie als hierboven geldt:

$$\forall (i,j) \in \{1, \ldots, l\} \times \{1, \ldots, n\}, \quad (ab)_{i,j} = \sum_{k=1}^{m} a_{i,k} b_{k,j}. \tag{VII.3}$$

Bewijs. We volgen de definities en gebruiken de lineariteit van f_b en f_a. De j-de kolom van ab is

$$\begin{aligned}
(f_a \circ f_b)(e_j) = f_a(f_b(e_j)) = f_a\left(\sum_{k=1}^{m} b_{k,j} e_k\right) = \sum_{k=1}^{m} f_a(b_{k,j} e_k) = \sum_{k=1}^{m} b_{k,j} f_a(e_k) \\
= \sum_{k=1}^{m} b_{k,j} \sum_{i=1}^{l} a_{i,k} e_i = \sum_{k=1}^{m} \sum_{i=1}^{l} b_{k,j} a_{i,k} e_i = \sum_{i=1}^{l} \sum_{k=1}^{m} b_{k,j} a_{i,k} e_i \\
= \sum_{i=1}^{l} \sum_{k=1}^{m} a_{i,k} b_{k,j} e_i = \sum_{i=1}^{l} \left(\sum_{k=1}^{m} a_{i,k} b_{k,j}\right) e_i .
\end{aligned}$$

■

Een geschikte manier om grafisch weer te geven wat hier gebeurt is als volgt. We schrijven de matrix a links van ab en de matrix b boven ab. Dan is de (i,j)-coëfficiënt $c_{i,j}$ van ab het 'inproduct' van de rij van a links van deze coëfficiënt met de kolom van b erboven:

$$\begin{aligned} &\qquad\qquad\qquad\qquad\qquad\qquad \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & & \vdots \\ b_{m,1} & b_{m,2} & \cdots & b_{m,n} \end{pmatrix} = b \\ a = &\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & & \vdots \\ a_{l,1} & a_{l,2} & \cdots & a_{l,m} \end{pmatrix} \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & & \vdots \\ c_{l,1} & c_{l,2} & \cdots & c_{l,n} \end{pmatrix} = ab \end{aligned} \tag{VII.4}$$

Matrix-optelling

Op dezelfde manier waarop we matrixvermenigvuldiging hebben gedefiniëerd kunnen we ook matrixoptelling definiëren. Het uitgangspunt is dan dat we, voor V en W vectorruimten, $\mathrm{Hom}(V,W)$ van puntsgewijze optelling hebben voorzien in Stelling VII.2.9.

Laat $m,n \in \mathbb{N}$, en $a,b \in \mathrm{M}_{m,n}(F)$. Vanwege Propositie VII.2.8 is er een unieke $f_a : F^m \to F^l$ met $\mathrm{mat}_{\mathrm{st}}(f_a) = a$, en is er een unieke $f_b : F^n \to F^m$ met $\mathrm{mat}_{\mathrm{st}}(f_b) = b$. Dan is er vanwege Stelling VII.2.9 en Propositie VII.2.8 ook een unieke $c \in \mathrm{M}_{m,n}(F)$ met $c = \mathrm{mat}_{\mathrm{st}}(f_a + f_b)$. Deze c noemen we *de som van a met b*, en we noteren die als $a+b$. De afbeelding

$$\mathrm{M}_{m,n}(F) \times \mathrm{M}_{m,n}(F) \to \mathrm{M}_{m,n}(F), \quad (a,b) \mapsto a+b \tag{VII.5}$$

heet *matrixoptelling*.

VII.2.11 Propositie. In de notatie als hierboven geldt:

$$\forall (i,j) \in \{1,\ldots,m\} \times \{1,\ldots,n\}, \quad (a+b)_{i,j} = a_{i,j} + b_{i,j}. \tag{VII.6}$$

Bewijs. De j-de kolom van $a+b$ is

$$(f_a + f_b)(e_j) = f_a(e_j) + f_b(e_j) = \sum_{i=1}^{n} a_{i,j} e_i + \sum_{i=1}^{n} b_{i,j} e_i = \sum_{i=1}^{n} (a_{i,j} + b_{i,j}) e_i.$$

■

Matrices en scalairvermenigvuldiging

In Stelling VII.2.9 hebben we, voor V en W vectorruimten, $\mathrm{Hom}(V,W)$ van een scalairvermenigvuldiging voorzien.

Laat $m,n \in \mathbb{N}$, en $a \in \mathrm{M}_{m,n}(F)$ en $\lambda \in F$. Vanwege Propositie VII.2.8 is er een unieke $f_a : F^m \to F^l$ met $\mathrm{mat}_{\mathrm{st}}(f_a) = a$. Dan is er vanwege Stelling VII.2.9 en Propositie VII.2.8 ook een unieke $c \in \mathrm{M}_{m,n}(F)$ met $c = \mathrm{mat}_{\mathrm{st}}(\lambda f_a)$. Deze c noemen we *het veelvoud van a onder λ*, en we noteren die als λa. De afbeelding

$$F \times \mathrm{M}_{m,n}(F) \to \mathrm{M}_{m,n}(F), \quad (\lambda, a) \mapsto \lambda a \tag{VII.7}$$

heet *matrixscalairvermenigvuldiging*.

VII.2.12 Propositie. In de notatie als hierboven geldt:

$$\forall (i,j) \in \{1,\ldots,m\} \times \{1,\ldots,n\}, \quad (\lambda a)_{i,j} = \lambda a_{i,j}. \tag{VII.8}$$

Bewijs. De j-de kolom van λa is

$$(\lambda f_a)(e_j) = \lambda f_a(e_j) = \lambda \sum_{i=1}^{n} a_{i,j} e_i = \sum_{i=1}^{n} \lambda a_{i,j} e_i.$$

■

Nu kunnen we de vruchten plukken van Stelling VII.2.9 en ons werk aan het verband tussen matrices en lineaire afbeeldingen.

Eigenschappen van operaties op matrices

VII.2.13 Stelling. 1. Laat $n,m,l,k \in \mathbb{N}$, $a \in \mathrm{M}_{k,l}(F)$, $b \in \mathrm{M}_{l,m}(F)$, $c \in \mathrm{M}_{m,n}(F)$. Dan geldt $(ab)c = a(bc)$ in $\mathrm{M}_{k,n}(F)$. In woorden: *matrixvermenigvuldiging is associatief*.

2. Laat $n,m \in \mathbb{N}$. Dan is $\mathrm{M}_{m,n}(F)$ met matrixoptelling en scalairvermenigvuldiging een F-vectorruimte. De bijectie $\mathrm{mat}_{\mathrm{st}} \colon \mathrm{Hom}(F^n,F^m) \to \mathrm{M}_{m,n}(F)$ is een isomorfisme.
3. Laat $n,m,l \in \mathbb{N}$. Laat $a,b \in \mathrm{M}_{m,n}(F)$, $c \in \mathrm{M}_{l,m}(F)$, en $\lambda \in F$. Dan geldt dat $c(a+\lambda b) = ca + \lambda cb$; *matrixvermenigvuldiging is lineair in de 2-de variabele*.
4. Laat $n,m,l \in \mathbb{N}$. Laat $c \in \mathrm{M}_{m,n}(F)$, $a,b \in \mathrm{M}_{l,m}(F)$, en $\lambda \in F$. Dan geldt dat $(a+\lambda b)c = ac + \lambda bc$; *matrixvermenigvuldiging is lineair in de 1-ste variabele*.

Bewijs. Onderdeel 1 volgt uit de associativiteit van samenstelling van afbeeldingen. Voor wie van formules houdt:

$$\begin{aligned}(ab)c &= \mathrm{mat}_{\mathrm{st}}(f_{ab} \circ f_c) = \mathrm{mat}_{\mathrm{st}}((f_a \circ f_b) \circ f_c) = \mathrm{mat}_{\mathrm{st}}(f_a \circ (f_b \circ f_c)) \\ &= \mathrm{mat}_{\mathrm{st}}(f_a \circ f_{bc}) = a(bc).\end{aligned}$$

De andere onderdelen volgen uit de definities van de operaties en Stelling VII.2.9. ■

Ringen van matrices

VII.2.14 Gevolg. Laat $n \in \mathbb{N}$. Dan is de verzameling $\mathrm{M}_{n,n}(F)$ van n-bij-n matrices met coëfficiënten in F, met optelling en vermenigvuldiging, en met de elementen 0_n en 1_n, een ring. Deze is commutatief precies dan als $n \leq 1$.

Bewijs. Alleen de uitspraak over commutativiteit behoeft een bewijs. De ring $\mathrm{M}_0(F)$ is de nulring, en die is commutatief. De ring $\mathrm{M}_1(F)$ is isomorf met F, dus commutatief. Stel nu dat $n \geq 2$. Laat $a = \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ en laat $b = \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$. Dan geldt dat $ab = \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$ en $ba = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$. ■

De inverse van $\mathrm{mat}_{\mathrm{st}}$

Matrixvermenigvuldiging kan ook gebruikt worden om de inverse afbeelding van $\mathrm{mat}_{\mathrm{st}} \colon \mathrm{Hom}(F^n,F^m) \to \mathrm{M}_{m,n}(F)$ te beschrijven. Laat daarom $m,n \in \mathbb{N}$ en $a \in \mathrm{M}_{m,n}(F)$. In het bewijs van Propositie VII.2.7 is de lineaire afbeelding $f_a \colon F^n \to F^m$ met $\mathrm{mat}_{\mathrm{st}}(f_a) = a$ expliciet beschreven:

$$\forall v \in F^n, \quad f_a(v) = \sum_{j=1}^{n} v_j a_j, \quad \text{met } a_j \text{ de } j\text{-de kolom van } a.$$

In termen van matrixvermenigvuldiging ziet dit eruit als:

$$f_a \colon \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \mapsto \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} a_{1,1}v_1 + \cdots + a_{1,n}v_n \\ \vdots \\ a_{m,1}v_1 + \cdots + a_{m,n}v_n \end{pmatrix}.$$

Om dit in fatsoenlijke formules zonder stippeltjes te beschrijven, voeren we de afbeelding

$$\mathrm{kol}_n \colon F^n \to \mathrm{M}_{n,1}(F), \quad \mathrm{kol}_n(v)_i = v_i$$

in, die van een element van F^n een kolomvector maakt. Deze afbeelding is een isomorfisme van F-vectorruimten. Dan luidt de formule:

$$\forall v \in F^n, \quad \mathrm{kol}_m(f_a(v)) = a \cdot \mathrm{kol}_n(v).$$

In de hedendaagse wiskunde geeft men dit soort formules graag weer in de vorm van een *commutatief diagram*:

Commutatief diagram

$$\begin{array}{ccc} F^n & \xrightarrow{f_a} & F^m \\ {\scriptstyle \mathrm{kol}_n}\downarrow & & \downarrow{\scriptstyle \mathrm{kol}_m} \\ \mathrm{M}_{n,1}(F) & \xrightarrow{a\cdot} & \mathrm{M}_{m,1}(F). \end{array} \tag{VII.9}$$

De commutativiteit betekent dat de twee samenstellingen $a\cdot \circ \mathrm{kol}_n$ en $\mathrm{kol}_m \circ f_a$ gelijk zijn. Aangezien kol_n en kol_m isomorfismen zijn drukt dit perfect uit dat de lineaire afbeelding f_a en de afbeelding $a\cdot$ slechts administratief (via kol_n en kol_m) verschillen.

Slordigheid

Het verschil tussen F^n en $\mathrm{M}_{n,1}(F)$ is zo klein dat de meeste teksten over dit onderwerp het niet eens noemen, maar kortweg zeggen dat "men elementen van F^n en van F^m opvat als kolomvectoren", en spreken van de afbeelding

$$a\cdot : F^n \to F^m, \quad x \mapsto ax. \tag{VII.10}$$

Wij zullen ons deze slordigheid ook permitteren. Een bijkomend voordeel is dat dat ons de notatie $a\cdot$ geeft voor de lineaire afbeelding bij een matrix a; hierin zitten geen overbodige symbolen meer.

Kern en beeld deelruimten

VII.2.15 Definitie. Laat V en W vectorruimten zijn en $f : V \to W$ lineair. De *kern van f* is de deelverzameling $\{v \in V : f(v) = 0\}$. Notatie: $\ker(f)$.

VII.2.16 Stelling. Laat V en W vectorruimten zijn en $f : V \to W$ lineair. Dan is $\ker(f)$ een deelruimte van V en $f(V)$ een deelruimte van W.

Bewijs. Opgave VII.2.5. ∎

Opgaven

1. Bewijs de claims van Voorbeeld VII.2.3.

2. Laat V, C D en de v_a zoals in Voorbeeld VII.2.3.

(a) Laat zien dat de deelruimten C en D van V *invariant* zijn onder alle v_a: $v_a(C) = C$ en $v_a(D) = D$.

(b) Laat zien dat de v_a de deelruimte $W = \langle \sin, \cos \rangle$ invariant laten.

(c) Laat zien dat voor alle $a \in \mathbb{R}$ geldt: $v_a \circ d = d \circ v_a$ en $v_a \circ p = p \circ v_a$.

(d) Wat kun je zeggen over $d \circ p$?

(e) En kunnen we praten over $p \circ d$?

3. Laat V en W vectorruimten zijn, en $f : V \to W$ een afbeelding. Bewijs dat f lineair is precies dan als:
(L) $\forall v_1, v_2 \in V$, $\forall \lambda \in F$, $f(v_1 + \lambda v_2) = f(v_1) + \lambda f(v_2)$.

4. Bewijs de overige onderdelen van Stelling VII.2.9

5. Bewijs Stelling VII.2.16.

6. Geef een voorbeeld van een lichaam F, a en b in $\mathrm{M}_2(F)$ met $ab = 0$ en $ba \neq 0$.

7. Laat F een lichaam zijn, en $n \in \mathbb{N}$.

(a) Laat $a, b, c \in \mathrm{M}_n(F)$ en neem aan dat $ab = 1_n$ en $ca = 1_n$. Bewijs dan dat $c = b$.

(b) Laat $a, b \in \mathrm{M}_n(F)$ en neem aan dat $ab = 1_n$. Geldt dan dat $ba = 1_n$? (Dit is met de kennis die je nu hebt een te moeilijke opgave! In Opgave VII.3.5 komen we hier op terug.)

VII.3 Dimensie, basis en (on)afhankelijkheid

In deze sectie definiëren we voor 'eindig voortgebrachte vectorruimten' de begrippen dimensie en basis, en bewijzen we er een aantal eigenschappen van. Het hoofdresultaat is dat het aantal elementen in een basis gelijk is aan de dimensie. Eigenlijk is dit één van de weinige echte stellingen in de lineaire algebra, veel van de theorie is meer 'taal'. Met andere woorden: hier gaat wat gebeuren! Omdat wát er gaat gebeuren meestal (maar niet in deze tekst) impliciet wordt gebruikt in de vorm van een definitie, valt dit niet zo op. Toch wordt het bestaan van een goede notie van dimensie elke keer gebruikt als we een uitspraak doen waarin het woord 'dimensie' voorkomt. Best belangrijk, dus.

Laat F een lichaam zijn. Omdat er in deze sectie alleen F-vectorruimten voorkomen noemen we F-vectorruimten gewoon vectorruimten.

Lineaire combinatie

VII.3.1 Definitie. Laat V een vectorruimte zijn. Voor $n \in \mathbb{N}$, $\lambda = (\lambda_1, \ldots, \lambda_n) \in F^n$ en $v = (v_1, \ldots, v_n) \in V^n$ heet $\lambda_1 v_1 + \cdots + \lambda_n v_n$ de *lineaire combinatie van de v met coëfficiënten λ*.

Eindig voortgebracht

VII.3.2 Definitie. Een vectorruimte V heet *eindig voortgebracht* als er een eindige deelverzameling $S \subseteq V$ bestaat met $\langle S \rangle = V$. Met bijna dezelfde woorden: V is eindig voortgebracht als er een $n \in \mathbb{N}$ is en er $v_1, \ldots, v_n$ in V zijn zodat iedere $w \in V$ een lineaire combinatie van de $v_1, \ldots, v_n$ is,

$$\forall w \in V, \exists \lambda_1, \ldots, \lambda_n \in F, \sum_{i=1}^{n} \lambda_i v_i = w.$$

Dimensie

VII.3.3 Definitie. Laat V een eindig voortgebrachte vectorruimte zijn. Dan is de verzameling van $n \in \mathbb{N}$ waarvoor er een $v \in V^n$ bestaat die V voortbrengt niet leeg, en heeft dus een kleinste element heeft vanwege Stelling IV.2.4. De *dimensie van V* is dit kleinste element. Notatie: $\dim(V)$.

Op dit moment hebben we nog niet veel aan deze definitie, want het is niet duidelijk dat $\dim(F^n) = n$. Wat duidelijk is, is dat $\dim(F^n) \leq n$ omdat F^n is voortgebracht door $e = (e_1, \ldots, e_n)$ in $(F^n)^n$. Maar wie garandeert dat het niet met minder dan n kan? Het volgende lemma is ons breekijzer in deze.

Breekijzer dimensie

VII.3.4 Lemma. Laat V en W eindig voortgebrachte vectorruimten, en $f : V \to W$ een surjectieve lineaire afbeelding. Dan geldt $\dim(W) \leq \dim(V)$. Als bovendien f niet injectief is dan geldt $\dim(W) < \dim(V)$.

Bewijs. Laat $d = \dim(V)$ en $v \in V^d$ een voortbrengend d-tupel. Voor $i \in \{1,\dots,d\}$ laat $w_i = f(v_i)$. Dan is $(w_1,\dots,w_d)$ een voortbrengend d-tupel van W. Dit bewijst $\dim(W) \leq \dim(V)$. Maar we laten zien dat als f niet injectief is, het ook met minder kan. Laat $u \in V$ met $u \in \ker(f)$ en $u \neq 0$. Laat $\lambda \in F^d$ met $u = \sum_{i=1}^{d} \lambda_i v_i$. Omdat $u \neq 0$ is er een i met $\lambda_i \neq 0$; na als nodig de v_i te permuteren kunnen we aannemen dat $\lambda_d \neq 0$. Dan geldt $\lambda_d v_d = u - \sum_{i=1}^{d-1} \lambda_i v_i$. We passen f toe, dat geeft

$$w_d = f(v_d) = \lambda_d^{-1}\left(0 - \sum_{i=1}^{d-1} \lambda_i f(v_i)\right) = -\sum_{i=1}^{d-1} \lambda_d^{-1}\lambda_i w_i.$$

Dan brengt $(w_1,\dots,w_{d-1})$ W voort: lineaire combinaties in $(w_1,\dots,w_d)$ worden door substitutie van w_d als lineaire combinatie van $(w_1,\dots,w_{d-1})$ lineaire combinaties van $(w_1,\dots,w_{d-1})$. Dat geeft $\dim(W) \leq d-1 < \dim(V)$. ∎

$\dim(F^n) = n$

VII.3.5 Stelling. Voor alle $n \in \mathbb{N}$ geldt $\dim(F^n) = n$.

