Fundamenten

Lerarenprogramma Mastermath, werkversie 3 september 2019

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 een handje in de kantlijn). De uitwerkingen zijn soms beperkt tot een aantal aanwijzingen.

We hopen dat de lezer, gewapend met de ervaring en kennis opgedaan in dit dictaat, klaar zal zijn om verder te gaan in de wiskunde door zelf kritisch teksten te lezen, ‘goede’ definities te hanteren, stellingen te formuleren en te bewijzen. Definities doen wonderen! Wie iets ernstig mist, wordt verzocht dat de auteurs te laten weten.

We bedanken Steve Alberts voor zijn bijdrage aan dit vak, zowel als assistent als mede-docent en verbeteraar van dit dictaat, en Jan Brinkhuis voor zijn vele suggesties en verbeteringen (zomer 2018), en ook de deelnemers aan het college in het najaar van 2017 voor hun suggesties. Ook dank aan Wouter Zomervrucht voor zijn werk aan het dictaat in augustus 2019: rubriceren van de opgaven, en het geven en verwerken van veel commentaar, en het beter maken van de index en kantlijn, en de latex-code.

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 (theo.vandenbogaart@hu.nl)
Bas Edixhoven (edix@math.leidenuniv.nl)

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. Het hoofdstuk over logica is deels geïnspireerd door het boek 'Logic and structure' van Dirk van Dalen [Da].

Alternatief en aanvullend materiaal

De TUD is al enige tijd geleden bij het vak 'Wiskundige Structuren' overgestapt van het bovengenoemde dictaat naar het boek [La]: 'Analysis. An introduction to proof'. Dit boek behandelt alle stof van dit dictaat behalve de lineaire algebra, in grote lijnen op dezelfde manier, maar in een iets andere volgorde (eerst logica, dan verzamelingen en afbeeldingen), en in een groter detail (dubbel aantal pagina's). Dit laatste maakt het geschikt als een aanvulling.

Het boek [EV] 'Inzien en bewijzen' van Jan van Eijck en Albert Visser is een aanrader voor wie een uitgebreide behandeling op zeer toegankelijk niveau over bewijzen zoekt (met dank aan Jos Hoevenaars-Pols voor deze referentie).

Voor nog meer detail over wiskundig redeneren, het lezen van wiskunde, het vinden en daarna opschrijven van bewijzen kan men terecht bij het boek [Ho] 'How to think like a mathematician'. Dit boek maakt veel werk van de theorie en voorbeelden en zal daarbij heel nuttig zijn, maar laat helaas wel serieuze steken vallen bij de behandeling in Hoofdstuk V van delingseigenschappen van de gehele getallen. De reële getallen worden in dit boek niet behandeld.

Een vergelijkbaar boek, in het Duits, is [HHP] 'Einführung in mathematisches Denken und Arbeiten'. Het is opvallend hoeveel dit boek lijkt op dit dictaat, alhoewel beiden onafhankelijk tot stand zijn gekomen.

Voor een aardig overzicht van de huidige wiskunde, zie `https://web.archive.org/web/20030130131813/http://math-atlas.org/` en voor de geschiedenis zie ook `http://www-history.mcs.st-andrews.ac.uk`.

Toelichting bij de opgaven

De opgaven in dit dictaat zijn vooral bedoeld om kennis en vaardigheden te leren. Hierbij onderscheiden we

S
V
B
✯

- startopgaven: oefenen met definities, simpele voorbeelden en niet-voorbeelden,
- vervolgopgaven: toepassen van stellingen, en eenvoudige bewijzen,
- bewijsopgaven: zelf bewijzen vinden en opschrijven,
- steropgaven: uitdagende opgaven die een origineel idee vereisen.

De opgaven zijn natuurlijk ook bedoeld om jezelf te kunnen toetsen. Daarbij is het goed te weten dat de tentamens grofweg zullen bestaan uit 25% startopgaven, 50% vervolgopgaven en 25% bewijsopgaven.