Bewijs. We weten al dat voor alle $n \in \mathbb{N}$ geldt dat $\dim(F^n) \leq n$. Voor $n = 0$: $F^0 = \langle\varnothing\rangle$ dus $0 \leq \dim(F^0) \leq 0$. Laat $n \in \mathbb{N}$ en laat

$$p : F^{n+1} \to F^n, \quad (x_1,\dots,x_{n+1}) \mapsto (x_1,\dots,x_n)$$

de projectie op de eerste n coördinaten zijn. Dan is p een surjectieve lineaire afbeelding die niet injectief is, dus volgens Lemma VII.3.4 geldt $\dim(F^n) < \dim(F^{n+1})$. Dit wetende is het bewijs nu snel klaar met inductie.

Stap 1: voor $n = 0$ is het waar. Stap 2. Laat $n \in \mathbb{N}$ en neem aan dat $\dim(F^n) = n$. Dan hebben we $n = \dim(F^n) < \dim(F^{n+1}) \leq n+1$. Maar dan $\dim(F^{n+1}) = n+1$. ∎

Basis

VII.3.6 Definitie. Laat V een vectorruimte, $n \in \mathbb{N}$ en $v \in V^n$. Dan definiëren we

$$\varphi_v : F^n \to V, \quad \lambda \mapsto \sum_{i=1}^{n} \lambda_i v_i.$$

Het n-tupel v heet een *basis van* V als φ_v bijectief is, dat wil zeggen, als er voor ieder element w van V een unieke $\lambda \in F^n$ is met $w = \sum_{i=1}^{n} \lambda_i v_i$.

Lineair (on-) afhankelijk

VII.3.7 Definitie. Laat V een vectorruimte zijn, $n \in \mathbb{N}$ en $v \in V^n$. Dan heet v *lineair afhankelijk* als er een $\lambda \in F^n$ is met $\lambda \neq 0$ en $\sum_i \lambda_i v_i = 0$. Als v niet lineair afhankelijk is dan noemen we v *lineair onafhankelijk*.

De stelling

VII.3.8 Stelling. Laat V een vectorruimte, $n \in \mathbb{N}$ en $v \in V^n$.

1. De afbeelding $\varphi_v : F^n \to V$ uit Definitie VII.3.6 lineair.
2. De afbeelding φ_v is surjectief precies dan als V voortgebracht wordt door v.
3. De afbeelding φ_v is injectief precies dan als v onafhankelijk is.
4. v is een basis van V precies dan als v voortbrengt en onafhankelijk is.
5. Als $(v_1,\dots,v_n)$ een basis is van V dan geldt $\dim(V) = n$.
6. Als V voortgebracht is door v dan zijn er een d in $\{0,\dots,n\}$ en een $w \in V^d$ zodat $\{w_1,\dots,w_d\} \subseteq \{v_1,\dots,v_n\}$ en w een basis is van V.
7. Als V eindig voortgebracht is dan heeft V een basis.
8. Als V voortgebracht is door $v \in V^n$ en $\dim(V) = n$ dan is v een basis van V.

Bewijs. De bewijzen van 1–4 zijn triviaal. We bewijzen 5, en dat bewijs illustreert een belangrijk principe. Stel dat $(v_1,\dots,v_n)$ een basis is van V. Dan is $\varphi_v : F^n \to V$ een bijectieve lineaire afbeelding. Onderdeel 2 van Stelling VII.2.9 zegt dat φ_v^{-1} lineair is. Daaruit volgt dat $\dim(F^n) = \dim(V)$, want ieder tupel voortbrengers van F^n wordt door φ_v afgebeeld op een tupel voortbrengers van V, en vice versa door φ_v^{-1}. Dus het bewijs van 5 is klaar. We hebben hier een mooi voorbeeld gezien van het belang van isomorfismen.

We bewijzen nu onderdelen 6–8. Merk op dat onderdeel 7 direct uit onderdeel 6 volgt. We bewijzen nu onderdeel 6. Voor $i \in \{0,\dots,n\}$ laat $V_i = \langle\{v_1,\dots,v_i\}\rangle$. Merk op dat $\{0\} = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$. Laat

$$I = \{i \in \{1,\dots,n\} : V_{i-1} \neq V_i\}, \quad d = \#I, \text{ en schrijf } \quad I = \{i_1,\dots,i_d\},$$

met $i_1 < \cdots < i_d$. Voor $j \in \{1,\dots,d\}$ laat $w_j = v_{i_j}$. We bewijzen dat $w \in V^d$ een basis is van V. Merk op dat $\langle\{w_1,\dots,w_d\}\rangle = V_{i_d} = V$ want voor $i \in \{i_d+1,\dots,n\}$ geldt dat $V_{i-1} = V_i$. Net zo geldt dat voor $j \in \{0,\dots,d-1\}$ en $i \in \{i_j,\dots,i_{j+1}-1\}$ dat $V_i = V_{i_j}$. Nu bewijzen we met inductie naar j dat voor $j \in \{1,\dots,d\}$ het j-tupel $(w_1,\dots,w_j)$ een basis is van V_{i_j}.

Stap 1. Voor $j = 1$ is het waar, want $V_{i_1-1} = \{0\}$ en $\{0\} \neq V_{i_1} = \langle\{w_1\}\rangle$.

Stap 2. Laat nu $j \in \{1,\dots,d-1\}$ en neem aan dat $(w_1,\dots,w_j)$ een basis is van V_{i_j}. Dan is $(w_1,\dots,w_j)$ onafhankelijk en $\langle\{w_1,\dots,w_j\}\rangle = V_{i_j}$. Dus $\langle\{w_1,\dots,w_j,w_{j+1}\}\rangle = V_{i_{j+1}}$. We bewijzen dat $(w_1,\dots,w_j,w_{j+1})$ onafhankelijk is. Laat $(\lambda_1,\dots,\lambda_{j+1}) \in F^{j+1}$ en stel dat $\sum_{k=1}^{j+1} \lambda_k w_k = 0$. Dan $\lambda_{j+1} = 0$ omdat $w_{j+1} \notin V_{i_j}$. De onafhankelijkheid van $(w_1,\dots,w_j)$ impliceert dat $\lambda_k = 0$ voor alle k. Dus $(w_1,\dots,w_j,w_{j+1})$ is onafhankelijk, en dus een basis van $V_{i_{j+1}}$. Het bewijs van onderdeel 6 is nu klaar.

We bewijzen onderdeel 8. Laat d en $w \in V^d$ als in onderdeel 6. Onderdeel 5 zegt dat $\dim(V) = d$. Dus $d = n$ en $w = v$, dus is v een basis van V. ∎

Deelruimten uitbreiding

VII.3.9 Stelling. Laat V een eindig voortgebrachte vectorruimte zijn, en W een deelruimte van V.

1. Dan is W eindig voortgebracht.
2. Voor iedere basis van W is er een basis van V die haar uitbreidt.
3. $\dim(W) \leq \dim(V)$.
4. $\dim(W) = \dim(V) \Leftrightarrow W = V$.

Bewijs. We bewijzen onderdeel 1. Omdat V isomorf is met $F^{\dim(V)}$ is het genoeg te bewijzen dat de uitspraak waar is voor $V = F^n$, voor alle $n \in \mathbb{N}$. We doen dat met inductie naar n.

Stap 1. Het is waar voor $n = 0$ en ook voor $n = 1$: de enige deelruimten zijn $\{0\}$ en F^n.

Stap 2. Laat $n \in \mathbb{N}$ met $n \geq 1$, en neem aan dat de uitspraak waar is voor F^n. Laat $W \subseteq F^{n+1}$ een deelruimte zijn, en laat

$$p : F^{n+1} \to F^n, \quad (x_1,\dots,x_{n+1}) \mapsto (x_1,\dots,x_n).$$

Volgens de inductiehypothese is $p(W)$ eindig voortgebracht. Laat $d \in \mathbb{N}$ en laat $w \in W^d$ zodat $p(W)$ is voortgebracht door $(p(w_1),\dots,p(w_d))$. De kern van p is 1-dimensionaal, met basis e_{n+1}, en $W \cap \langle e_{n+1}\rangle$ is $\{0\}$ of gelijk aan $\langle e_{n+1}\rangle$. In beide gevallen is $W \cap \langle e_{n+1}\rangle$ voortgebracht door 1 element. Laat w_0 dus een voortbrenger zijn van $W \cap \langle e_{n+1}\rangle$.

Claim: W is voortgebracht door $(w_0, w_1,\dots,w_d)$.

Bewijs. Laat $w \in W$. Laat $\lambda \in F^d$ met $p(w) = \lambda_1 p(w_1) + \cdots + \lambda_d p(w_d)$. De lineariteit van p geeft $p(w) = p(\lambda_1 w_1 + \cdots + \lambda_d w_d)$, dus $p(w - \lambda_1 w_1 - \cdots \lambda_d w_d) = 0$. Dus er is een $\lambda_0 \in F$ met $w - \lambda_1 w_1 - \cdots - \lambda_d w_d = \lambda_0 v_0$. Dus $w = \lambda_0 v_0 + \lambda_1 w_1 + \cdots + \lambda_d w_d$. De

claim is bewezen, en daarmee ook Stap 2, en daarmee is het bewijs van onderdeel 1 klaar.

We bewijzen onderdeel 2 voor $V = F^n$. Laat $d = \dim(W)$ en laat $w \in W^d$ een basis van W zijn. Voor $i \in \{0,\ldots,n\}$ laat

$$V_i = \langle \{w_1,\ldots,w_d\} \cup \{e_1\ldots,e_i\} \rangle.$$

Merk op dat $V_0 = W$ en $V_n = F^n$. We volgen nu de methode van het bewijs van onderdeel 6 van Stelling VII.3.8. Laat $I = \{i \in \{1,\ldots,n\} : V_{i-1} \neq V_i\}$, laat $m = \#I$ en schrijf $I = \{i_1,\ldots,i_m\}$ met $i_1 < \cdots < i_m$. Dan is $(w_1,\ldots,w_d,u_{i_1},\ldots,u_{i_m})$ een basis van V die de basis w van W uitbreidt.

We bewijzen onderdeel 3. Laat w een basis van W zijn. Dan is er volgens onderdeel 2 een basis v van V die w uitbreidt. Dan is het aantal elementen in de basis w hoogstens dat in v, dus $\dim(W) \leq \dim(V)$.

We bewijzen onderdeel 4. Laat w een basis van W zijn. Deze kan uitgebreid worden tot een basis v van V. Omdat $\dim(W) = \dim(V)$ geldt dan $w = v$. Maar dan is V voortgebracht door w en dus gelijk aan W. ∎

We eindigen deze sectie met de de *dimensiestelling voor lineaire afbeeldingen*.

Dimensie kern en beeld

VII.3.10 Stelling. Laat V en W vectorruimten zijn met V eindig voortgebracht, en $f : V \to W$ een lineaire afbeelding. Dan geldt

$$\dim(f(V)) + \dim(\ker(f)) = \dim(V).$$

Bewijs. De kern van f, $\ker(f)$, is een deelruimte van V. Volgens Stelling VII.3.9 is $\ker(f)$ eindig voortgebracht en vanwege Stelling VII.3.8, onderdeel 7 bestaat er een basis van $\ker(f)$. Laat dan $d_1 \in \mathbb{N}$ en $v \in \ker(f)^{d_1}$ zodat v een basis van $\ker(f)$ is. Volgens Stelling VII.3.9 is er een $d_2 \in \mathbb{N}$ en een $(v_{d_1+1},\ldots,v_{d_1+d_2})$ in V^{d_2} zodat $(v_1,\ldots,v_{d_1},v_{d_1+1},\ldots,v_{d_1+d_2})$ een basis van V is. We gaan bewijzen dat $(f(v_{d_1+1}),\ldots,f(v_{d_1+d_2}))$ een basis van $f(V)$ is. De stelling is dan bewezen, want dan geldt $d_2 = \dim(f(V))$, $d_1 = \dim(\ker(f))$ en $d_1 + d_2 = \dim(V)$.

Omdat V voortgebracht is door $(v_1,\ldots,v_{d_1},v_{d_1+1},\ldots,v_{d_1+d_2})$, is $f(V)$ voortgebracht door het beeld hiervan in $f(V)$, en dus door $(f(v_{d_1+1}),\ldots,f(v_{d_1+d_2}))$ want voor $i \in \{1,\ldots,d_1\}$ geldt dat $f(v_i) = 0$.

Rest nog te bewijzen dat $(f(v_{d_1+1}),\ldots,f(v_{d_1+d_2}))$ onafhankelijk is. Stel dat $(\lambda_{d_1+1},\ldots,\lambda_{d_1+d_2})$ in F^{d_2} en $\sum_{i=1} \lambda_{d_1+i} f(v_{d_1+i}) = 0$. Lineariteit van f geeft dan dat $f(\sum_{i=1} \lambda_{d_1+i} v_{d_1+i}) = 0$. Dat wil zeggen dat $\sum_{i=1} \lambda_{d_1+i} v_{d_1+i}$ in $\ker(f)$ zit en dat er een $(\lambda_1,\ldots,\lambda_{d_1})$ in F^{d_1} is zodat

$$\sum_{i=1} \lambda_{d_1+i} v_{d_1+i} = \sum_{j=1}^{d_1} \lambda_j v_j.$$

Onafhankelijkheid van $(v_1,\ldots,v_{d_1},v_{d_1+1},\ldots,v_{d_1+d_2})$ geeft dan de gewenste conclusie. ∎

Opgaven

1. Laat V de vectorruimte van alle F-waardige functies op $\mathbb{N}$ zijn, met puntsgewijze optelling en scalairvermenigvuldiging. Bewijs dat V niet eindig voortgebracht is.

2. Laat $W = \{(x_1,x_2,x_3) \in F^3 : x_1 + x_2 + x_3 = 0\}$. Geef een basis van W.

3. Laat $n \in \mathbb{N}_{>0}$. Laat $W = \{x \in F^n : x_1 + \cdots + x_n = 0\}$. Bepaal $\dim(W)$.

✍ **4.** Laat $W = \{x \in F^2 : x_1 + x_2 = 0 \wedge x_1 - x_2 = 0\}$. Bepaal $\dim(W)$.

5. Maak onderdeel (b) van Opgave VII.2.7. Hint: gebruik Stelling VII.3.10 om te bewijzen dat a injectief is.

6. Laat $F = \mathbb{R}$, V de $\mathbb{R}$-vector van alle functies $f : \mathbb{R} \to \mathbb{R}$ met puntsgewijze optelling en scalairvermenigvuldiging. Laat W de deelruimte van V zijn voortgebracht door de elementen cos, sin, $\cos^2$ ($x \mapsto \cos(x)^2$, niet $x \mapsto \cos(\cos(x))$) en $\sin^2$. Geef een basis van W.

7. Laat $F = \mathbb{Q}$ en W de deelruimte van $\mathbb{R}$ voortgebracht door 1, $\sqrt{2}$ en $\sqrt{3}$. Bepaal $\dim(W)$.[1]

VII.4 Lineaire afbeeldingen, bases en matrices

Laat F een lichaam zijn. Omdat er in deze sectie alleen F-vectorruimten voorkomen noemen we F-vectorruimten gewoon vectorruimten.

In deze sectie definiëren we 'de matrix van een lineaire afbeelding $f : V \to W$ ten opzichte van bases $v \in V^n$ van het domein V en $w \in W^m$ van het codomein W'. Omdat we de bijectie $\mathrm{mat}_{\mathrm{st}} : \mathrm{Hom}(F^n, F^m) \to \mathrm{M}_{m,n}(F)$ van Propositie VII.2.8 al hebben, en v en w per definitie (Definitie VII.3.6) isomorfismen $\varphi_v : F^n \to V$ en $\varphi_w : F^m \to W$ geven, hoeven we deze zaken slechts te combineren.

Matrices en bases

Laat V en W eindig voortgebrachte vectorruimten zijn, en $f : V \to W$ een lineaire afbeelding. Laat $n = \dim(V)$ en $m = \dim(W)$. Laat $v \in V^n$ een basis van V zijn, en $w \in W^m$ een basis van W. Definitie VII.3.6 zegt dat we isomorfismen hebben:

$$\varphi_v : F^n \to V, \quad \lambda \mapsto \sum_{i=1}^{n} \lambda_i v_i$$
$$\varphi_w : F^m \to W, \quad \mu \mapsto \sum_{j=1}^{m} \mu_j w_j .$$

We geven de afbeeldingen die we hebben weer in een diagram:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \uparrow{\scriptstyle \varphi_v} & & \uparrow{\scriptstyle \varphi_w} \\ F^n & & F^m \end{array}$$

We kunnen zo nog geen afbeelding van $F^n \to F^m$ maken, maar dat kunnen we wel als we φ_w vervangen door $\varphi_w^{-1} : W \to F^m$:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \uparrow{\scriptstyle \varphi_v} & & \downarrow{\scriptstyle \varphi_w^{-1}} \\ F^n & & F^m \end{array}$$

De matrix ${}_w\mathrm{mat}_v(f)$.