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. We zullen twee van die tegenspraken bekijken.

paradoxen

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.

axioma's

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 $\varnothing$.

lege verzameling

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] Verder schrijven we $\mathbb{Z} = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$ 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.

getalssystemen

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.

(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.

[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 $\mathbb{Z}_{\geqslant 0}$; deze maakt meteen duidelijk dat $0 \in \mathbb{N}$.

(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 $\cos(\pi x/2) = 0$. ∎

gelijkheid van verzamelingen

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.

deelverzameling

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

Hieruit volgt dat $A = B$ equivalent[4] is met: $A \subseteq B$ 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 gelijk aan 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 $1 \in B$. ∎

interval

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] en $[a,b] = \{x \in \mathbb{R} : a \leqslant x \leqslant b\}$ een *gesloten interval*. De verzamelingen $[a,b) = \{x \in \mathbb{R} : a \leqslant x < b\}$ 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.

(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.

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

[4] In plaats van 'equivalent' wordt vaak de uitdrukking 'dan en slechts dan als' gebruikt, maar 'als en alleen als' is eenvoudiger.

[5] Deze notatie hebben we niet geïntroduceerd, maar de betekenis is duidelijk. Een andere mogelijke 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.

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

(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 II.1.5 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 $[0,-1]$. ∎

Het volgende begrip wordt vaak gebruikt.

cartesisch product

I.1.7 Definitie. Het *cartesisch product* van twee verzamelingen A en B is de verzameling geordende paren[8]

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

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 alleen 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

S ✍ **1.** 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) $E = \{1,\{1,2,3,4,5\}\}$.

S **2.** 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) $E = \varnothing$.

V **3.** Welke van de volgende verzamelingen zijn aan elkaar gelijk? Bewijs je bewering of geef een tegenvoorbeeld.

[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 $\mathbb{R}^2$.

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

V ✍ **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) $C \subseteq B$.

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

S ✍ **6.** (a) Vind alle deelverzamelingen van $\{0, 1\}$.
(b) Vind alle deelverzamelingen van $\{0, 1, 2\}$.
(c) Vind alle deelverzamelingen van $\{0, 1, 2, 3\}$.
B (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.

S ✍ **7.** 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 het cartesisch product $\mathscr{P}(A) \times \mathscr{P}(B)$, waarbij $A = \{0, 1\}$ en $B = \{\varnothing\}$.

B ✍ **8.** Als $A = B$, dan geldt natuurlijk $A \times B = B \times A$. Dat is echter geen noodzakelijke voorwaarde! Geef de precieze voorwaarden op de verzamelingen A en B opdat $A \times B = B \times A$.

I.2 Operaties op verzamelingen

De basisoperaties op verzamelingen zijn als volgt gedefinieerd.

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

complement (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);

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

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

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

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

verschil

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

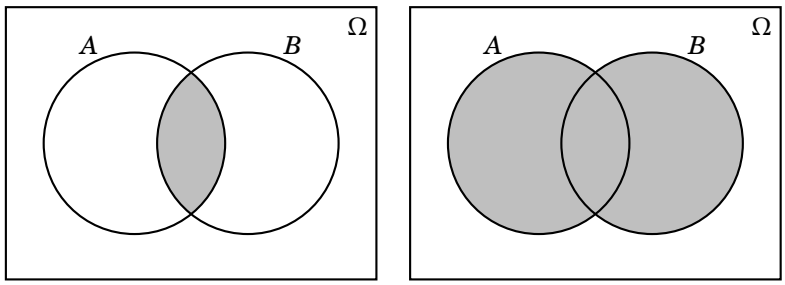
$$A \setminus B = \{x \in \Omega : x \in A \text{ en } x \notin B\}.$$

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 $A \cup B = A$. ∎

venndiagram

Om doorsnede en vereniging van A en B te illustreren kunnen we *venndiagrammen* tekenen. In Figuur I.2.4 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.2.5 en I.2.6.