Dit diagram nodigt ons uit om naar $\varphi_w^{-1} \circ f \circ \varphi_v : F^n \to F^m$ te kijken. Deze li-

[1] Lineaire algebra over $\mathbb{Q}$ maakt het mogelijk in de getaltheorie te bewijzen dat trisectie van bijvoorbeeld $\pi/6$ niet mogelijk is met passer en latje.

neaire afbeelding is volgens Propositie VII.2.8 gegeven door een uniek element van $\mathrm{M}_{m,n}(F)$ dat we noteren als ${}_w\mathrm{mat}_v(f)$, *de matrix van f ten opzichte van de bases v van V en w van W*. De j-de kolom van de m-bij-n matrix ${}_w\mathrm{mat}_v(f)$ is $(\varphi_w^{-1} \circ f \circ \varphi_v)(e_j) = \varphi_w^{-1}(f(v_j))$. In de notatie van (VII.10) hebben we dan een commutatief diagram:

$$\begin{array}{ccc} V & \xrightarrow{\quad f \quad} & W \\ {\scriptstyle\varphi_v}\uparrow & & \uparrow{\scriptstyle\varphi_w} \\ F^n & \xrightarrow[{}_w\mathrm{mat}_v(f)\cdot]{} & F^m \end{array} \tag{VII.11}$$

Dit diagram zegt dat f kan worden uitgedrukt in ${}_w\mathrm{mat}_v(f)$, en vice versa:

$$f = \varphi_w \circ {}_w\mathrm{mat}_v(f)\cdot \circ \varphi_v^{-1}, \quad {}_w\mathrm{mat}_v(f)\cdot = \varphi_w^{-1} \circ f \circ \varphi_v\,. \tag{VII.12}$$

Vector t.o.v. basis: $\mathrm{vec}_v = \varphi_v^{-1}$

Niet iedereen is een fan van commutatieve diagrammen. Ze zijn nuttig omdat we zo visueel zijn ingesteld, maar in een formeel bewijs kun je er bijvoorbeeld niets mee, en in de praktijk leidt het gebruik ervan vaak tot veel gebaren en maar weinig opschrijven. Daarom geven we het bovenstaande ook nog eens weer in formules. We noteren daartoe de inverse afbeelding van φ_v als vec_v, de *vector van een element van V ten opzichte van de basis v*. In die notatie geldt:

$$\forall x \in V, \quad \mathrm{vec}_w(f(x)) = {}_w\mathrm{mat}_v(f)\cdot\mathrm{vec}_v(x), \tag{VII.13}$$

en de j-de kolom van ${}_w\mathrm{mat}_v(f)$ is $\mathrm{vec}_w(f(v_j))$.

Matrices, samenstellen, en domino's

VII.4.1 Stelling. Laat V, W, U vectorruimten zijn, met bases $v \in W^n$, $w \in W^m$ en $u \in U^l$. Laat $f\colon V \to W$ en $g\colon W \to U$ lineaire afbeeldingen zijn. Dan geldt:

$${}_u\mathrm{mat}_v(g \circ f) = {}_u\mathrm{mat}_w(g) \cdot {}_w\mathrm{mat}_v(f)\,.$$

Bewijs. We gebruiken Formule VII.12. Toegepast op g en f hebben we:

$${}_u\mathrm{mat}_w(g)\cdot = \varphi_u^{-1} \circ g \circ \varphi_w\,, \quad {}_w\mathrm{mat}_v(f)\cdot = \varphi_w^{-1} \circ f \circ \varphi_v\,.$$

Dus

$$\big({}_u\mathrm{mat}_w(g)\cdot\big) \circ \big({}_w\mathrm{mat}_v(f)\cdot\big) = \big(\varphi_u^{-1} \circ g \circ \varphi_w\big) \circ \big(\varphi_w^{-1} \circ f \circ \varphi_v\big) = \varphi_u^{-1} \circ \big(g \circ f\big) \circ \varphi_v\,.$$

Formule VII.12 toegepast op $g \circ f$ geeft:

$$\varphi_u^{-1} \circ \big(g \circ f\big) \circ \varphi_v = {}_u\mathrm{mat}_v(g \circ f)\cdot\,.$$

De laatste drie gelijkheden combinerend hebben we:

$$\big({}_u\mathrm{mat}_w(g)\cdot\big) \circ \big({}_w\mathrm{mat}_v(f)\cdot\big) = {}_u\mathrm{mat}_v(g \circ f)\cdot\,.$$

Associativiteit van matrixvermenigvuldigen geeft

$$\forall x \in V, \quad \big({}_u\mathrm{mat}_w(g) \cdot {}_w\mathrm{mat}_v(f)\big) \cdot x = {}_u\mathrm{mat}_w(g) \cdot \big({}_w\mathrm{mat}_v(f) \cdot x\big)$$

dus

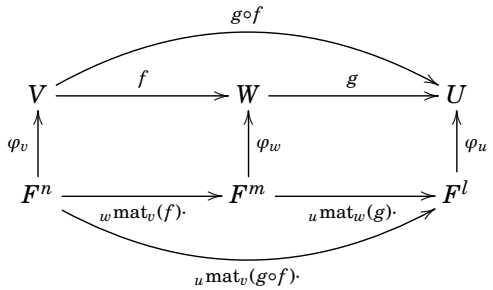
$$\big({}_u\mathrm{mat}_w(g) \cdot {}_w\mathrm{mat}_v(f)\big)\cdot = \big({}_u\mathrm{mat}_w(g)\cdot\big) \circ \big({}_w\mathrm{mat}_v(f)\cdot\big)\,.$$

Dit met de voorlaatste gelijkheid combineren geeft:

$$\big({}_u\mathrm{mat}_w(g) \cdot {}_w\mathrm{mat}_v(f)\big)\cdot = {}_u\mathrm{mat}_v(g \circ f)\cdot\,.$$

Aangezien matrices bijectief met lineaire afbeeldingen corresponderen (in dit geval $\mathrm{Hom}(F^n, F^l)$ en $\mathrm{M}_{l,n}(F)$) is de stelling bewezen.

Fans van commutatieve diagrammen wijzen op het volgende diagram:



en gaan dan uitleggen waarom 'het commuteert'. ■

Matrices en verandering van bases

VII.4.2 Gevolg. Laat V en W vectorruimten zijn, $f : V \to W$ een lineaire afbeelding, v en v' bases van V, en w en w' bases van W. Dan geldt:

$$ {}_{w'}\mathrm{mat}(f)_{v'} = {}_{w'}\mathrm{mat}_w(\mathrm{id}_W) \cdot {}_w\mathrm{mat}_v(f) \cdot {}_v\mathrm{mat}_{v'}(\mathrm{id}_V). $$

De matrices ${}_{w'}\mathrm{mat}_w(\mathrm{id}_W)$ en ${}_v\mathrm{mat}_{v'}(\mathrm{id}_V)$ heten de *matrices van basisverandering* van w naar w' en van v' naar v, en er geldt

$$ \begin{aligned} \forall x \in V \quad & \mathrm{vec}_v(x) = {}_v\mathrm{mat}_{v'}(\mathrm{id}_V) \cdot \mathrm{vec}_{v'}(x), \\ \forall y \in W \quad & \mathrm{vec}_{w'}(x) = {}_{w'}\mathrm{mat}_w(\mathrm{id}_W) \cdot \mathrm{vec}_w(y). \end{aligned} $$

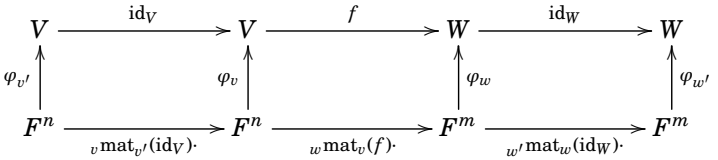
De j-de kolom van ${}_v\mathrm{mat}_{v'}(\mathrm{id}_V)$ is $\mathrm{vec}_v(v'_j)$, en de i-de kolom van ${}_{w'}\mathrm{mat}_w(\mathrm{id}_W)$ is $\mathrm{vec}_{w'}(w_i)$.

Bewijs. Voor de eerste identiteit, gebruik dat samenstellen en matrixvermenigvuldiging beiden associatief zijn, en pas Stelling VII.4.1 toe op $\mathrm{id}_W \circ f \circ \mathrm{id}_V$, en de bases (van rechts naar links) v', v, w, w'.

Voor de tweede identiteit, pas (VII.13) toe met $f = \mathrm{id}_V$ en de bases v' en v. Voor de derde identiteit: idem op administratie na.

De laatste twee uitspraken volgen direct uit de definitie van de matrix van een lineaire afbeelding t.o.v. bases van domein en codomein. ■

De verhandeling over basisverandering en matrices van lineaire afbeeldingen wordt samengevat door dit commutatieve diagram:



(VII.14)

Normaalvorm lineaire afbeelding, rang

Laat V en W eindig voortgebrachte vectorruimten zijn, $f : V \to W$ lineair, en laat $r := \dim(f(V))$; r heet de *rang* van f. In Opgave VII.4.2 wordt bewezen dat er bases v van V en w van W zijn zodat $({}_w\mathrm{mat}_v(f))_{i,j} = 1$ als $i = j \leq r$ en 0 anders. Met

andere woorden, en met $n = \dim(V)$ en $m = \dim(W)$:

$$ {}_w\mathrm{mat}_v(f) = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} = \left(\begin{array}{c|c} 1_r & 0_{r,n-r} \\ \hline 0_{m-r,r} & 0_{m-r,n-r} \end{array}\right). $$

Endomorfismen, iteratie

Een lineaire afbeelding $f : V \to V$ van een vectorruimte V naar zichzelf heet een *endomorfisme van V*. Voor het beschrijven van zo'n f in termen van een matrix is het meestal een goed idee om in het domein en het codomein dezelfde basis v te gebruiken. Het voordeel daarvan is dat er dan geldt:

$$ \forall k \in \mathbb{N} \quad {}_v\mathrm{mat}_v(f^k) = \left({}_v\mathrm{mat}_v(f)\right)^k. $$

Diagonaalmatrix, machten

Dit is met name heel handig als de matrix ${}_v\mathrm{mat}_v(f)$ *diagonaal* is, d.w.z., alle coëfficiënten buiten de diagonaal zijn 0. Voor diagonaalmatrices geldt namelijk:

$$ \forall k \in \mathbb{N}, \quad \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}^k = \begin{pmatrix} \lambda_1^k & 0 & \cdots & 0 \\ 0 & \lambda_2^k & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n^k \end{pmatrix}. $$

Opgave VII.4.3 geeft hier een voorbeeld van.

Opgaven

1. Laat V de $\mathbb{R}$-vectorruimte zijn van alle functies van $\mathbb{R}$ naar $\mathbb{R}$. Laat W de deelruimte zijn voortgebracht door cos en sin.

(a) Geef een basis w van W.

(b) Laat zien dat voor alle f in W geldt dat f differentieerbaar is en dat $f' \in W$. Laat $d : W \to W$, $f \mapsto f'$ de afbeelding 'differentiëren' zijn. Deze is lineair.

(c) Geef de matrix ${}_w\mathrm{mat}_w(d)$.

2. Laat F een lichaam zijn, V en W F-vectorruimten van dimensie n en m, en $f : V \to W$ een lineaire afbeelding. Laat $r := \dim(f(V))$. Bewijs dat er bases v van V en w van W zijn zodat $({}_w\mathrm{mat}_v(f))_{i,j} = 1$ als $i = j \leq r$ en 0 anders. Hint: gebruik het bewijs van Stelling VII.3.10.

3. De *rij van Fibonacci* is recursief gedefiniëerd door $F_0 = 0$, $F_1 = 1$, en voor alle $n \geq 2$: $F_n = F_{n-1} + F_{n-2}$.

(a) Bereken $F_2, \ldots, F_{10}$.

(b) Een manier om een formule voor F_n te vinden is als volgt. Voor alle $n \geq 2$ geldt:

$$ \begin{pmatrix} F_{n-1} \\ F_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} F_{n-2} \\ F_{n-1} \end{pmatrix} $$

Laat zien dat voor alle $n \geq 1$ geldt

$$\begin{pmatrix} F_{n-1} \\ F_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

(c) We definiëren $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\binom{x_1}{x_2} \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \cdot \binom{x_1}{x_2}$. Laat $\lambda_1 = (1+\sqrt{5})/2 \approx 1.618$ (de *gulden snede)* en $\lambda_2 = (1-\sqrt{5})/2 \approx -0.618$. Laat $v_1 = \binom{1}{\lambda_1}$ en $v_2 = \binom{1}{\lambda_2}$. Laat zien dat $f(v_1) = \lambda_1 v_1$ en $f(v_1) = \lambda_1 v_1$.

(d) Laat zien dat $v = (v_1, v_2) \in (\mathbb{R}^2)^2$ een basis van $\mathbb{R}^2$ is. Bepaal ${}_v\mathrm{mat}(f)_v$.

(e) Bepaal $\mathrm{vec}_v\binom{0}{1}$ en bewijs dat

$$\forall n \in \mathbb{N}, \quad F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

(f) Zie `https://nl.wikipedia.org/wiki/Rij_van_Fibonacci` voor meer informatie over de rij van Fibonacci. Vaak wordt verteld dat de rij onstaat uit een model voor populatiegroei van konijnen (Fibonacci's konijnenprobleem), maar [Sc-Ma] argumenteren dat de oorsprong in de genealogie van bijen ligt.

VII.5 Lineaire vergelijkingen, rij-operaties, Gauss eliminatie, rijtrapvorm

De voorgaande secties van dit hoofdstuk zijn theoretisch van aard. Deze sectie gaat daarentegen over het oplossen van stelsels van lineaire vergelijkingen, en heeft daarom zowel een theoretisch als een praktisch en zelfs algoritmisch karakter. Vanaf Voorbeeld VII.5.3 is de inhoud van deze sectie vrij direct vertaald uit [vLuijk], dat op zich gedeeltelijk weer is gebaseerd op een dictaat [Stoll] van Michael Stoll.

In deze sectie is F een lichaam.

Homogeen stelsel lineaire vergelijkingen

Voor m en n in $\mathbb{N}$ is een *homogeen stelsel van m lineaire vergelijkingen over F in n onbekenden* een m-tal vergelijkingen van de vorm

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n &= 0 \\ \quad\vdots & \vdots \quad \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n &= 0 \end{cases} \quad \text{met } a_{i,j} \in F.$$

De vraag is dan hoe we de verzameling van oplossingen $x \in F^n$ van dit stelsel kunnen vinden. Het eerste dat we opmerken is dat als a de m-bij$n$-matrix is gegeven door de $a_{i,j}$, deze verzameling van oplossingen precies de kern is van de lineaire afbeelding $a\cdot : F^n \to F^m$, want voor x in F^n zijn de linkerleden van de m vergelijkingen de coördinaten van $a \cdot x$. Stelling VII.2.16 zegt dat $\ker(a\cdot)$ een lineaire deelruimte is van F^n. We kunnen de vraag naar een beschrijving van de verzameling van oplossingen explicieter maken: hoe vinden we een basis van $\ker(a\cdot)$? De dimensiestelling, Stelling VII.3.10, zegt ons dat $\dim(\ker(a\cdot)) = n - \dim(a \cdot F^n)$. Deze relatie tussen de dimensies van kern en beeld van $a\cdot$ is nuttig als we al 1 van de 2 dimensies weten, maar op dit moment hebben we nog geen methode om 1 van de 2 uit te rekenen. We kiezen ervoor om de kern aan te pakken, want dat is hetzelfde als het oplossen van het stelsel vergelijkingen.

Rij-operaties op matrices

De methode waarmee we een basis van $\ker(a\cdot)$ gaan berekenen is door een a' in $\mathrm{M}_{m,n}(F)$ te berekenen met $\ker(a'\cdot) = \ker(a\cdot)$ door middel van *rij-operaties*, die een

speciale vorm heeft die het mogelijk maakt om direct een basis van $\ker(a'\cdot)$ te geven. Deze methode van rij-operaties staat bekend als*Gauss eliminatie* en wordt ook wel *matrix vegen* genoemd.

We definiëren 3 elementaire rij-operaties op $\mathrm{M}_{m,n}(F)$. Om deze te beschrijven definiëren we voor $i \in \{1,\ldots,m\}$ de functie

$$\mathrm{rij}_i : \mathrm{M}_{m,n}(F) \to F^n, \quad a \mapsto \mathrm{rij}_i(a) = (a_{i,1},\ldots,a_{i,n})$$

die a stuurt naar zijn i-de rij. De 3 typen operaties zijn:

De elementaire rij-operaties

1. $R(i,\lambda)$**.** Voor $i \in \{1,\ldots,m\}$ en $\lambda \in F^\times$ is $R(i,\lambda)(a)$ het element van $\mathrm{M}_{m,n}(F)$ verkregen door de i-de rij van a te vermenigvuldigen met λ. In een formule:

$$\mathrm{rij}_l(R(i,\lambda)(a)) = \begin{cases} \lambda\cdot\mathrm{rij}_l(a) & \text{als } l = i \\ \mathrm{rij}_l(a) & \text{anders.} \end{cases}$$

2. $R(i,j)$**.** Voor $i,j \in \{1,\ldots,m\}$ met $i \neq j$ is $R(i,j)(a)$ het element van $\mathrm{M}_{m,n}(F)$ verkregen door de i-de en j-de rijen van a te verwisselen. In een formule:

$$\mathrm{rij}_l(R(i,j)(a)) = \begin{cases} \mathrm{rij}_j(a) & \text{als } l = i \\ \mathrm{rij}_i(a) & \text{als } l = j \\ \mathrm{rij}_l(a) & \text{anders.} \end{cases}$$

3. $R(i,j,\alpha)$**.** Voor $i,j \in \{1,\ldots,m\}$ met $i \neq j$ en $\alpha \in F$ is $R(i,j,\alpha)(a)$ het element van $\mathrm{M}_{m,n}(F)$ verkregen door α maal de i-de rij bij de j-de rij op te tellen. In een formule:

$$\mathrm{rij}_l(R(i,j,\alpha)(a)) = \begin{cases} \mathrm{rij}_j(a) + \alpha\cdot\mathrm{rij}_i(a) & \text{als } l = j \\ \mathrm{rij}_l(a) & \text{anders.} \end{cases}$$

Rij-operaties zijn inverteerbaar

VII.5.1 Stelling. De bovenstaande rij-operaties zijn inverteerbaar: de inverse van $R(i,\lambda)$ is $R(i,\lambda^{-1})$, de inverse van $R(i,j)$ is $R(i,j)$ en de inverse van $R(i,j,\alpha)$ is $R(i,j,-\alpha)$.

Bewijs. We laten zien dat voor λ en μ in $F^\times$ geldt dat $R(i,\lambda)\circ R(i,\mu) = R(i,\lambda\mu)$; hieruit volgt dat $R(i,\lambda)\circ R(i,\lambda^{-1}) = R(i,1) = \mathrm{id}$ en $R(i,\lambda^{-1})\circ R(i,\lambda) = R(i,1) = \mathrm{id}$. Voor $l \neq i$ geldt:

$$\mathrm{rij}_l(R(i,\lambda)(R(i,\mu)a)) = \mathrm{rij}_l(R(i,\mu)a) = \mathrm{rij}_l(a) = \mathrm{rij}_l(R(i,\lambda\mu)a),$$

en ook

$$\mathrm{rij}_i(R(i,\lambda)(R(i,\mu)a)) = \lambda\cdot\mathrm{rij}_i(R(i,\mu)a)) = \lambda\cdot\mu\cdot\mathrm{rij}_i(a) = \mathrm{rij}_i(R(i,\lambda\mu)a).$$

Het uitschrijven van de overige twee gevallen laten we aan de lezer over. Informeel zijn de uitspraken wel duidelijk. In het eerste geval vermenigvuldigen we de i-de rij eerst met μ en dan met λ, dus in totaal met $\lambda\mu$, terwijl de andere rijen niet veranderen. In het tweede geval is het tweemaal verwisselen van de rijen i en j de identiteit. In het derde geval tellen we eerst α maal rij i bij rij j op en halen dat er dan weer af (of andersom), hetgeen wederom de identiteit is. ■

Rij-operaties en kernen

VII.5.2 Stelling. Laat a en a' in $\mathrm{M}_{mn,}(F)$ zodat a' gekregen is uit a door een eindig aantal van de bovenstaande rij-operaties. Dan $\ker(a'\cdot) = \ker(a\cdot)$.

Bewijs. Het is natuurlijk voldoende dit te bewijzen voor 1 rij-operatie (inductie op het aantal rij-operaties). We nemen dus aan dat er een rij-operatie is waaronder a' het beeld is van a. Vanwege Stelling VII.5.1 is het ook zo dat a het beeld is van a' onder de inverse rij-operatie. Het is dus voldoende te bewijzen dat $\ker(a\cdot) \subseteq \ker(a'\cdot)$.

Laat $x \in \ker(a\cdot)$. Dan geldt dus voor alle $l \in \{1,\dots,m\}$ dat $\sum_j a_{l,j}x_j = 0$. We gaan nu de 3 typen rij-operaties af.

Stel dat $a' = R(i,\lambda)(a)$. Dan geldt

$$\sum_j a'_{l,j}x_j = \sum_j \lambda a_{i,j}x_j = \lambda\cdot\sum_j a_{i,j}x_j = 0,$$

en voor alle $l \in \{1,\dots,m\}$ met $l \neq i$ dat

$$\sum_{l,j} a'_{l,j}x_j = \sum_{l,j} a_{l,j}x_j = 0.$$

We concluderen dat $x \in \ker(a'\cdot)$.

Stel nu dat $a' = R(i,j)(a)$. Dan geldt voor iedere $l \in \{1,\dots,m\}$ dat $\sum_j a'_{l,j}x_j = 0$, want het zijn dezelfde vergelijkingen als voor a (maar in een iets andere volgorde).

Stel dat $a' = R(i,j,\alpha)(a)$. Dan geldt

$$\sum_k a'_{j,k}x_k = \sum_k (a_j + \alpha a_i)x_k = \sum_k a_j x_j + \sum_k \alpha a_i x_k = 0 + \alpha\sum_k a_i x_k = \alpha 0 = 0.$$

En ook geldt voor alle $l \in \{1,\dots,m\}$ met $l \neq j$ dat $\sum_k a'_{l,k}x_k = \sum_k a_{l,k}x_k = 0$. ∎

Voordat we nu het algemene geval behandelen doen we eerst een voorbeeld.

Voorbeeld van Gauss eliminatie

VII.5.3 Voorbeeld. We gaan een basis berekenen voor $\ker(a\cdot)$, met $F = \mathbb{Q}$ en

$$a = \begin{pmatrix} -1 & 2 & 1 & 1 \\ 1 & -1 & 1 & 0 \\ 2 & -3 & 0 & 1 \end{pmatrix}.$$

We voeren elementaire rij-operaties uit waarmee we van links naar rechts in kolommen die niet geheel nul zijn één coëfficiënt 1 maken en dan alle andere nul.

$$\begin{pmatrix} -1 & 2 & 1 & 1 \\ 1 & -1 & 1 & 0 \\ 2 & -3 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{matrix} -R_1 \\ R_2 \\ R_3 \end{matrix} \begin{pmatrix} 1 & -2 & -1 & -1 \\ 1 & -1 & 1 & 0 \\ 2 & -3 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{matrix} R_1 \\ R_2 - R_1 \\ R_3 - 2R_1 \end{matrix} \begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

$$\rightsquigarrow \begin{matrix} R_1 + 2R2 \\ R_2 \\ R_3 - R_2 \end{matrix} \begin{pmatrix} 1 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \rightsquigarrow \begin{matrix} R_1 \\ R_2 \\ 2^{-1}R_3 \end{matrix} \begin{pmatrix} 1 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\rightsquigarrow \begin{matrix} R_1 - R_3 \\ R_2 - R_3 \\ R_3 \end{matrix} \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

De laatst verkregen matrix hierboven noemen we a'. Laat nu $x = (x_1,x_2,x_3,x_4) \in F^4$. Dan geldt

$$a'\cdot x = \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 + 3x_3 \\ x_2 + 2x_3 \\ x_4 \end{pmatrix},$$

dus

$$x \in \ker(a'\cdot) \quad \Leftrightarrow \quad \begin{cases} x_1 + 3x_3 = 0, \\ x_2 + 2x_3 = 0, \\ x_4 = 0. \end{cases} \quad \Leftrightarrow \quad \begin{cases} x_1 = -3x_3, \\ x_2 = -2x_3, \\ x_4 = 0, \end{cases} \quad \Leftrightarrow \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = x_3 \cdot \begin{pmatrix} -3 \\ -2 \\ 1 \\ 0 \end{pmatrix}.$$

Dus is $(-3,-2,1,0)$ een basis van $\ker(a'\cdot) = \ker(a\cdot)$. ∎

De matrix a' in Voorbeeld VII.5.3 blijkt een speciale vorm te hebben, genaamd rijtrapvorm, die het makkelijk maakt om een basis van de kern te vinden. We geven nu een formele definitie van deze vorm, en ook van het begrip spil van een rij die niet nul is.

Definitie spil en rijtrapvorm

VII.5.4 Definitie. Laat a in $\mathrm{M}_{m,n}(F)$. Dan is a in *rijtrapvorm* als de rijen die nul zijn (als ze bestaan) onderaan staan, en het eerste niet nul element in een rij (de *spil* geheten) verder naar rechts staat dan de spillen in de rijen erboven.

In andere woorden, matrices in rijtrapvorm waarvan de spillen 1 zijn zijn van de volgende vorm:

$$\begin{array}{c} \\ 1 \\ 2 \\ \vdots \\ r \\ r+1 \\ \vdots \\ m \\ \\ \end{array} \begin{pmatrix} 0\cdots0 & 1 & *\cdots* & * & *\cdots* & * & *\cdots* \\ 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & * & *\cdots* \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 \end{pmatrix} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}$$
$$\begin{array}{ccccccc} & j_1 & & j_2 & \cdots & j_r & \end{array}$$

De getallen $r \in \{0,\ldots,m\}$, $j_1,\ldots,j_r \in \{1,\ldots,n\}$ hebben hier de volgende betekenis: r is het aantal rijen dat niet nul is, en voor iedere $i \in \{1,\ldots,r\}$ is (i,j_i) de positie van de spil in de i-de rij. Er geldt dus dat $a_{i,j} = 0$ als $i > r$ of $(i \leqslant r$ en $j < j_i)$, en voor $i \in \{1,\ldots,r\}$ dat $a_{i,j_i} = 1$.

Gereduceerde en rijtrapvorm

VII.5.5 Definitie. Laat a in $\mathrm{M}_{m,n}(F)$. Dan is a in *gereduceerde rijtrapvorm* als a in rijtrapvorm is, de spillen 1 zijn, en alle coëfficiënten boven de spillen 0 zijn.

Het is duidelijk hoe men van een $a \in \mathrm{M}_{m,n}(F)$ in rijtrapvorm door middel van rij-operaties een a' in gereduceerde rijtrapvorm maakt. De volgende stelling geeft een algoritme om van $a \in \mathrm{M}_{m,n}(F)$ door middel van rij-operaties een a' in rijtrapvorm te maken waarin de spillen 1 zijn, bovendien worden de posities van de spillen bepaald. Dit algoritme is de sleutel tot de meeste berekeningen met matrices.

Rijtrapvorm algoritme

VII.5.6 Stelling (Het rijtrapvorm-algoritme)**.** Laat $a \in \mathrm{M}_{m,n}(F)$. De volgende procedure levert in eindig veel elementaire rij-operaties een a' in rijtrapvorm op.

1. Zet $a' = a$, $r = 0$ en $j_0 = 0$.

2. [Op dit punt, $a'_{i,j} = 0$ als $(i > r$ en $j \leqslant j_r)$ of $(1 \leqslant i \leqslant r$ en $1 \leqslant j < j_i)$. Ook, $a'_{i,j_i} = 1$ voor $1 \leqslant i \leqslant r$.]
Als de $(r+1)$-de tot en met de m-de rijen van a' nul zijn, dan stop.

3. Vind de kleinste j zodat er een $i \in \{r+1,\ldots,m\}$ is met $a'_{i,j} \neq 0$. Vervang r door $r+1$, zet $j_r = j$, en als $r \neq i$ dan verwissel de r-de en de i-de rijen van a'. Merk op dat $j_r > j_{r-1}$.

4. Vermenigvuldig de r-de rij van a' met $(a'_{r,j_r})^{-1}$.

5. Voor alle $i = r+1,\ldots,m$, tel $-a'_{i,j_r}$ keer de r-de rij van a' bij de i-de rij van a' op.

6. Ga naar Stap 2.

Bewijs. Alle gebruikte operaties op a' zijn elementaire rij-operaties. Iedere keer als de lus in het algoritme wordt uitgevoerd wordt r 1 groter in stap 3. Als $r = m$ is, is aan de stop-voorwaarde in stap 2 voldaan, dus het algoritme stopt (termineert) gegarandeerd, na hoogstens m keer de lus te hebben uitgevoerd. We laten zien dat op het moment dat het algoritme stopt, a' in rijtrapvom is.

We controleren dat de claim aan het begin van stap 2 correct is. Dit is triviaal als stap 2 voor de eerste keer wordt bereikt. Nu nemen we aan dat de claim correct is als we in stap 2 zijn, en laten zien dat de claim dan ook correct is als we terugkomen in stap 2.

Aangezien de eerste r rijen niet veranderen in de lus is het deel van de claim dat over deze rijen gaat niet veranderd. In stap 3 verhogen we r met 1 en vinden we j_r (voor de nieuwe r) zodat $a'_{i,j} = 0$ als $i \geq r$ en $j < j_r$. Volgens onze aanname hebben we dan $j_r > j_{r-1}$. De operaties in stappen 3 en 4 produceren $a'_{r,j_r} = 1$. In stap 5 bereiken we dat voor $i > r$, $a'_{i,j_r} = 0$. Dus voor ($i > r$ en $j \leqslant j_r$) en als ($i = r$ en $j < j_r$) geldt dan $a'_{i,j} = 0$. Dit laat zien dat de claim in stap 2 weer correct is.

Dus na het termineren van het algoritme is de claim in stap 2 correct. We hebben ook gezien dat $0 < j_1 < j_2 < \cdots < j_r$. Dus is a' in rijtrapvorm, zijn, voor $i \in \{1,\ldots,r\}$, de (i, j_i) de posities van de spillen, en zijn de spillen 1. ∎

We zijn nu klaar voor de laatste stap van het berekenen van een basis van $\ker(a\cdot)$: het vinden van een basis als a in gereduceerde rijtrapvorm is. We beginnen met een voorbeeld (het algemene geval is alleen administratief minder makkelijk te doorgronden).

Basis van $\ker(a\cdot)$ voor a in gereduceerde rijtrapvorm

VII.5.7 Voorbeeld. Laat $F = \mathbb{Q}$ en laat

$$a = \begin{pmatrix} \textcircled{1} & 2 & 0 & 0 & 0 & 1 & -3 \\ 0 & 0 & \textcircled{1} & -1 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 & \textcircled{1} & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Merk op dat a in gereduceerde rijtrapvorm is, waarbij de spillen omcirkeld zijn. Dan geldt voor $x \in F^7$:

$$a\cdot x = \begin{pmatrix} 1 & 2 & 0 & 0 & 0 & 1 & -3 \\ 0 & 0 & 1 & -1 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} x_1 & +2x_2 & & & & +x_6 & -3x_7 \\ & & x_3 & -x_4 & & -x_6 & +2x_7 \\ & & & & x_5 & +x_6 & +x_7 \\ & & & & & & 0 \end{pmatrix},$$

dus

$$\begin{aligned} x \in \ker(a\cdot) \quad &\Leftrightarrow \quad \begin{cases} x_1 & +2x_2 & & & & +x_6 & -3x_7 & = 0 \\ & & x_3 & -x_4 & & -x_6 & +2x_7 & = 0 \\ & & & & x_5 & +x_6 & +x_7 & = 0 \end{cases} \\ &\Leftrightarrow \quad \begin{cases} x_1 &= & -2x_2 & +0x_4 & -x_6 & +3x_7 \\ x_3 &= & & x_4 & +x_6 & -2x_7 \\ x_5 &= & & & -x_6 & -x_7 \end{cases} \\ &\Leftrightarrow \quad \begin{cases} x_1 &= & -2x_2 & +0x_4 & -x_6 & +3x_7 \\ x_2 &= & x_2 & & & \\ x_3 &= & & x_4 & +x_6 & -2x_7 \\ x_4 &= & & x_4 & & \\ x_5 &= & & & -x_6 & -x_7 \\ x_6 &= & & & x_6 & \\ x_7 &= & & & & x_7 \end{cases} \\ &\Leftrightarrow \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = x_2\cdot \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_4\cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_6\cdot \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} + x_7\cdot \begin{pmatrix} 3 \\ 0 \\ -2 \\ 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}. \end{aligned}$$

Dus is $((-2,1,0,0,0,0,0),(0,0,1,1,0,0,0),(-1,0,1,0,-1,1,0),(3,0,-2,0,-1,0,1))$ een voortbrengend tupel van $\ker(a\cdot)$, want de vergelijkingen betekenen dat voor x in $\ker(a\cdot)$ de coördinaten x_2, x_4, x_6 en x_7 vrij gekozen kunnen worden (ze heten daarom ook de *vrije variabelen*), en dat daarmee x_1, x_3 en x_5, de *afhankelijke variabelen*, die horen bij de spillen, uniek bepaald zijn. Het voortbrengend tupel is zelfs een basis van $\ker(a\cdot)$, want onder de projectie

$$p\colon F^7 \to F^4, \quad (x_1,x_2,x_3,x_4,x_5,x_6,x_7) \mapsto (x_2,x_4,x_6,x_7)$$

is het beeld van het tupel gelijk aan $((1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1))$, de standaardbasis van F^4. ∎

De volgende stelling zegt dat we op de manier als in het bovenstaand bewijs voor elke $a \in \mathrm{M}_{m,n}(F)$ in gereduceerde rijtrapvorm een basis van de kern kunnen berekenen. Ter herinnering: $(e_1,\ldots,e_n)$ is de standaardbasis van F^n.

Basis van $\ker(a\cdot)$ algemeen

VII.5.8 Stelling. Als $a \in \mathrm{M}_{m,n}(F)$ in gereduceerde rijtrapvorm is, met r rijen ongelijk 0 en spillen in de kolommen $j_1 < \ldots < j_r$, dan vormen de $n-r$

$$w_k = e_k - \sum_{\substack{1 \leqslant i \leqslant r \\ j_i < k}} a_{i,k} e_{j_i}, \qquad \text{voor } k \in \{1,\ldots,n\} \setminus \{j_1,\ldots,j_r\}$$

een basis van $\ker(a\cdot)$.

Bewijs. Het bewijs kan geheel analoog aan het bewijs in Voorbeeld VII.5.7 gevoerd worden. ∎

Inhomogene stelsels

Nu we weten hoe we homogene stelstels lineaire vergelijkingen op kunnen lossen is het tijd om het onderwerp van *inhomogene* stelsels lineaire vergelijkingen aan te snijden. Deze hebben de volgende vorm:

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n &= b_1 \\ \qquad\vdots \qquad\qquad\quad &\vdots \quad\vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n &= b_m \end{cases} \qquad \text{met de } a_{i,j} \text{ en de } b_i \text{ in } F.$$

De oplossingsverzameling van dit stelsel is precies gelijk aan $(a\cdot)^{-1}\{b\}$, het inverse beeld van de 1-puntsverzameling $\{b\} \subseteq F^m$ onder de afbeelding $a\cdot\colon F^n \to F^m$. De volgende stelling zegt dat dit inverse beeld òf leeg is, òf de getransleerde is van de oplossingsverzameling van het bijbehorend homogene stelsel over een willekeurige 'particuliere oplossing' x_0.

particuliere en algemene oplossing

VII.5.9 Stelling. Laat $m,n \in \mathbb{N}$, $a \in \mathrm{M}_{m,n}(F)$ en $b \in F^m$. Stel dat $(a\cdot)^{-1}\{b\} \neq \varnothing$. Laat $x_0 \in (a\cdot)^{-1}\{b\}$. Dan geldt:

$$(a\cdot)^{-1}\{b\} = \{x_0 + y : y \in \ker(a\cdot)\} = x_0 + \ker(a\cdot).$$

Bewijs. We bewijzen beide inclusies. Stel dat $x \in (a\cdot)^{-1}\{b\}$. Laat $y = x - x_0$. Dan $a\cdot x = b$, en dus

$$a\cdot y = a\cdot(x - x_0) = a\cdot x - a\cdot x_0 = b - b = 0$$

dus $y \in \ker(a\cdot)$ en $x = x_0 + y$.

Stel nu dat $y \in \ker(a\cdot)$. Dan geldt

$$a\cdot(x_0 + y) = a\cdot x_0 + a\cdot y = b + 0 = b,$$

en dus $x_0 + y \in (a\cdot)^{-1}\{b\}$. ∎

Deze stelling reduceert het probleem van het oplossen van het inhomogene stelsel tot het oplossen van het homogene stelsel, en het bepalen van een particuliere oplossing of het laten zien dat die niet bestaat. Dit laatste geval kan inderdaad voorkomen, zoals de vergelijking $0\cdot x = 1$ laat zien (hier is $n = m = 1$); in dat geval heet het stelsel *strijdig*.

Gauss eliminatie lost ook dit probleem op: je veegt het stelsel door middel van rij-operaties, inclusief het inhomogene deel b, tot het in rijtrapvorm (of zelfs gereduceerde rijtrapvorm) is. Om niet de hele tijd de onnodige symbolen in de vergelijkingen op te schrijven werkt men met de m bij $n+1$ matrix verkregen door b als kolom achter a toe te voegen, en om te onthouden dat de laatste kolom 'inhomogeen' is, zet men een streep voor de laatste kolom:

$$\left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m,1} & \cdots & a_{m,n} & b_m \end{array}\right).$$

We geven twee voorbeelden, één waar er oplossingen zijn, en één waar er géén zijn.