I.2.4 Figuur. Doorsnede en vereniging van A en B.

disjunct

I.2.5 Definitie. Twee verzamelingen A en B heten *disjunct* als $A \cap B = \varnothing$.

I.2.6 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 I.2.7 zijn venndiagrammen voor drie respectievelijk vier deelverzamelingen van Ω getekend. Venndiagrammen voor meer dan vier verzamelingen zijn lastig: het is niet makkelijk om op een overzichtelijke manier alle mogelijke doorsneden in één plaatje te krijgen.

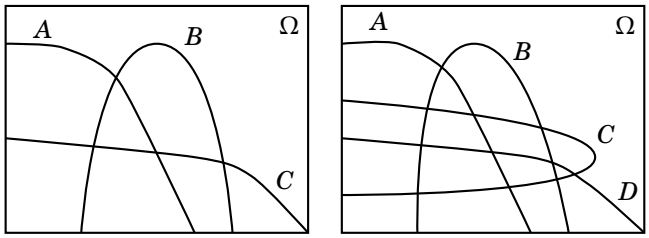
In de wiskunde onderzoeken we vaak oneindige objecten: er zijn oneindig veel natuurlijke getallen, oneindig veel breuken, oneindig veel punten in het platte vlak, oneindig veel lijnen, oneindig veel functies. Daarvoor is de taal van de verzamelingenleer ook handig.

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

oneindige vereniging en doorsnede

I.2.8 Definitie. Laat Ω een verzameling zijn. Laat L een verzameling zijn, en

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



I.2.7 Figuur. Venndiagrammen voor drie en vier verzamelingen.

voor elke $\lambda \in L$, A_λ een deelverzameling van Ω. Dan:

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

en

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

I.2.9 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.2.8 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 $1/(n+1) < x$. ∎

bewijs uit het ongerijmde

Dit soort bewijs heet een *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.2.10 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.2.8 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

S **1.** 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.

S **2.** (a) Zij $A = \{1,2,3,4,5,6,7,8,9\}$. Vind $A \cap A$, $A \cup A$ en $A \setminus A$.

V (b) Zij A een willekeurige verzameling. Vind en bewijs een algemene regel voor $A \cap A$, $A \cup A$ en $A \setminus A$.

S ✍ **3.** 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) $A_k = (k,\infty)$.

V ✍ **4.** 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 $\bigcup_{n\in\mathbb{N}} A_n$.

B ✍ **5. 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) $\Omega \setminus (A \cup B) = (\Omega \setminus A) \cap (\Omega \setminus B)$.
(c) Wat zou je aan de wetten van De Morgan kunnen hebben?

B ✍ **6.** Zij Ω een verzameling. Formuleer en bewijs de wetten van De Morgan
(a) voor drie deelverzamelingen van Ω;
(b) voor vier deelverzamelingen van Ω.

B **7.** Bewijs dat voor alle verzamelingen A, B en C de volgende gelijkheden gelden, en geef ook in elk van de gevallen een tekening van het venndiagram:
(a) $B \setminus (B \setminus A) = A \cap B$;
(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

B ✍ **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 $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$?

B ✍ **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*.

functie

I.3.1 Definitie. Een *functie*[11] is een tripel (A,B,f) met A en B verzamelingen en 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 $f(a)$.

We zeggen wel dat f een *functie van A naar B* is. Notatie: $f : A \to B$, en $a \mapsto f(a)$.

domein, codomein
grafiek
beeld, origineel

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 $f : A \to B$.

injectief
(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 $f(a) = b$.)

surjectief
(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 $b \in B$ is er *minstens* één $a \in A$ met $f(a) = b$.)

bijectief
(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 $f(a) = b$.)

beeld
(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 $\{b \in B : \text{er bestaat een } a \in A \text{ met } b = f(a)\}$.

beperking
(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 $f(A) = B$.