Voorbeelden van inhomogene Gauss eliminatie

VII.5.10 Voorbeeld. We bekijken het inhomogene stelsel vergelijkingen $a\cdot x = b$, met $F = \mathbb{Q}$ en

$$a = \begin{pmatrix} -1 & 2 & 1 & 1 \\ 1 & -1 & 1 & 0 \\ 2 & -3 & 0 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} 3 \\ -1 \\ -4 \end{pmatrix}.$$

We reduceren de volgende matrix naar gereduceerde rijtrapvorm:

$$\begin{aligned} \left(\begin{array}{cccc|c} -1 & 2 & 1 & 1 & 3 \\ 1 & -1 & 1 & 0 & -1 \\ 2 & -3 & 0 & -1 & -4 \end{array}\right) &\rightsquigarrow \begin{array}{r} -R_1 \\ R_2 \\ R_3 \end{array} \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -3 \\ 1 & -1 & 1 & 0 & -1 \\ 2 & -3 & 0 & -1 & -4 \end{array}\right) \\ &\rightsquigarrow \begin{array}{r} R_1 \\ R_2 - R_1 \\ R_3 - 2R_1 \end{array} \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -3 \\ 0 & 1 & 2 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 \end{array}\right) \\ &\rightsquigarrow \begin{array}{r} R_1 \\ R_2 \\ R_3 - R_2 \end{array} \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -3 \\ 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \\ &\rightsquigarrow \begin{array}{r} R_1 + 2R_2 \\ R_2 \\ R_3 \end{array} \left(\begin{array}{cccc|c} 1 & 0 & 3 & 1 & 1 \\ 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right). \end{aligned}$$

Het stelsel $a\cdot x = b$ is dus equivalent met:

$$\begin{array}{rrrrl} x_1 & & +3x_3 & +x_4 & = 1 \\ & x_2 & +2x_3 & +x_4 & = 2. \end{array}$$

Een particuliere oplossing is dan $(1,2,0,0)$ (gebruik de *niet* vrije variabelen x_1 en x_2), en een basis van de oplossingsruimte van het homogene stelsel is

$$((-3,-2,1,0),(-1,-1,0,1)).$$

De oplossingsruimte is dus $\{(1,2,0,0) + \lambda\cdot(-3,-2,1,0) + \mu\cdot(-1,-1,0,1)\}$, wat we ook kunnen schrijven als

$$\{(1-3\lambda-\mu, 2-2\lambda-\mu, \lambda, \mu) : \lambda, \mu \in \mathbb{Q}\}.$$

VII.5.11 Voorbeeld. Nu bekijken we het inhomogene stelsel vergelijkingen $a \cdot x = b$, met $F = \mathbb{Q}$ en

$$a = \begin{pmatrix} -1 & 2 & 1 & 1 \\ 1 & -1 & 1 & 0 \\ 2 & -3 & 0 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

We reduceren de volgende matrix naar gereduceerde rijtrapvorm:

$$\left(\begin{array}{cccc|c} -1 & 2 & 1 & 1 & 1 \\ 1 & -1 & 1 & 0 & 1 \\ 2 & -3 & 0 & -1 & 1 \end{array}\right) \begin{matrix} -R_1 \\ R_2 \\ R_3 \end{matrix} \rightsquigarrow \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 \\ 2 & -3 & 0 & -1 & 1 \end{array}\right)$$

$$\begin{matrix} R_1 \\ R_2 - R_1 \\ R_3 - 2R_1 \end{matrix} \rightsquigarrow \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -1 \\ 0 & 1 & 2 & 1 & 2 \\ 0 & 1 & 2 & 1 & 3 \end{array}\right)$$

$$\begin{matrix} R_1 \\ R_2 \\ R_3 - R_2 \end{matrix} \rightsquigarrow \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -1 \\ 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

Het stelsel $a \cdot x = b$ is strijdig, want de laatste vergelijking is $0 = 1$. Er zijn dus geen oplossingen. ∎

Opgaven

1. Bereken hoeveel rij-operaties maximaal gedaan moeten worden om een m bij n matrix in rijtrapvorm te krijgen. En idem met gereduceerde rijtrapvorm.

2. Laat $F = \mathbb{Q}$. Voor elk van de volgende stelsels lineaire vergelijkingen, vind een matrix a en een vector b zodat het equivalent is met $a \cdot x = b$, en beschrijf de oplossingsverzameling. Om breuken te vermijden kan het handig zijn om door geschikte rij-operaties op nuttige plaatsen eerst een coëfficiënt 1 te maken.

$$\begin{cases} 2x_1 + 3x_2 - 2x_3 = 0 \\ 3x_1 + 2x_2 + 2x_3 = 0 \\ -x_2 + 2x_3 = 0 \end{cases}$$

$$\begin{cases} 2x_1 + 3x_2 - 2x_3 = 1 \\ 3x_1 + 2x_2 + 2x_3 = -1 \\ -x_2 + 2x_3 = -1 \end{cases}$$

$$\begin{cases} 2x_1 + 3x_2 - 2x_3 = 1 \\ 3x_1 + 2x_2 + 2x_3 = 1 \\ -x_2 + 2x_3 = 1 \end{cases}$$

$$\begin{cases} 3x_1 + x_2 + 2x_3 - 2x_4 = 1 \\ 2x_1 - x_2 + 2x_3 = 2 \\ x_1 + x_3 = 3 \\ -2x_1 - x_2 - x_3 + x_4 = 4 \end{cases}$$

3. Laat nu $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, het lichaam met 2 elementen. Los de stelsels uit de vorige opgave op, maar nu met coëfficiënten en variabelen in $\mathbb{F}_2$. Wie dan nog fut heeft kan het ook nog voor $F = \mathbb{F}_3$ uitwerken.

4. De formule voor trinitrotolueen (TNT) is $C_7H_5N_3O_6$. Als het ontploft, dan kan het ontbinden in N_2, H_2O, CO en C. Bepaal de reactie:

$$a \cdot C_7H_5N_3O_6 \to b \cdot N_2 + c \cdot H_2O + d \cdot CO + e \cdot C.$$

5. Laat $F = \mathbb{Q}$. Bepaal het snijpunt van de lijn door de punten $(-1,0,1)$ en $(2,3,4)$ met het vlak door de punten $(2,1,3)$, $(1,3,2)$ en $(2,2,2)$.

6. Laat $n \in \mathbb{N}$, F een lichaam, en $a \in \mathrm{M}_n(F)$ van rang n.

(a) Laat zien dat de gereduceerde rijtrapvorm van a de identiteitsmatrix is.

(b) Laat zien dat voor iedere b in F^n het stelsel $a \cdot x = b$ een unieke oplossing heeft.

(c) Laat zien dat a inverteerbaar is: er is een c in $\mathrm{M}_n(F)$ met $ac = ca = 1_n$.

(d) Laat zien dat zo'n c uniek is. Notatie: a^{-1}.

(e) Kun je a^{-1} berekenen door één geschikte matrix naar gereduceerde rijtrapvorm te brengen? (Hoe groot is die matrix?)

7. (Deze opgave is moeilijker! Moskou, wiskunde-olympiade, 1949.) Een boer heeft 101 koeien, en voor elk van deze koeien kunnen de overige 100 in twee groepen van 50 worden verdeeld zodat elke groep hetzelfde totale gewicht heeft. Bewijs dat alle koeien even zwaar zijn. Hint: het gaat om de rang van een 101 bij 101 matrix die je niet eens weet, maar kijk eens of een ander lichaam uitkomst biedt...

8. Laat $n \in \mathbb{N}$, $a \in \mathrm{M}_n(\mathbb{Z})$ een matrix met coëfficiënten in de ring $\mathbb{Z}$. Dan kunnen we a opvatten als een element $a_{\mathbb{Q}}$ van $\mathrm{M}_n(\mathbb{Q})$, maar ook, voor ieder priemgetal p, als element a_p van $\mathrm{M}_n(\mathbb{F}_p)$. Bewijs dat voor elk priemgetal p geldt dat de rang van a_p hoogstens de rang van $a_{\mathbb{Q}}$ is, en dat voor bijna alle p er gelijkheid is. Hint: met rij- en kolom-operaties zonder delen kun je a omzetten in een a' die diagonaal is, met $a'_{1,1}|a'_{2,2}|\cdots|a'_{n,n}$.

VII.6 Een leuke toepassing: lights out

Lineaire algebra is één van de werkpaarden van de wiskunde: een basistechniek die in veel situaties gebruikt kan worden. Het is de algemene theorie achter stelsels lineaire vergelijkingen. Meestal is het wel duidelijk of je met lineaire vergelijkingen te maken hebt of niet. Maar het komt ook wel voor het lineaire karakter van een probleem niet meteen duidelijk is. Een voorbeeld daarvan is het spel 'lights out'.

De klassieke variant van dit spel is een veld van 5 bij 5 lampjes die tegelijkertijd knoppen zijn. Elk lampje kan aan of uit zijn, dus er zijn $2^{25} > 32 \cdot 10^6$ mogelijke toestanden. Als je op een knop drukt, dan verandert dat lampje van toestand, maar ook naaste buren. We geven hier enkele voorbeelden, waarin we 'uit' weergeven met 0 en 'aan' met 1, en waar we de knoppen nummeren als coëfficiënten van een matrix:

knop $(1,1)$:
$$\begin{bmatrix} 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1&1&0&0&0\\ 1&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{bmatrix}$$

knop $(2,1)$:
$$\begin{bmatrix} 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1&0&0&0&0\\ 1&1&0&0&0\\ 1&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{bmatrix}$$

knop $(2,2)$:
$$\begin{bmatrix} 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 0&1&0&0&0\\ 1&1&1&0&0\\ 0&1&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{bmatrix}$$

De opgave is dan om bij een gegeven begintoestand de knoppen zo in te drukken dat alle lampjes uitgaan. Een beetje nadenken laat zien dat dit een probleem

is dat met lineaire algebra over $\mathbb{F}_2$ aangepakt kan worden. Laat namelijk V de $\mathbb{F}_2$-vectorruimte zijn van alle functies $f\colon \{1,2,3,4,5\}\times\{1,2,3,4,5\}\to\mathbb{F}_2$. Dit is de verzameling van de toestanden waarin de lampjes zich kunnen bevinden. De knop (i,j) geeft dan een element $f_{i,j}\in V$:

$$\begin{aligned} f_{i,j}(k,l) &= 1 \quad \text{als } |k-i|+|l-j|\leq 1 \\ &= 0 \quad \text{anders.} \end{aligned}$$

Het indrukken van de knop (i,j) geeft dan de afbeelding

$$V\to V,\quad f\mapsto f+f_{i,j}.$$

Omdat optellen associatief en commutatief is, maakt het niet uit in welke volgorde we een aantal knoppen indrukken, dat is op zich al opmerkelijk. Om een gegeven toestand f uit te krijgen moet f dus geschreven worden als lineaire combinatie van de $f_{i,j}$. Met andere woorden, we zoeken $x_{i,j}\in\mathbb{F}_2$ zodat $\sum_{i,j}x_{i,j}f_{i,j}=f$. En dat is een inhomogeen stelsel lineaire vergelijkingen over $\mathbb{F}_2$ met 25 onbekenden en 25 vergelijkingen (bekijk de functiewaarden in alle (k,l)).

Omdat het veel werk is een 25 bij 25 matrix met de hand te vegen, raden we de lezer aan om een kleinere variant te proberen: het 3 bij 3 geval. We verklappen daarbij dat in dat geval iedere beginsituatie op te lossen is. Wie het 3 bij 5 geval analyseert zal zien dat daar niet alle beginsituaties op te lossen zijn: de deelruimte voortgebracht door de $f_{i,j}$ is dan van dimensie 12. Dit betekent dat de 3 bij 5 puzzel makkelijk opgelost kan worden in de situtaties waarin dat mogelijk is.

Er is veel geschreven over lights out. Laten we volstaan met te verwijzen naar de mooie website van Jaap Scherphuis. Om het spel te spelen:

`http://www.jaapsch.net/puzzles/lights.htm#java`.

En de wiskunde erover:

`http://www.jaapsch.net/puzzles/lomath.htm`.

VII.7 Meer over lineaire algebra

Volgend jaar meer.

VIII APPENDIX

VIII.1 Redeneerregels

VIII.2 De Axioma's van Zermelo en Fraenkel

We geven hier een zeer korte beschrijving van de formele taal van verzamelingentheorie en het ZFC axiomastelsel. Voor meer details zie [Da-Do-Sw], waar deze beschrijving deels op is geïnspireerd.

symbolen

In de verzamelingenleer gebruiken we letters (variabelen, aftelbaar oneindig veel) en de logische symbolen ($\forall$, $\exists$, $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftarrow$, en $\Leftrightarrow$), het $=$-teken (gelijkheid) en natuurlijk $\in$ (is element van).

interpretatie

De interpretatie van de logische symbolen is als volgt: $\forall$ is "voor alle", $\exists$ is "er is een", $\wedge$ is "en", $\vee$ is "of", $\neg$ is "niet", $\Rightarrow$ is "impliceert", $\Leftarrow$ is "is gevolg van", $\Leftrightarrow$ is "dan en slechts dan", of ook wel "precies dan als" of ook wel "is equivalent met". Als men wil, dan kan men zuiniger zijn met het aantal logische symbolen (bijvoorbeeld kunnen ze allemaal in $\wedge$ en $\neg$ uitgedrukt worden). Verder is elk individu dat we tegenkomen een verzameling (de variabelen staan voor verzamelingen). In het bijzonder zijn de elementen van al onze verzamelingen zelf dus ook weer verzamelingen.

formules

Formules in de taal van verzamelingenleer zijn als volgt gedefiniëerd:

1. de atomaire formules zijn van de vorm $A \in B$ of $A = B$, waarbij A en B variabelen zijn;
2. als φ en ψ formules zijn, dan ook $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $\neg\varphi$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftarrow \psi)$, en $(\varphi \Leftrightarrow \psi)$;
3. als φ een formule is en A een variabele dan zijn ook $\forall A\,\varphi$ en $\exists A\,\varphi$ formules;
4. iedere formule wordt in eindig veel stappen opgebouwd uit de atomaire formules via de stappen 2 en 3.

Axioma's

We zijn nu klaar om de axioma's te formuleren. Het zijn er negen. We geven eerst een beschrijving en soms wat toelichting in gewone taal en vervolgens de formule, en voeren daarna soms wat notatie in.

Extensionaliteit

Verzamelingen zijn gelijk dan en slechts dan als ze dezelfde elementen hebben.

$$\big(A = B \Leftrightarrow \forall X\,(X \in A \Leftrightarrow X \in B)\big).$$

Paarvorming

Voor elk tweetal verzamelingen A en B is er een verzameling die uit alleen de elementen A en B bestaat.

$$\forall A\,\forall B\,\exists C\,\forall X\,\big(X \in C \Leftrightarrow (X = A \vee X = B)\big).$$

Deze verzameling C wordt ook wel als $\{A, B\}$ genoteerd.

Vereniging

Voor elke verzameling A bestaat een verzameling die uit alle elementen van elementen van A bestaat.

$$\forall A\,\exists B\,\forall X\,\big(X \in B \Leftrightarrow \exists Y\,(Y \in A \wedge X \in Y)\big)$$

Voor deze B gebruiken we de notatie $\cup_{Y \in A} Y$.

Machtsverzameling Voor elke verzameling A bestaat een verzameling die uit alle deelverzamelingen van A bestaat.

$$\forall A\,\exists B\,\forall X\,\big(X \in B \Leftrightarrow \forall Y\,(Y \in X \Rightarrow Y \in A)\big).$$

We gebruiken hiervoor de notatie $\mathscr{P}(A)$.

Afscheiding Dit is een axioma-schema. Voor iedere formule φ en voor iedere verzameling A is er een verzameling die bestaat uit alle elementen van A die aan φ voldoen. Voor iedere formule φ hebben we het axioma

$$\forall A\,\exists B\,\forall X\,(X \in B \Leftrightarrow (X \in A \wedge \varphi)).$$

Substitutie Dit is ook een axioma-schema. Als φ een formule is die een "afbeelding" F definieert, dat wil zeggen uit $\varphi(X,Y)$ en $\varphi(X,Z)$ volgt $Y = Z$ en we noteren $Y = F(X)$, dan bestaat voor elke verzameling A de beeldverzameling $F(A)$. Voor iedere formule φ en variabele B die niet in φ voorkomt hebben we het axioma

$$\forall X\,\exists! Y\,\varphi \Rightarrow \forall A\,\exists B\,\forall Y\,\big(Y \in B \Leftrightarrow \exists X\,(X \in A \wedge \varphi)\big).$$

Merk op dat we stiekem het symbool $\exists!$ hebben gebruikt, anders paste het axioma niet op één regel.

We geven een voorbeeld. We nemen voor φ de formule "Y is de machtsverzameling van X". Dan volgt dat voor iedere A er een B bestaat waarvan de elementen precies de machtsverzamelingen van de elementen van A zijn.

Oneindigheid De axioma's hierboven zijn nog niet sterk genoeg om ons oneindige verzamelingen te geven; die moeten we expliciet postuleren. We gebruiken het symbool $\varnothing$ voor de lege verzameling.

$$\exists A\,\big(\varnothing \in A \wedge \forall X\,(X \in A \Rightarrow X \cup \{X\} \in A)\big).$$

Zo'n verzameling A is 'oneindig' want de afbeelding $S\colon A \to A$, $X \mapsto X \cup \{X\}$ is injectief maar niet surjectief.

Regulariteit Elke niet-lege verzameling heeft een $\in$-minimaal element.

$$\forall A\,\big(A \neq \varnothing \Rightarrow \exists B\,(B \in A \wedge \forall C\,(C \in B \Rightarrow C \notin A))\big).$$

Regulariteit zegt dat niet alles een verzameling kan zijn (denk aan Russels paradox); het verhindert het bestaat van oneindige rijtjes van de vorm $X_0 \ni X_1 \ni X_2 \ni \cdots$.

Keuze Elke verzameling S van niet-lege verzamelingen heeft een keuzefunctie, dat wil zeggen, er is een functie $f : S \to \cup_{X \in S} X$ zó dat voor alle $X \in S$ geldt $f(X) \in X$.

We schrijven dit axioma niet in de formele taal, want dat wordt te lang.

Geschiedenis De bovenstaande axioma's vormen het axioma-systeem van Zermelo (Duits wiskundige, 1871–1953) en Fraenkel (Duits en Israëlisch wiskundige, 1891–1965), uitgebreid met het keuzeaxioma, het geheel ook wel afgekort tot ZFC (de 'C' staat voor 'choice').

Hier en nu In dit dictaat werken we in een model van ZFC.