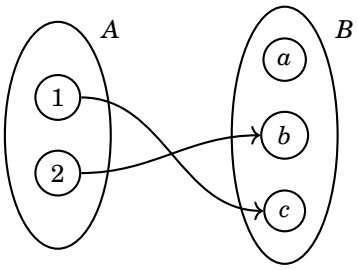
We krijgen een surjectieve afbeelding door het codomein van f te beperken tot het beeld van f: de afbeelding $g : A \to f(A)$, $x \mapsto f(x)$ is surjectief.

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

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

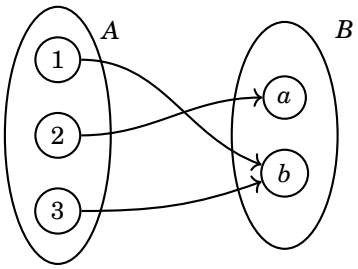
Als A en B eindig zijn dan is het makkelijk functies van A naar B grafisch weer te geven: zie de volgende voorbeelden.

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 I.3.8). ∎



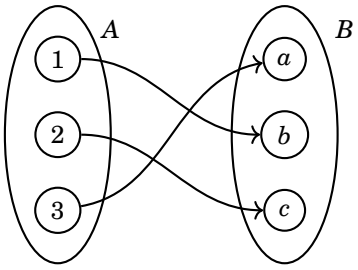
I.3.8 Figuur. Een injectieve, niet surjectieve functie $f : A \to B$.

I.3.9 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 I.3.10). ∎



I.3.10 Figuur. Een surjectieve, niet injectieve functie $f : A \to B$.

I.3.11 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 I.3.12). ∎

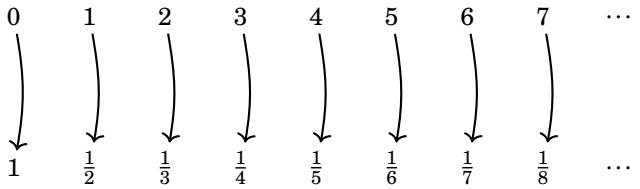


I.3.12 Figuur. Een bijectieve functie $f : A \to B$.

rij

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.3.13 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 $1/(n+1) = 0$). ∎

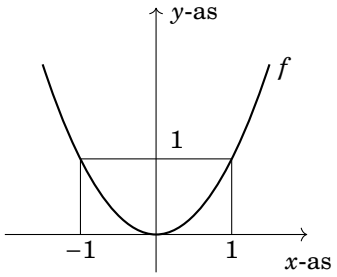


I.3.14 Figuur. De rij $(1/(n+1))_{n\in\mathbb{N}}$ als een functie $f : \mathbb{N} \to \mathbb{R}$.

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.3.15 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 I.3.16). 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.3.16 Figuur. Grafiek van de functie $f(x) = x^2$.

I.3.17 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. ∎

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.

samenstelling

I.3.18 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.3.19 Opmerking. Als $f : A \to B$ en $g : B \to A$ functies zijn dan geldt niet altijd dat $f \circ g = g \circ f$, in mooie woorden: samenstelling van functies is niet *commutatief*. Als $A \neq B$ dan is $f \circ g$ zeker niet gelijk aan $g \circ f$, want de domeinen verschillen.

Maar ook als $A = B$ zijn $f \circ g$ en $g \circ f$ niet noodzakelijk gelijk. Neem bijvoorbeeld $A = B = \mathbb{R}$, de functie $f : \mathbb{R} \to \mathbb{R}$ gegeven door $f(x) = \sin x$, en de functie $g : \mathbb{R} \to \mathbb{R}$ door $g(x) = x^2$. Dan is $f \circ g : \mathbb{R} \to \mathbb{R}$ de functie gedefinieerd door $(f \circ g)(x) = \sin(x^2)$, en $g \circ f : \mathbb{R} \to \mathbb{R}$ is gedefinieerd door $(g \circ f)(x) = (\sin x)^2$.