VIII.3 Axioma's van Peano

De axioma's van Peano (Italiaans wiskundige, 1858-1932) vormen een korte karakterisering van de natuurlijke getallen met de operaties optelling en vermenigvuldiging. In plaats van direct naar de operaties '+' en '·' te kijken, beschouwt men de afbeelding $S\colon \mathbb{N} \to \mathbb{N}$ gegeven door $a \mapsto a+1$. Deze afbeelding S heet de *opvolger*-afbeelding (de S staat voor de Engelse term 'successor'). De *gegevens* zijn dan:

(a) een verzameling $\mathbb{N}$;
(b) een element $0 \in \mathbb{N}$;
(c) een afbeelding $S\colon \mathbb{N} \to \mathbb{N}$.

Deze gegevens moeten voldoen aan de volgende *axioma's*:

(P0) er is geen $a \in \mathbb{N}$ met $S(a) = 0$;
(P1) de afbeelding S is injectief;
(P2) (axioma van inductie) als $A \subseteq \mathbb{N}$ de eigenschappen heeft dat $0 \in A$ en dat $a \in A \Rightarrow S(a) \in A$, dan $A = \mathbb{N}$.

Uniciteit

De volgende stelling laat zien dat een gegeven $(\mathbb{N}, 0, S)$ uniek door Peano's axioma's wordt bepaald. Informeel zegt de stelling dat elk tweetal realisaties van Peano's axioma's op administratie na hetzelfde zijn. Formeel zegt de stelling dat elk tweetal realisaties 'uniek isomorf' zijn.

VIII.3.1 Stelling. Stel dat de gegevens $(\mathbb{N}, 0, S)$ en $(\mathbb{N}', 0', S')$ aan de axioma's P0, P1 en P2 voldoen. Dan is er een unieke bijectie $f\colon \mathbb{N} \to \mathbb{N}'$ is zodat $f(0) = 0'$, en zodat voor alle $a \in \mathbb{N}$ geldt $f(S(a)) = S'(f(a))$.

Bewijs. We definiëren de afbeelding $f\colon \mathbb{N} \to \mathbb{N}'$ met recursie, dat wil zeggen, we passen Stelling IV.3.1 toe met $X = \mathbb{N}'$, $x = 0'$ en $F = S'$. Dat geeft ons een unieke $f\colon \mathbb{N} \to \mathbb{N}'$ met $f(0) = 0'$ en met $\forall a(a \in \mathbb{N} \Rightarrow f(S(a)) = S'(f(a)))$.

Om te laten zien dat f bijectief is maken we een afbeelding f' die de inverse van f zal zijn. We passen Stelling IV.3.1 toe op het gegeven $(\mathbb{N}', 0', S')$ (dat immers aan Peano's axioma's voldoet) met $X = \mathbb{N}$, $x = 0$ en $F = S$. Dat geeft ons een unieke $f'\colon \mathbb{N}' \to \mathbb{N}$ met $f'(0') = 0$ en met $\forall a(a \in \mathbb{N}' \Rightarrow f'(S'(a)) = S(f'(a)))$.

Voor de samenstelling $f' \circ f\colon \mathbb{N} \to \mathbb{N}$ geldt dan $(f' \circ f)(0) = f'(f(0)) = f'(0') = 0$ en, ook dat voor alle $a \in \mathbb{N}$ dat

$$(f' \circ f)(S(a)) = f'(f(S(a))) = f'(S'(f(a))) = S(f'(f(a))) = S((f' \circ f)(a)).$$

Maar deze twee eigenschappen gelden ook voor $\mathrm{id}_{\mathbb{N}}$. Stelling IV.3.1, toegepast op $(\mathbb{N}, 0, S)$ met $X = \mathbb{N}$ en $x = 0$ en $F = S$ zegt dat er een unieke afbeelding is met deze twee eigenschappen, en dus dat $f' \circ f = \mathrm{id}_{\mathbb{N}}$.

Omdat onze aannamen op $(\mathbb{N}, 0, S)$ en $(\mathbb{N}', 0', S')$ hetzelfde zijn, geeft hetzelfde argument maar dan met de twee verwisseld dat $f \circ f' = \mathrm{id}_{\mathbb{N}'}$. We hebben bewezen dat f bijectief is, want f heeft een inverse afbeelding. ■

Van Peano naar $(\mathbb{N}, 0, 1, +, \cdot)$

Voorts kan men dan, gebruikmakend van de recursiestelling, bewijzen dat er unieke afbeeldingen $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ en $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ bestaan zodat voor alle $a, b \in \mathbb{N}$ geldt:

(P3) $0 + a = a$;
(P4) $S(a) + b = S(a + b)$;
(P5) $0 \cdot a = 0$;
(P6) $S(a) \cdot b = a \cdot b + b$.

Men definieert dan $1 = S(0)$, en dan kan men bewijzen dat het gegeven $(\mathbb{N}, 0, 1, +, \cdot)$ aan alle eigenschappen N0 tot en met N11 van sectie IV.1 voldoet. We gaan dit programma nu uitvoeren.

VIII.3.2 Stelling. Laat $(\mathbb{N}, 0, S)$ voldoen aan P0, P1 en P2. Dan is er een unieke afbeelding $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ die voldoet aan P3 en P4.

Bewijs. We moeten voor (a, b) in $\mathbb{N} \times \mathbb{N}$ definiëren wat $a + b$ is, zodat voldaan is aan P3 en P4. We doen dit eerst 'voor vaste b' (want $S(a)$ komt voor in P4). Laat daartoe $b \in \mathbb{N}$. Dan moeten we een functie $s_b : \mathbb{N} \to \mathbb{N}$ definiëren. In deze notatie zijn P3 en P4 equivalent met: $s_b(0) = b$ en $s_b(S(a)) = S(s_b(a))$. Stelling IV.3.1 toegepast met $X = \mathbb{N}$, $x = b$ en $F = S$ geeft ons dat er een unieke functie s_b is met deze eigenschappen. We kunnen $a + b$ dus definiëren als $s_b(a)$:

$$a + b := s_b(a).$$

■

VIII.3.3 Stelling. Laat $(\mathbb{N}, 0, S)$ voldoen aan P0, P1 en P2, en laat $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ de afbeelding zijn als in Stelling VIII.3.2. Dan is er een unieke afbeelding $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ zodat $(\mathbb{N}, +, \cdot)$ voldoet aan P3, P4, P5 en P6.

Bewijs. We moeten voor (a, b) in $\mathbb{N} \times \mathbb{N}$ definiëren wat $a \cdot b$ is. We doen dit eerst 'voor vaste b' (want $S(a)$ komt in P6 voor). Laat daartoe $b \in \mathbb{N}$. Dan moeten we een functie $v_b : \mathbb{N} \to \mathbb{N}$ definiëren. In deze notatie zijn P5 en P6 equivalent met: $v_b(0) = 0$ en $v_b(S(a)) = v_b(a) + b$. Stelling IV.3.1 toegepast met $X = \mathbb{N}$, $x = 0$ en $F = s_b$ geeft ons dat er een unieke functie v_b is met deze eigenschappen. We kunnen $a \cdot b$ dus definiëren als $v_b(a)$:

$$a \cdot b := v_b(a).$$

■

VIII.3.4 Stelling. Laat $(\mathbb{N}, 0, S)$ voldoen aan P0, P1 en P2, en laat $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ de afbeelding zijn als in Stelling VIII.3.2 en $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ als in Stelling VIII.3.3. Laat $1 = S(0)$. Dan voldoet $(\mathbb{N}, 0, 1, +, \cdot)$ aan N0 tot en met N10.

Bewijs. We beginnen met N0. We moeten bewijzen dat voor alle a en b in $\mathbb{N}$ geldt dat $a + b = b + a$. We gaan dit doen met inductie naar b. Maar eerst bewijzen we het volgende lemma.

VIII.3.5 Lemma. Laat $(\mathbb{N}, 0, S)$ voldoen aan P0, P1 en P2, en laat $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ de afbeelding zijn als in Stelling VIII.3.2. Voor alle a en b in $\mathbb{N}$ geldt

$$a + S(b) = S(a + b).$$

Bewijs. Laat $b \in \mathbb{N}$. Inductie naar a. Voor $a = 0$ geldt het:

$$\begin{aligned} 0 + S(b) &= S(b) && \text{P3 met S(b)} \\ S(b) &= S(0 + b) && \text{P3 met } b\text{, dan } S. \end{aligned}$$

Laat nu a in $\mathbb{N}$ en neem aan dat $a + S(b) = S(a + b)$. Dan geldt

$$\begin{aligned} S(a) + S(b) &= S(a + S(b)) && \text{P4 met } a \text{ en } S(b) \\ S(a + S(b)) &= S(S(a + b)) && \text{inductiehypothese, dan } S \\ S(S(a + b)) &= S(S(a) + b) && \text{P4 met } a \text{ en } b\text{, dan } S \end{aligned}$$

Het bewijs van het lemma is nu af. ■

We gaan nu verder met het bewijs van N0. Met Inductie naar b bewijzen we '$\forall a \in \mathbb{N},\ a+b=b+a$'.

Stap 1: $b=0$. Vanwege P3 geldt $0+a=a$. We bewijzen met inductie naar a dat '$\forall a \in \mathbb{N},\ a+0=a$'. Substap 0: $0+0=0$ vanwege P3. Substap 1. Laat $a \in \mathbb{N}$ en neem aan dat $a+0=a$. Dan

$$\begin{aligned} S(a)+0 &= S(a+0) && \text{P4 met } a \text{ en } 0\\ S(a+0) &= S(a) && \text{inductiehypothese, dan } S. \end{aligned}$$

We hebben nu bewezen '$\forall a \in \mathbb{N},\ a+0=0+a$'. Stap 1 is af.

Stap 2: laat $b \in \mathbb{N}$ en neem aan dat '$\forall a \in \mathbb{N},\ sa+b=b+a$'. Laat $a \in \mathbb{N}$. Dan geldt

$$\begin{aligned} a+S(b) &= S(a+b) && \text{voorgaande Lemma}\\ S(a+b) &= S(b+a) && \text{inductiehypothese, dan } S\\ S(b+a) &= S(b)+a && \text{P4 met } b \text{ en } a. \end{aligned}$$

Het bewijs van N0 is hiermee afgerond.

We bewijzen nu N1, de associativiteit van $+$. Alhoewel deze uitspraak drie variabelen heeft en N0 maar twee, hebben we hiervan een korter bewijs dan voor N0. Laat b en c in $\mathbb{N}$. We bewijzen met inductie naar a dat '$\forall a \in \mathbb{N},\ (a+b)+c=a+(b+c)$'. Stap 1. Voor $a=0$ hebben we

$$\begin{aligned} (0+b)+c &= b+c && \text{P3 met } b, \text{ dan } +c\\ b+c &= 0+(b+c) && \text{P3 met } b+c. \end{aligned}$$

Stap 2. Laat $a \in \mathbb{N}$ en neem aan dat $(a+b)+c=a+(b+c)$. Dan geldt

$$\begin{aligned} (S(a)+b)+c &= S(a+b)+c && \text{P4 met } a \text{ en } b, \text{ dan } +c\\ S(a+b)+c &= S((a+b)+c) && \text{P4 met } a+b \text{ en } c\\ S((a+b)+c) &= S(a+(b+c)) && \text{inductiehypothese}\\ S(a+(b+c)) &= S(a)+(b+c) && \text{P4 met } a \text{ en } b+c. \end{aligned}$$

Het bewijs van N1 is nu afgerond. Het bewijs van N2 is triviaal nu we N0 al hebben. We bewijzen nu N3: '$\forall a,b,c \in \mathbb{N},\ a+b=a+c \Rightarrow b=c$'. Laat b en c in $\mathbb{N}$. We bewijzen met inductie naar a: '$\forall a \in \mathbb{N},\ a+b=a+c \Rightarrow b=c$'. Stap 1: voor $a=0$ is het waar: neem aan dat $0+b=0+c$ en merk op dat $0+b=b$ en $0+c=c$. Stap 2. Laat $a \in \mathbb{N}$ en neem aan '$a+b=a+c \Rightarrow b=c$'. We moeten nu bewijzen dat '$S(a)+b=S(a)+c \Rightarrow b=c$'. Neem dus aan dat $S(a)+b=S(a)+c$. Vanwege P4 hebben we dan $S(a+b)=S(a+c)$. De injectiviteit van S (P1) geeft dat $a+b=a+c$. De inductiehypothese geeft nu $b=c$. Het bewijs van N3 is klaar.

Het bewijs van N4: 1 is in $S(\mathbb{N})$ per definitie van 1, en 0 niet vanwege P0. Voor N5: vanwege P0 is 0 niet in $S(\mathbb{N})$. Voor N6: dat is P2.

Nu zijn N7–N10 aan de beurt. Voor de bewijzen van N7 en N8 kunnen we de bewijzen van N0 en N1 aanpassen, want de definities en de te bewijzen uitspraken hebben dezelfde vorm voor de vermenivuldiging als voor de optelling: operaties die voldoen aan P5 en P6 in plaats van P3 en P4, commutativiteit en associativiteit voor vermenigvuldiging in plaats van optelling. We schrijven hier dus niet alles meer uit, en we gebruiken wat we al over de optelling weten.

We bewijzen N7: '$\forall a,b \in \mathbb{N},\ b\cdot a=a\cdot b$'. Het analogon van het lemma in het bewijs van N0 is:

$$\forall a,b \in \mathbb{N},\ a\cdot S(b)=a\cdot b+a.$$

Het bewijs van dit lemma laten we aan de lezer over. Nu doen we een 'copy-paste-adapt' van het bewijs van N0 (men zegt wel: mutatis mutandis). Met inductie naar b bewijzen we '$\forall a \in \mathbb{N},\ a\cdot b=b\cdot a$'.

Stap 1: $b = 0$. P5 zegt '$\forall a \in \mathbb{N},\ 0{\cdot}a = 0$'. We bewijzen met inductie naar a dat '$\forall a \in \mathbb{N},\ a{\cdot}0 = 0$'. Stap 1: voor $a = 0$ is dit P5. Stap 2. Laat $a \in \mathbb{N}$ en neem aan dat $a{\cdot}0 = 0$. Dan hebben we

$$\begin{aligned} S(a){\cdot}0 = a{\cdot}0 + 0 &\quad \text{P6 met } a \text{ en } 0 \\ a{\cdot}0 + 0 = 0 + 0 &\quad \text{inductiehypothese} \\ 0 + 0 = 0 &\quad \text{P3 met } 0. \end{aligned}$$

We hebben nu bewezen '$\forall a \in \mathbb{N},\ a{\cdot}0 = 0{\cdot}a$'.

Stap 2: laat $b \in \mathbb{N}$ en neem aan dat '$\forall a \in \mathbb{N},\ a{\cdot}b = b{\cdot}a$'. Laat $a \in \mathbb{N}$. Dan geldt

$$\begin{aligned} a{\cdot}S(b) = a{\cdot}b + a &\quad \text{analogon van het lemma} \\ a{\cdot}b + a = b{\cdot}a + a &\quad \text{inductiehypothese, dan } +a \\ b{\cdot}a + a = S(b){\cdot}a &\quad \text{P6 met } b \text{ en } a. \end{aligned}$$

Het bewijs van N7 is hiermee afgerond. We bewijzen nu eerst N10 want we gebruiken N10 in ons bewijs van N8. Omdat we N7 (commutativiteit van vermenigvuldiging) al hebben, is N10 equivalent met '$\forall a, b, c \in \mathbb{N},\ (b + c){\cdot}a = b{\cdot}a + c{\cdot}a$'. Laat $a, c \in \mathbb{N}$. We bewijzen met inductie naar b dat '$\forall b \in \mathbb{N},\ (b + c){\cdot}a = b{\cdot}a + c{\cdot}a$'. Stap 1: het is waar voor $b = 0$:

$$\begin{aligned} (0 + c){\cdot}a = c{\cdot}a &\quad \text{P3 met } c, \text{ dan } {\cdot}a \\ c{\cdot}a = 0 + c{\cdot}a &\quad \text{P3 met } c{\cdot}a \\ 0 + c{\cdot}a = 0{\cdot}a + c{\cdot}a &\quad \text{P5 met } a, \text{ dan } +c{\cdot}a. \end{aligned}$$

Stap 2: laat $b \in \mathbb{N}$ en neem aan dat $(b + c){\cdot}a = b{\cdot}a + c{\cdot}a$. Dan:

$$\begin{aligned} (S(b) + c){\cdot}a = S(b + c){\cdot}a &\quad \text{P4 met } b \text{ en } c, \text{ dan } {\cdot}a \\ S(b + c){\cdot}a = (b + c){\cdot}a + a &\quad \text{P6 met } b + c \text{ en } a \\ (b + c){\cdot}a + a = (b{\cdot}a + c{\cdot}a) + a &\quad \text{inductiehypothese, dan } +a \\ (b{\cdot}a + c{\cdot}a) + a = (b{\cdot}a + a) + c{\cdot}a &\quad \text{N1 en N0} \\ (b{\cdot}a + a) + c{\cdot}a = S(b){\cdot}a + c{\cdot}a &\quad \text{P6 met } b \text{ en } a, \text{ dan } +c{\cdot}a. \end{aligned}$$

Hiermee is N10 bewezen.

We bewijzen nu N8: '$\forall a, b, c \in \mathbb{N},\ (a{\cdot}b){\cdot}c = a{\cdot}(b{\cdot}c)$'. Laat b en c in $\mathbb{N}$. We bewijzen met inductie naar a dat '$\forall a \in \mathbb{N},\ (a{\cdot}b){\cdot}c = a{\cdot}(b{\cdot}c)$'. Stap 1. We hebben

$$\begin{aligned} (0{\cdot}b){\cdot}c = 0{\cdot}c &\quad \text{P5 met } b, \text{ dan } {\cdot}c \\ 0{\cdot}c = 0 &\quad \text{P5 met } c \\ 0 = 0{\cdot}(b{\cdot}c) &\quad \text{P5 met } b{\cdot}c. \end{aligned}$$

Stap 2. Laat nu $a \in \mathbb{N}$ en neem aan dat $(a{\cdot}b){\cdot}c = a{\cdot}(b{\cdot}c)$. Dan geldt

$$\begin{aligned} (S(a){\cdot}b){\cdot}c = (a{\cdot}b + b){\cdot}c &\quad \text{P6 met } a \text{ en } b, \text{ dan } {\cdot}c \\ (a{\cdot}b + b){\cdot}c = (a{\cdot}b){\cdot}c + b{\cdot}c &\quad \text{N10 en N0} \\ (a{\cdot}b){\cdot}c + b{\cdot}c = a{\cdot}(b{\cdot}c) + b{\cdot}c &\quad \text{inductiehypothese} \\ a{\cdot}(b{\cdot}c) + b{\cdot}c = S(a){\cdot}(b{\cdot}c) &\quad \text{P6 met } a \text{ en } b{\cdot}c. \end{aligned}$$

Het bewijs van N8 is nu afgerond. Uitspraak N9 volgt direct uit de commutativiteit van de vermenigvuldiging en

$$\begin{aligned} 1{\cdot}b = S(0){\cdot}b &\quad \text{definitie van } 1 \\ S(0){\cdot}b = 0{\cdot}b + b &\quad \text{P6 met } 0 \text{ en } b \\ 0{\cdot}b + b = 0 + b &\quad \text{P5 met } b, \text{ dan } +b \\ 0 + b = b &\quad \text{P3 met } b. \end{aligned}$$

■

Van ZFC naar Peano

De standaardmanier om, uitgaand van ZFC, een tripel $(\mathbb{N}, 0, S)$ te maken dat voldoet aan Peano's axioma's **P0**, **P1** en **P2**, is als volgt. Laat A een verzameling zijn als in het Axioma van Oneindigheid. Laat dan $\mathbb{N}$ de doorsnede zijn van alle deelverzamelingen B van A met de eigenschap dat $\varnothing \in B$ en dat $(X \in B) \Rightarrow (X \cup \{X\} \in B)$. Voor het bestaan van die doorsnede, gebruik het Axioma van Machtsverzameling (om de machtsverzameling $\mathscr{P}(A)$ te krijgen), het Afscheidingsaxioma (om de verzameling C van de $B \in \mathscr{P}(A)$ met de gewenste eigenschap te krijgen), en nogmaals het Afscheidingsaxioma (om de deelverzameling $\mathbb{N}$ van A te krijgen, bestaand uit die a die in alle $B \in C$ zitten). Voor $0 \in \mathbb{N}$ neemt men dan $\varnothing$, en voor $X \in \mathbb{N}$ definiëert men $S(X) = X \cup \{X\}$. In deze realisatie geldt bijvoorbeeld dat:

- $0 = \varnothing$,
- $1 = S(0) = 0 \cup \{0\} = \{\varnothing\}$,
- $2 = S(1) = 1 \cup \{1\} = \{\varnothing, \{\varnothing\}\}$,
- $3 = S(2) = 2 \cup \{2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$,
- $4 = S(3) = 3 \cup \{3\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\}$.

Het is duidelijk zijn dat dit systeem als notatie voor getallen bijzonder inefficiënt is, maar het is bijzonder mooi door de eigenschap dat voor iedere $n \in \mathbb{N}$ geldt dat $n = \{0, 1, \ldots, n-1\}$.

VIII.3.6 Stelling. De hierboven geconstrueerde $(\mathbb{N}, 0, S)$ voldoet aan P0, P1 en P2.

Bewijs. We beginnen met P0. Aangezien $0 = \varnothing$ en voor alle verzamelingen X geldt dat $S(X)$ niet leeg is (X is zelf een element van $S(X)$) is 0 geen opvolger.

Dan P2: S is injectief. We doen dit uit het ongerijmde. Stel dat X en Y verzamelingen zijn met $X \neq Y$, en dat $S(X) = S(Y)$. Dan is X een element van $S(Y)$, en dus een element van Y (want $X \neq Y$). Maar net zo is Y een element van X. Maar dan heeft de verzameling $\{X, Y\}$ geen $\in$-minimaal element en dat is in tegenspraak met het regulariteitsaxioma.

Tenslotte P2, het axioma van inductie. Laat $A \subseteq \mathbb{N}$ met $\varnothing \in A$ en zodat $\forall X$, $X \in A \to X \cup \{X\} \in A$. We moeten bewijzen dat $A = \mathbb{N}$. Vanwege de definitie van $\mathbb{N}$ als de doorsnede van alle verzamelingen B die voldoen aan

$$\varnothing \in A \text{ en } \forall X, X \in A \Rightarrow X \cup \{X\} \in A$$

geldt dat $\mathbb{N} \subseteq A$, dus $A = \mathbb{N}$ want de andere inclusie hadden we al.

■

ANTWOORDEN EN UITWERKINGEN

Paragraaf I.1.

2. (a) 12;
(b) 3;
(c) 1;
(d) 1;
(e) 2.

3. (a) $\{0,1\}$, $\{0\}$, $\{1\}$, $\varnothing$;
(b) $\{0,1,2\}$, $\{1,2\}$, $\{0,2\}$, $\{0,1\}$, $\{2\}$, $\{0\}$, $\{1\}$, $\varnothing$;
(c) $\{0,1,2,3\}$, $\{1,2,3\}$, $\{0,2,3\}$, $\{0,1,3\}$, $\{0,1,2\}$, $\{0,3\}$,$\{1,3\}$,$\{2,3\}$, $\{1,2\}$,$\{0,2\}$, $\{0,1\}$,$\{3\}$, $\{2\}$, $\{0\}$,$\{1\}$,$\varnothing$;
(d) Een verzameling van n elementen heeft precies 2^n deelverzamelingen, want voor elk element kun je kiezen of die wel of niet in de deelverzameling zit. Merk op dat bij opgaven a, b en c het aantal deelverzamelingen van V verdubbelt als je een element toevoegt aan V.

4. (a) niet waar;
(b) niet waar;
(c) niet waar;
(d) niet waar;
(e) waar;
(f) waar.

5. Laat A een verzameling zijn. We bewijzen dat $\varnothing \subseteq A$. Dat is equivalent met: ieder element van $\varnothing$ is element van A. Aangezien $\varnothing$ geen element heeft is dat waar. Een andere formulering is: er zijn geen elementen van $\varnothing$ die *niet* in A zitten. Nu bewijzen we dat $A \subseteq A$. Dat is equivalent met: ieder element van A is element van A. En dat is waar.

7. $A = \varnothing$ of $B = \varnothing$ of $A = B$. Om de equivalentie te bewijzen kan men gevallen onderscheiden: $A = \varnothing$ of $B = \varnothing$ of ($A \neq \varnothing$ en $B \neq \varnothing$).

8. $\mathscr{P}(A) = \{\{0,1\},\{0\},\{1\},\varnothing\}$ ($2^2 = 4$ elementen).
$\mathscr{P}(B) = \{\{\varnothing\},\varnothing\}$ ($2^1 = 2$ elementen).
$\mathscr{P}(A) \times \mathscr{P}(B) = \{(\{0,1\},\varnothing),(\{0,1\},\{\varnothing\}),(\{0\},\varnothing),(\{0\},\{\varnothing\}),(\{1\},\varnothing),(\{1\},\{\varnothing\}),(\varnothing,\varnothing),(\varnothing,\{\varnothing\})\}$
($4 \cdot 2 = 8$ elementen).

Paragraaf I.2.

1. (a) We laten eerst zien dat voor iedere $x \in \Omega \setminus (A \cap B)$ geldt dat ook $x \in (\Omega \setminus A) \cup (\Omega \setminus B)$. Stel dus $x \in \Omega \setminus (A \cap B)$. Er zijn twee mogelijkheden: ofwel $x \notin A$ of $x \in A$. In het eerste geval geldt $x \in \Omega \setminus A$ en dus ook $x \in (\Omega \setminus A) \cup (\Omega \setminus B)$. In het tweede geval moet gelden $x \notin B$ (gezien onze aanname dat $x \in \Omega \setminus (A \cap B)$). Dus $x \in \Omega \setminus B$ en dan ook weer $x \in (\Omega \setminus A) \cup (\Omega \setminus B)$.
Nu laten omgekeerd zien dat als $x \in (\Omega \setminus A) \cup (\Omega \setminus B)$ dan ook $x \in \Omega \setminus (A \cap B)$. Laat $x \in (\Omega \setminus A) \cup (\Omega \setminus B)$. We weten dat $x \in \Omega \setminus A$ of $x \in \Omega \setminus B$. In het eerste geval geldt dat $x \notin A$ en dus ook $x \notin A \cap B$, dus $x \in \Omega \setminus (A \cap B)$. Het geval $x \in \Omega \setminus B$ gaat net zo.
(b) We laten door equivalenties zien dat de twee verzamelingen dezelfde elementen hebben. Laat $x \in \Omega$. Dan zijn equivalent:

$$
\begin{aligned}
& x \in \Omega \setminus (A \cup B) && \\
& x \notin A \cup B && \text{vanwege definitie van complement,} \\
& x \notin A \quad \text{en} \quad x \notin B && \text{definitie vereniging,} \\
& x \in \Omega \setminus A \quad \text{en} \quad x \in \Omega \setminus B && \text{definitie complement,} \\
& x \in (\Omega \setminus A) \cap (\Omega \setminus B) && \text{definitie doorsnede.}
\end{aligned}
$$

2. (a) $\Omega \setminus (A \cap B \cap C) = (\Omega \setminus A) \cup (\Omega \setminus B) \cup (\Omega \setminus C)$.
(b) $\Omega \setminus (A \cup B \cup C) = (\Omega \setminus A) \cap (\Omega \setminus B) \cap (\Omega \setminus C)$.

6. (a) $\bigcup_{k\in K} A_k = \{1,4,16\}$ en $\bigcap_{k\in K} A_k = \varnothing$.
(b) $\bigcup_{k\in K} A_k = [0,5]$ en $\bigcap_{k\in K} A_k = \varnothing$.
(c) $\bigcup_{k\in K} A_k = (1,\infty)$ en $\bigcap_{k\in K} A_k = (4,\infty)$.

7. (a) $[1,2] = \{x \in \mathbb{R} : 1 \leqslant x \leqslant 2\}$
(b) $(0,3) = \{x \in \mathbb{R} : 0 < x < 3\}$

8. (a) Deze vraag is wat vaag. Maar er geldt dat $(A \cup B) \setminus (A \cup C) \subseteq A \cup (B \setminus C)$, en dat $(A \cup (B \setminus C)) \setminus ((A \cup B) \setminus (A \cup C)) = A$ (gebruik een venndiagram).
(b) Precies dan als $A = \varnothing$.

9. Men vindt met het venndiagram dat de verzameling gelijk is aan $A \cap B$. Het kan ook zonder venndiagram. Merk op dat volgens de Morgan geldt dat $C^{\mathrm{c}} \cup D^{\mathrm{c}} = (C \cap D)^{\mathrm{c}}$, dus $C^{\mathrm{c}} \cup D^{\mathrm{c}} \cup (C \cap D) = \Omega$. Laat $x \in \Omega$. Dan zijn equivalent:

$$\begin{aligned}
x &\in (A \cap B \cap C^c) \cup (A \cap B \cap D^c) \cup (A \cap B \cap C \cap D) \\
\big(x \in A \cap B \wedge x \in C^{\mathrm{c}}\big) &\vee \big(x \in A \cap B \wedge x \in D^{\mathrm{c}}\big) \vee (x \in A \cap B \wedge x \in C \cap D) \\
(x \in A \cap B) &\wedge \big(x \in C^{\mathrm{c}} \vee x \in D^{\mathrm{c}} \vee x \in C \cap D\big) \\
(x \in A \cap B) &\wedge x \in \big((C^{\mathrm{c}} \cup D^{\mathrm{c}} \cup (C \cap D)\big) \\
(x \in A \cap B) &\wedge x \in \Omega \\
x &\in A \cap B\,.
\end{aligned}$$

Paragraaf I.3.

1. 1, $(x-1)/(x+1)$, $(1+x)/(1-x)$.

2. (a) $f(x) = x^2 - 7x + 7$;
(b) $1/x + \sqrt{1+x^2}/|x|$.

3. $\{\pm\sqrt{k\pi} : k \in \mathbb{N}\}$; $\{\pm\sqrt{3\pi/2 + 2k\pi} : k \in \mathbb{N}\}$; $\varnothing$.

4. (a) nee.
(b) ja.
(c) nee.
(d) ja.

5. (a) 9.
(b) 1.
(c) 0 als A niet leeg is en 1 als A wel leeg is.

9. (a) waar;
(b) niet waar;
(c) niet waar;
(d) waar.

10. niet waar; niet waar

12. (b) $B = (-5,-4]$, $g^{-1}(x) = 1/(x+5)$

13. (a) $B = \mathbb{R}$, $g(x) = (3+x)/7$;
(b) $B = [0,\infty)$, $g(x) = -\sqrt{x}$;
(c) $B = \mathbb{R} \setminus \{-1\}$, $g(x) = (1-2x)/(1+x)$;
(d) $B = [0,1]$, $g(x) = -\sqrt{1-x^2}$.

Paragraaf I.4.

Paragraaf I.5.

Paragraaf I.6.

Paragraaf II.1.

1. (a) $(P \vee Q) \wedge \neg(P \wedge Q)$ (bewijs: waarheidstabel)
(b) $P \vee Q$ is equivalent met $(P \veebar Q) \veebar (P \wedge Q)$ (bewijs: waarheidstabel)

Paragraaf II.2.

1. (a) $\exists_{n\in\mathbb{Z}}(x = n + n)$.
(b) $(x > 1) \wedge (\forall_{r\in\mathbb{N}} \forall_{s\in\mathbb{N}}(x = rs \Rightarrow (r = 1 \vee s = 1)))$.

Paragraaf II.3.

Paragraaf II.4.

1. (a) Van een definitie, omdat zo (althans in de schoolwiskunde) het getal π wordt geïntroduceerd. Hierbij wordt echter (in schoolboeken vaak impliciet) gebruik gemaakt van een aantal stellingen:

- iedere cirkel heeft een welgedefinieerde omtrek (voor de introductie van reële getallen was dit niet zo — de Grieken moesten hier heel voorzichtig mee omgaan!);
- de verhouding tussen omtrek en diameter is voor iedere cirkel hetzelfde (dit kun je bewijzen met gebruik van het concept vergrotingsfactor);
- de omtrek is niet gelijk aan nul en de verhouding van twee reële getallen bestaat (met andere woorden, je kunt twee reële getallen delen).

(b) Dit is een stelling. N.B. Een bewijs van deze stelling kan in de schoolwiskunde, althans voor de introductie van limieten, niet worden gegeven. Dat wil niet zeggen dat het onmogelijk is om argumenten te geven die de stelling geloofwaardig maken, zoals het opknippen van een schijf in een aantal taartpunten, om hier vervolgens bij benadering een rechthoek van te leggen.

Paragraaf III.1.

1. (a) $(x^3) + (2x^2) + (3x) + 4$.
(b) Nu moet je een volgorde kiezen, bijvoorbeeld van links naar rechts:

$$\Big(\big((x^3) + (2x^2)\big) + (3x)\Big) + 4.$$

4. $(a + b)^c = a^c + b^c$. Dit is een vorm van distributiviteit. (Terzijde: als je 'modulo c' rekent en c is een priemgetal, dan geldt deze regel wel voor tot-de-macht-c!

7. (a) $2 \uparrow 1 = 2$, $2 \uparrow 2 = 4$, $2 \uparrow 3 = 16$ en $2 \uparrow 4 = 65536$.
(b) 2^{65536} is een getal dat is decimale notatie uit 19729 decimale cijfers bestaat. Want $\log_{10}(2^{65536}) = 65536 \cdot \log 2 \approx 19729$.
(c) Nee: $(2 \uparrow 2) \uparrow 2 = 4 \uparrow 2 = 4^4 = 256$, terwijl$2 \uparrow (2 \uparrow 2) = 2 \uparrow 4 = 65536$.
(d) Nee, uit het vorige antwoord blijkt dat $4 \uparrow 2 \neq 2 \uparrow 4$.
(e) Omdat $(a^a)^a = a^{(a^2)}$. Zouden de haakjes andersom staan, dan geldt $a \uparrow b = a^{(a^b)}$ en dit kan dus gewoon in de bekende notatie worden uitgedrukt.

8. Het intuïtieve idee van oneindig is dat van een 'heel groot getal'. Als we dit aangeven met het symbool ∞, dan moet gelden $\infty + a = a + \infty = \infty$ voor iedere $a \in \mathbb{Z}_\infty$. Op deze manier blijven commutativiteit en associativiteit van optelling geldig, maar kan het element ∞ geen inverse voor optelling hebben. Sterker nog, door de toevoeging van oneindig is de oplossing van de vergelijking $a + x = b$, als deze bestaat, niet altijd uniek!

Vermenigvuldigen geeft nog grotere problemen. Want wat is $-1 \cdot \infty$? Als het gelijk is aan ∞, dan lijkt distributiviteit niet meer op te gaan (want $\infty = \infty + \infty = (1 - 1) \cdot \infty = 0 \cdot \infty$). Als er een tweede soort oneindig, namelijk $\infty' = -\infty$ wordt toegevoegd, dan is het weer niet duidelijk hoe optellen werkt (want wat is $1 + \infty + -\infty = (1 + \infty) + -\infty = \infty - \infty$?)
Kortom: door toevoegen van oneindig gaan veel rekenregels de mist in.

Paragraaf III.2.

Paragraaf IV.2.

1. Zij $a \in \mathbb{N}$ met $a \neq 0$. We laten eerst zien dat ten minste één $b \in \mathbb{N}$ bestaat met $a = b + 1$. Beschouw

$$A = \{0\} \cup \{n \in \mathbb{N} : \text{er is een } m \in \mathbb{N} \text{ met } n = m + 1\}.$$

Blijkbaar $0 \in A$. Als $n \in A$, dan zeker $n \in \mathbb{N}$, en dus $n + 1 \in A$. Volgens **(N6)** geldt nu $A = \mathbb{N}$. Aangezien $a \neq 0$, en ook $a \in A$, is er een $b \in \mathbb{N}$ met $a = b + 1$.
Nu moeten we bewijzen dat ten hoogste één zo'n $b \in \mathbb{N}$ bestaat. Neem aan dat $a \neq 0$, en $a = b + 1$ en $a = b' + 1$. Volgens **(N0)** geldt $b + 1 = 1 + b$ en $b' + 1 = 1 + b'$. Bijgevolg $1 + b = 1 + b'$ en volgens **(N3)** geldt $b = b'$.

5. $(n + 1)^2$

10. STAP 1: Het getal $11^0 - 4^0 = 1 - 1 = 0$ is deelbaar door 7.
STAP 2: Stel dat $11^n - 4^n$ deelbaar is door 7 voor een natuurlijk getal n. Dan geldt:

$$\begin{aligned} 11^{n+1} - 4^{n+1} &= 11 \cdot 11^n - 4 \cdot 4^n \\ &= 7 \cdot 11^n + 4 \cdot 11^n - 4 \cdot 4^n \\ &= 7 \cdot 11^n + 4(11^n - 4^n). \end{aligned}$$

Uit de inductieveronderstelling volgt dat $11^n - 4^n$ deelbaar is door 7, dus het getal $7 \cdot 11^n + 4 \cdot (11^n - 4^n)$ is ook deelbaar door 7.