I.3.20 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 dat $f : A \to B$, $g : B \to C$ 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

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

identieke functie

I.3.21 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.3.22 Opmerking. Als A en B verzamelingen zijn, en $f : A \to B$, dan geldt

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

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

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

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.

inverse

I.3.23 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

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

We gebruiken als notatie: $g = f^{-1}$. Zie Opgave I.3.18 voor een karakterisering van inverse functies in termen van samenstelling.

I.3.24 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.3.19. ∎

I.3.25 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 $x \in \mathbb{R}$,

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

De inverse $f^{-1} : \mathbb{R} \to \mathbb{R}$ is dus gegeven door het voorschrift $f^{-1}(x) = (2-x)/3$.[13] Opgave I.3.21 geeft een eenvoudig verband tussen de grafieken van f en f^{-1}. ∎

inverse beeld

I.3.26 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.3.27 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

S ✍ **1.** Teken de grafieken van de functies in de voorbeelden I.3.7 en I.3.9.

S ✍ **2.** 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 $1/f(x)$.

S ✍ **3.** (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 $f(x)$.

S ✍ **4.** Zij $f : \mathbb{R} \to \mathbb{R}$ gegeven door $f(x) = \sin(x^2)$; vind alle originelen van 0, -1 en π.

S ✍ **5.** 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
$g : \mathbb{R} \setminus \{1\} \to \mathbb{R}$, $x \mapsto \frac{x^2-1}{x-1}$.

V ✍ **6.** (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?

V **7.** 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.

V **8.** 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.

B **9.** 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 $\#A \geqslant \#B$.

B ✍ **10.** 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.

B **11.** 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 $f(V_1 \cap V_2) = f(V_1) \cap f(V_2)$.

V **12.** Vind een verzameling A met zo min mogelijk elementen en twee functies $f : A \to A$, $g : A \to A$ waarvoor $f \circ g$ niet gelijk is $g \circ f$.

V **13.** Bewijs dat elk 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 $f(x) = 1/x$.

V **14.** 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.

V ✍ **15.** 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) $A = [-1, 0]$, $f(x) = \sqrt{1 - x^2}$.

V **16.** 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: $f^{-1}(\mathbb{Z}) \cap \mathbb{Q} = \mathbb{Z}$.

V **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.3.26. Merk op dat we voor beide verzamelingen de notatie $f^{-1}(C)$ gebruiken.)

B **18.** Laat A en B verzamelingen zijn, en $f : A \to B$ en $g : B \to A$.
(a) Bewijs dat de volgende twee uitspraken equivalent zijn:
1. f en g zijn beide bijectief, en inversen van elkaar;
2. $g \circ f = \mathrm{id}_A$ en $f \circ g = \mathrm{id}_B$.
(b) Geef een voorbeeld waar $g \circ f = \mathrm{id}_A$ en $f \circ g \neq \mathrm{id}_B$.

B **19.** Bewijs Lemma I.3.24.

B **20.** 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 $f^{-1} = f$.

B **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?

B **22.** 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 alleen als .....
en bewijs dat dit dezelfde afbeelding oplevert als Definitie I.3.18. Bewijs ook, uitgaande van de voorgaande formulering, dat $f \circ (g \circ h) = (f \circ g) \circ h$.

S **23.** Probeer eens de interactieve opgaven over inverse functies op de WIMS server [WIMS] (zoek onder 'inverse'): `http://wims.unice.fr/wims/wims.cgi?lang=nl`.

I.4 Aftelbare en overaftelbare 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 $\mathbb{N}$.

gelijkmachtig

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.

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

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

eindig
(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 $A = \varnothing$).

aftelbaar oneindig
(ii) A heet *aftelbaar oneindig* als A en $\mathbb{N}$ gelijkmachtig zijn.

aftelbaar
(iii) A heet *aftelbaar* als A eindig of aftelbaar oneindig is.

overaftelbaar
(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 $\mathrm{id}_{\mathbb{N}}\colon \mathbb{N} \to \mathbb{N}$ 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 $f(n) \geqslant 0$ als en alleen 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 $m \geqslant 0$ 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.