15. nee

16. In STAP 2 moeten we bewijzen dat *voor elke* $n \geqslant 1$ geldt: 'als P_n waar is dan is ook P_{n+1} waar.' Maar de implicatie $P_1 \Rightarrow P_2$ is niet juist.

Paragraaf V.1.

1. We laten voor het gemak de index $_R$ uit de notatie weg.
(ii) $(a + b) + ((-a) + (-b)) = (a + (-a)) + (b + (-b)) = 0 + 0 = 0$ en dus is $(-a) + (-b)$ een inverse van $a + b$; maar de inverse van een element is uniek en dus $(-a) + (-b) = -(a + b)$.
(iii) $(-a) + a = 0$ en dus is a een inverse van $-a$; omdat de inverse uniek is volgt $a = -(-a)$.
(iv) $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$ en dus is $(-a)b$ een inverse van ab; vanwege uniciteit volgt weer $-(ab) = (-a)b$.
(v) volgt uit combinatie van (iv) en (iii).

8. Zij $f : R \to S$ een bijectief homomorfisme (van ringen). Om f bijectief is, bestaat er een inversefunctie $f^{-1} : S \to R$; we moeten laten zien dat f^{-1} een homomorfisme is. Zij dus $a, b \in S$. Omdat f een homomorfisme is, geldt

$$f^{-1}(a + b) = f^{-1}(f(f^{-1}(a)) + f(f^{-1}(b))) = f^{-1}(f(f^{-1}(a) + f^{-1}(b))) = f^{-1}(a) + f^{-1}(b).$$

Paragraaf V.2.

1. Tellen we links en rechts van de gelijkheid $-ac$ op, dan krijgen we $0 = ab - ac = a(b - c)$. Dus zegt Stelling V.2.3 dat $a = 0$ of $b - c = 0$. Dit laatste is equivalent aan $b = c$.

Paragraaf V.3.

3. W, W, W, W, W, O, W, O, W, W, O ($a = -b$ kan ook), W, O, W, W, O ($b = 0$ vormt de enige uitzondering), O, O. Als voorbeeld bewijzen we (o). Er geldt $b = ma$ en $c = na$ voor zekere $m, n \in \mathbb{Z}$. Daaruit volgt $b + c = (m + n)a$, hetgeen laat zien dat $a | (b + c)$.

4. (a) Waar, want ieder getal is deelbaar door -1.
(b) Waar. Dit geldt alleen voor $a = 0$.
(c) Niet waar. Het is waar als bovendien $p \neq q$.
(d) Waar. Delers van a zijn ook delers van een veelvoud van a.

7. We gebruiken de notatie voorafgaand aan de stelling. Zij $d \in D_a \cap D_b$; dan geldt $a = sd$ en $b = td$ voor zeker $s, t \in \mathbb{Z}$. Er is ook een $q \in \mathbb{Z}$ waarvoor geldt $a = qb + r$. Combinatie geeft

$$r = a - qb = sd - qtd = (s - qt)d.$$

Hieruit volgt $d | r$ en dus $d \in D_r$. Hiermee is aangetoond dat $D_a \cap D_b \subseteq D_b \cap D_r$. Op analoge wijze volgt $D_b \cap D_r \subseteq D_a \cap D_b$ en dus $D_b \cap D_r = D_a \cap D_b$.

9. (a) Er geldt $54 = 2 \cdot 3^3$. Iedere deler van 54 is dus van de vorm $2^i 3^j$ met $i \in \{0,1\}$ en $j \in \{0,1,2,3\}$.
(b)

$\times$	2^0	2^1	2^2	2^3
5^0	1	2	4	8
5^1	5	10	20	40
5^2	25	50	100	200

(c) $19800 = 2^3 3^2 5^2 11^1$. Dat geeft $4 \cdot 3 \cdot 3 \cdot 2 = 72$ delers.
(d) $105 = 3 \cdot 5 \cdot 7$. Het kleinste getal is $2^6 3^4 5^2$. De getallen 2^{104}, $2^{14}3^6$, ... zijn alle groter.
(e) $10 = 5 \cdot 2$, dus het gaat om getallen van de vorm $p^4 q$ of p^9, met p, q priem en $p \neq q$. Maar p^9 is te groot. Blijft over:

- $p = 2$ en $q \in \{3,5,7,11\}$; dit geeft 48, 80, 112 en 176.
- $p = 3$ en $q = 2$; dit geeft 162.

10. (a) Als $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ een priemontbinding is van n, dan is $p_1^{2a_1} p_2^{2a_2} \ldots p_r^{2a_r}$ een priemontbinding van n^2.
(b) Dan komt ieder priemgetal in n-voud voor (dus p_i^{kn}).

12. Er geldt:

$$\begin{aligned}(3^{100} + 2^{100}, 3^{100} - 2^{100}) &= (3^{100} - 2^{100}, 3^{100} + 2^{100} - (3^{100} - 2^{100})) \\ &= (3^{100} - 2^{100}, 2^{101}).\end{aligned}$$

Dit is gelijk aan 1, want $3^{100} - 2^{100}$ is niet even en alle delers $\neq \pm 1$ van 2^{101} zijn even.

13. De ggd van a en b deelt ook $a - b$ en is daarmee dus ook de ggd van a, b en $a - b$. Hieruit volgt dat de ggd van de getallen waarmee je begint ook de ggd is van de getallen waarmee je eindigt. De vraag is nog waarom je aan het einde de ggd hebt gevonden: in dit geval, waarom is 6 deler van alle getallen in de rij? Antwoord: Als een van de getallen, n, niet deelbaar zou zijn door 6, dan is de rest van deling van n door 6 een getal kleiner dan 6 en ongelijk 0. Dit zou nog een nieuw getal in het rijtje opleveren.

14. Zie `http://www.youtube.com/watch?v=lZ64IR2bz5o`. Hoewel Willis waarschijnlijk door slim gokken op het antwoord komt, zou je dit probleem (en soortgelijke) prima met het uitgebreide euclidische algoritme kunnen oplossen.

15. (a) Bijvoorbeeld: Het *kleinste* positieve, gehele getal d dat zowel gedeeld wordt door a als door b, heet het kleinste gemene veelvoud van a en b. Voorwaarde is dat a of b niet gelijk is aan nul. (Een definitie waarin $d = 0$ is toegestaan, is niet correct.) Alternatief: Bekijk de verzameling K_x van natuurlijke getallen die een veelvoud zijn van x. Dan is het kgv van a en b het kleinste positieve getal in $K_a \cap K_b$.
(b) Afhankelijk van de keuze die je maakt, geldt altijd $\text{kgd}(a,b) = 1$ of $\text{kgd}(a,b) = -\text{ggd}(a,b)$.

(c) Gemeenschappelijke veelvouden (van getallen ongelijk aan 0) kunnen willekeurig groot worden. Er is dus geen 'grootste' gemeenschappelijk veelvoud.
(d) Voor alle gehele getallen $a, b > 0$ geldt $\text{ggd}(a,b) \cdot \text{kgv}(a,b) = a \cdot b$. Om dit te bewijzen, kun je bijvoorbeeld alle priemgetallen p aflopen. Als i de hoogste macht is waarvoor $p^i | a$ en j de hoogste macht waarvoor $p^j | b$, dan is de hoogste macht van p die de ggd deelt het minimum van i en j, terwijl de hoogste macht die het kgv deelt juist het maximum is. Maar nu geldt $i + j = \min(i,j) + \max(i,j)$.

Paragraaf V.4.

Paragraaf V.5.

2. We doen een stukje, namelijk de controle dat we een equivalentierelatie hebben:

i) *reflexiviteit:* $a + b = a + b$, dus $(a,b) \sim (a,b)$;

ii) *symmetrie:* als $(a,c) \sim (b,d)$, dan $a + d = b + c$ en dus ook $(b,d) \sim (a,c)$;

iii) *transitiviteit:* als $(a,c)\sim(b,d)$ en $(b,d)\sim(e,f)$, dan $a+d=b+c$ en $b+f=e+d$, waaruit volgt $a+d+b+f=b+c+e+d$ hetgeen equivalent is met $a+f=c+e$, oftewel $(a,c)\sim(e,f)$.

Voor compatibiliteit

5. Voor distributiviteit is het voldoende dit op het niveau van representanten van equivalentieklassen te controleren:

$$\begin{aligned}(a,b)\cdot\big((c,d)+(e,f)\big) &= (a,b)\cdot(c+e,d+f) = \big(a(c+e)+b(d+f),a(d+f)+b(c+e)\big)\\ &= (ac+bd+ae+bf,ad+bc+af+be) = (ac+bd,ad+bc)+(ae+bf,af+be)\\ &= (a,b)\cdot(c,d)+(a,b)\cdot(e,f).\end{aligned}$$

Paragraaf V.6.

Paragraaf VI.1.

4. Nu gaan we na dat er inderdaad sprake is van een inverse. Als A een dedekindsnede is, dan geldt

$$gf(A)=\{x\in Q : x<\sup(A)\}.$$

Als $x\in A$ dan geldt natuurlijk $x\in\mathbb{Q}$ en $x<\sup(A)$ en dus $x\in gf(A)$, waaruit volgt dat $A\subseteq gf(A)$. Is omgekeerd $x\in gf(A)$ terwijl $x\notin A$, dan is x een bovengrens van A, in tegenspraak met $x<\sup(A)$. Dus ook $gf(A)\subseteq A$ en dus $A=gf(A)$. Als $r\in R$ dan geldt

$$fg(r)=\sup\{x\in\mathbb{Q} : x<r\}.$$

Stel dat dit supremum niet gelijk is aan r. Dan geldt $r'<r$, maar volgens Stelling VI.1.5 is er een $x\in\mathbb{Q}$ zodat $r'<x<r$; tegenspraak.

Paragraaf VI.2.

2. We tonen aan dat de rij uit Opgave VI.2.1 (b) naar 1 convergeert. Zij $\varepsilon>0$ willekeurig. We moeten een $N\in\mathbb{N}$ vinden zó dat voor alle $n\geqslant N$ geldt

$$\left|\frac{n}{n+1}-1\right|<\varepsilon.$$

Er geldt

$$\left|\frac{n}{n+1}-1\right| = \left|\frac{n-(n+1)}{n+1}\right| = \left|\frac{1}{n+1}\right| = \frac{1}{n+1}.$$

Volgens Archimedische Eigenschap is er een $N\in\mathbb{N}$ met $N>\frac{1}{\varepsilon}-1$. We laten zien dat deze N als gewenst is. Kies $n\in\mathbb{N}$ met $n\geqslant N$ willekeurig. Dan geldt $1/(n+1)\leq 1/(N+1)<\varepsilon$. Dus

$$\left|\frac{n}{n+1}-1\right| = \frac{1}{n+1}\leqslant\frac{1}{N+1}<\varepsilon.$$

5. $\lim_{n\to\infty} a_n = 0$

9. *Aanwijzing:* Bewijs met volledige inductie dat $a_n=n$ als n even is, en $a_n=n-2$ als n oneven is.

10. (a) *Aanwijzing*: Redeneer uit het ongerijmde.

11. Zij $\varepsilon>0$. Kies $N_1\in\mathbb{N}$ zó dat voor alle $n\geq N_1$ geldt dat $|x_{2n}-x|<\varepsilon$. Kies $N_2\in\mathbb{N}$ zó dat voor alle $n\geq N_2$ geldt dat $|x_{2n+1}-x|<\varepsilon$. Kies $N=1+2\max\{N_1,N_2\}$. Kies $k\geq N$ wilekeurig. Er zijn twee mogelijkehden (1) k is even of (2) k is oneven. (1): Laat $k=2n$ met $n\in\mathbb{N}$. Dan geldt $n\geq N/2\geq N_1$ en dus

$$|x_k-x| = |x_{2n}-x|<\varepsilon.$$

(2): Laat $k=2n+1$ met $n\geq 1$, dan geldt $n\geq N/2\geq N_2$ en dus

$$|x_k-x| = |x_{2n+1}-x|<\varepsilon.$$

Dit bewijst dat $\lim_{k\to\infty} x_k = x$.

12. (a): Neem aan dat $|x|>1$. We kunnen een $h>0$ vinden zó dat $|x|=1+h$. Uit de ongelijkheid van Bernoulli (zie Opgave **??**) volgt dat

$$|x^n| = |x|^n = (1+h)^n\geq 1+nh.$$

Hier volgt dat $(x^n)_{n\geq 0}$ niet begrensd is, en dus divergent.

Paragraaf VI.3.

2. (a) $0,\overline{27}$; (b) $0,\overline{230769}$; (c) $0,6\overline{32}$; (d) $5,\overline{0}$

3. (a) $\frac{4234231}{10000000}$; (b) $\frac{3211}{9999}$; (c) $\frac{1909}{900}$

Paragraaf VI.4.

4. Zij $((_n)_{n\geqslant 0}a)$ een convergente rij in A. Zij $a \in A$ de limiet. Zij $\varepsilon > 0$ gegeven. Volgens de definitie van convergentie bestaat er dan een $N \in \mathbb{N}$ zodat $\mathrm{d}(a_n, a) < \frac{1}{2}\varepsilon$ voor alle $n \geqslant N$. Zij nu $m, n \geqslant N$. Dan volgt uit de driehoeksongelijkheid:

$$\mathrm{d}(a_n, a_m) \leqslant \mathrm{d}(a_n, a) + \mathrm{d}(a_m, a) < \varepsilon.$$

Paragraaf VI.5.

3. (c) We bewijzen dat f continu is in elke $c > 0$; als $c < 0$ is het bewijs analoog en het geval $c = 0$ wordt in onderdeel (a) aangetoond.
Zij $\varepsilon > 0$, we zoeken een $\delta > 0$ zó dat voor elke $x \in \mathbb{R}$ met $|x - c| < \delta$ geldt $|x^2 - c^2| < \varepsilon$. Merk eerst op: als $0 < x < 2c$ dan

$$|x^2 - c^2| = |x + c| \cdot |x - c| = (x + c) \cdot |x - c| < 3c \cdot |x - c|,$$

en

$$3c \cdot |x - c| < \varepsilon \qquad \Leftrightarrow \qquad |x - c| < \frac{\varepsilon}{3c}.$$

Kies $\delta = \min\{c, \varepsilon/3c\}$, we moeten nu laten zien dat de zo gekozen δ werkt.
Zij $x \in \mathbb{R}$ met $|x - c| < \delta$. Omdat $\delta \leqslant c$ geldt er $0 < x < 2c$, en dus

$$|x^2 - c^2| < 3c \cdot |x - c| < 3c \cdot \delta \leqslant 3c \cdot \frac{\varepsilon}{3c} = \varepsilon.$$

5. ja

7. (a) waar
(b) niet waar

12. (a) We bewijzen dat $\lim_{x\to 0} f(x) = 0$. We bewijzen dat $\lim_{x\to 0} f(x) = 0$. Zij $\varepsilon > 0$ willekeurig. Kies $\delta = 2007$. Dan is $\delta > 0$ en voor alle $x \in (-1, 1)$ met $x \neq 0$ met $|x - 0| = |x| < \delta$ geldt

$$\big|f(x) - 0\big| = |0 - 0| = 0 < \varepsilon;$$

merk op dat $f(x) = 0$ omdat $x \neq 0$.
(b) Als f continu in 0 is dan moet volgens Stelling **??** voor elke rij $(x_n)_{n\in\mathbb{N}}$ in $(-1, 1)$ met $\lim_{n\to\infty} x_n = 0$ gelden dat $\lim_{n\to\infty} f(x_n) = f(0) = 1$. Neem $x_n = 1/(n + 1)$. De rij $(1/(n + 1))_{n\in\mathbb{N}}$ is in $(-1, 1)$ en $\lim_{n\to\infty} 1/(n + 1) = 0$ maar

$$\lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} f\left(\frac{1}{n+1}\right) = 0 \neq 1 = f(0).$$

Conclusie: f is niet continu in 0.

13. Beschouw de rij $(1/(n + 1))_{n\geq 0}$. De rij is in $\mathbb{R} \setminus \{0\}$ en convergeert naar 0 maar

$$(f\left(\frac{1}{n+1}\right))_{n\geq 0} = (n + 1)_{n\geq 0}$$

is niet convergent. Conclusie de limiet bestaat niet.

Paragraaf VII.1.

1. (a)
(b) Voor alle $f \in V$ en voor alle $x \in X$: $(-f)(x) = -f(x)$.
(c) Als $V \neq \{0\}$ dan is niet voldaan aan V5. Aan alle andere axioma's is wel voldaan.
(d) Dan $V = \{0\}$.
(e) Nee, want per definitie bevat een vectorruimte een element 0.

5. (a) Ja, $0_V = 1$.
(b) Laat $f : V \to \mathbb{R}$, $v \mapsto v - 1$. Dan is f inverteerbaar, de inverse is $f^{-1} : \mathbb{R} \to V$, $x \mapsto x + 1$, en voor alle v en w in V geldt $v +_V w = f^{-1}(f(v) + f(w))$. Als F een lichaam is, V een F-vectorruimte, W een verzameling en $f : W \to V$ een bijectieve afbeelding, dan kun je de F-vectorruimte structuur van V naar W 'transporteren' via f en f^{-1}.

Paragraaf VII.2.

Paragraaf VII.3.

4. Het antwoord hangt van F af. Als $2 \neq 0$ in F dan $\dim(W) = 0$, en anders $\dim(W) = 1$.

Paragraaf VII.4.

Paragraaf VII.5.

Bibliografie

[Da-Do-Sw] D. van Dalen, H.C. Doets en H.C.M. de Swart. *Verzamelingen; naïef, axiomatisch en toegepast.* Oosthoek, Scheltema & Holkema, Utrecht, 1975.

[French] R.M. French. *The Banach-Tarski theorem.* Translated from the French by the author. Math. Intelligencer 10 (1988), no 4, 21–28. On-line: `http://leadserv.u-bourgogne.fr/files/publications/000293-the-banach-tarski-theorem.pdf`

[Hart] K.P. Hart. *Kreatief met sinaasappels.* Kennislink, 2007. On-line: `http://www.kennislink.nl/publicaties/een-sinaasappel-erbij-toveren`

[vLuijk] R. van Luijk. *Linear algebra I.* On-line: `http://websites.math.leidenuniv.nl/algebra/linalg1.pdf`

[Sc-Ma] T.C. Scott en P. Marketos. *On the origin of the Fibonacci Sequence*. `http://www-history.mcs.st-andrews.ac.uk/Publications/fibonacci.pdf`

[Stoll] M. Stoll. *Linear algebra I.* On-line: `http://www.mathe2.uni-bayreuth.de/stoll/lecture-notes/LinearAlgebraI.pdf`

Index