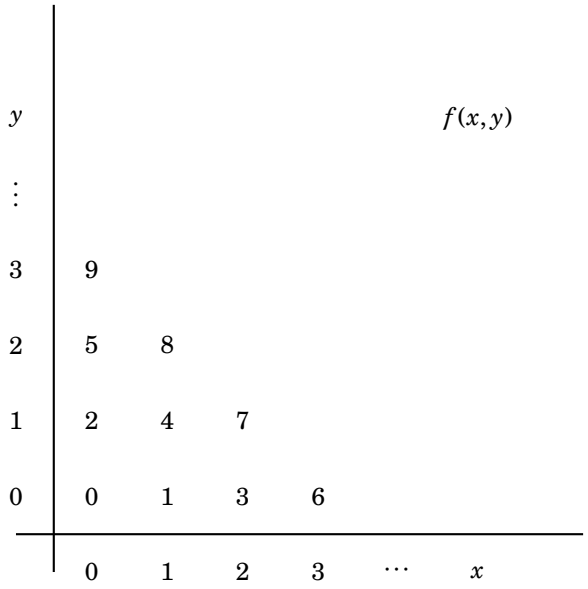
Omdat de afbeelding f zowel injectief als surjectief is, is hij bijectief. ∎

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.4.8 geeft een mooie formule voor de f hieronder).

Beschouw de functie $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ waarbij $f(x,y)$ in de Figuur I.4.7 is weergegeven. Bijvoorbeeld $f(2,1) = 7$ en $f(4,0) = 10$. Uit de constructie is het duidelijk dat f een bijectie is. ∎



I.4.7 Figuur. Grafische weergave van de functie $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Met een gelijkaardig argument kan men bewijzen dat ook $\mathbb{Q}$ aftelbaar is. Zie Opgave I.4.10.

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

machtsverzameling

I.4.8 Definitie. Zij A een verzameling. De *machtsverzameling* van A is de verzameling van alle deelverzamelingen van A. Notatie: $\mathscr{P}(A)$.

I.4.9 Voorbeeld. $\mathscr{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$. ∎

I.4.10 Opmerking. De volgende stelling en het bewijs ervan zullen bij velen vragen oproepen. We proberen hier alvast wat te helpen. Laat A een verzameling zijn, en $f : A \to \mathscr{P}(A)$ een afbeelding van A naar de machtsverzameling van A. Voor elke x in A is $f(x)$ een element van $\mathscr{P}(A)$ en dus een *deelverzameling* van A (geen element van A). Het is dus zinvol om te kijken of x (*wel* een element van A), wel of niet een element van $f(x)$ is. Hiermee is de deelverzameling $B \subseteq A$ gedefiniëerd. Deze definitie is van groot belang. Het is een variant van *Cantors diagonaalmethode*; het directe verband hiermee wordt duidelijker gemaakt in Opgave I.4.13. Deze methode zelf (een 'negatieve zelfreferentie') ligt weer aan de basis van Gödels bewijs van zijn *onvolledigheidsstelling* waar een uitspraak gefabriceerd wordt die zegt 'ik ben niet bewijsbaar,' en ook aan Turing's bewijs van de onbeslisbaarheid van het 'halting problem.'

stelling van Cantor

I.4.11 Stelling (Cantor). Zij A een verzameling.

1. Laat $f : A \to \mathscr{P}(A)$. Dan is de deelverzameling
$$B := \{x \in A : x \notin f(x)\}.$$
van A geen element van het beeld van f.
2. Er bestaat geen surjectieve afbeelding van A naar $\mathscr{P}(A)$.

Bewijs. We bewijzen het eerste deel. Laat A, f en B zoals in de uitspraak. Stel nu dat x een element van A is met $f(x) = B$. Er zijn twee mogelijkheden: (i) $x \in B$ of (ii)

$x \notin B$. Als (i) geldt, dus $x \in B$, dan 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. De conclusie is dat er geen $x \in A$ is met $f(x) = B$, en dat is wat we wilden bewijzen.

Een andere manier om onderdeel 1 te bewijzen is als volgt. We willen laten zien dat B verschillend is van *alle* $f(a)$, waar a de verzameling A doorloopt. Laat a in A. Om te laten zien dat B niet gelijk aan $f(a)$ is, is het voldoende (en ook noodzakelijk) dat er een element x van A is waar B en $f(a)$ verschillen, en dat betekent dat x wel in de ene zit maar niet in de andere. We nemen nu $x = a$, en dan zegt de definitie van B precies dat B en $f(a)$ verschillen in a. Dit legt ook uit hoe iemand op de definitie van B kan komen.

We bewijzen het tweede deel. Wel, dit is een direct gevolg van het eerste deel. ■

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

I.4.12 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

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

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

S **3.** Laat zien dat de intervallen $[0, 1)$ en $(2, 5]$ gelijkmachtig zijn.

V **4.** Laat zien dat $(0, 1)$ en $\mathbb{R}$ gelijkmachtig zijn.

B **5.** 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.

S **6.** Zij $2\mathbb{N}$ de verzameling van alle even natuurlijke getallen. Bewijs dat $2\mathbb{N}$ aftelbaar oneindig is.

V **7.** Beschouw $A = \{2^{-n} : n \in \mathbb{N}\}$ en $B = \{3^n : n \in \mathbb{N}\}$. Laat zien dat $A \cup B$ aftelbaar is.

B **8.** Laat zien dat de afbeelding $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ gegeven door

$$f(n, m) = \tfrac{1}{2}(n + m)(n + m + 1) + m$$

de bijectie uit het bewijs van Stelling I.4.6 is.

B **9.** Laat zien dat de afbeelding $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}_{\geqslant 1}$ gegeven door $f(n,m) = 2^n(2m+1)$ een bijectie is.

B **10.** Bewijs dat $\mathbb{Q}$ aftelbaar is.

S **11.** Zij A een verzameling en $\mathscr{P}(A)$ zijn machtsverzameling. Geef een injectieve afbeelding $f : A \to \mathscr{P}(A)$.

V **12.** Werk uit wat er in het bewijs van Stelling I.4.11 gebeurt in het geval dat $A = \{1,2\}$.

B **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 Stelling I.4.11. Wat is dan het element $F^{-1}(B)$? Kun je nu makkelijker uitleggen waarom de functie $F^{-1}(B) : A \to \{0,1\}$ verschillend is van alle $F^{-1}(f(a))$ (a doorloopt A)?

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

B **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.

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

I.5 Een echte toepassing: het honderdsmurfenprobleem

Het tweede deel van de titel van deze paragraaf 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!

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.

honderd smurfen

> 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. De kluisjes zijn genummerd van 1 tot en met 100. 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. 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*

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

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!

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.

permutatie

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, samenstelling en inverse: 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

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

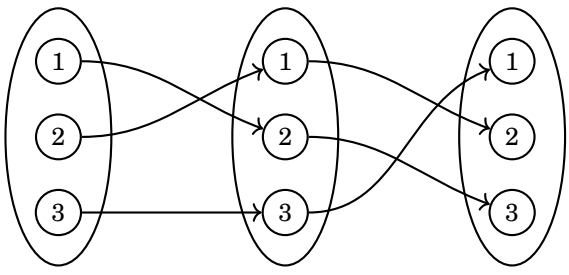
In deze notatie wordt de samenstelling $\sigma \circ \tau$ (éérst τ, dan σ) van σ en τ als volgt uitgerekend:

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

Bijvoorbeeld geldt

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

zie ook Figuur I.5.1.



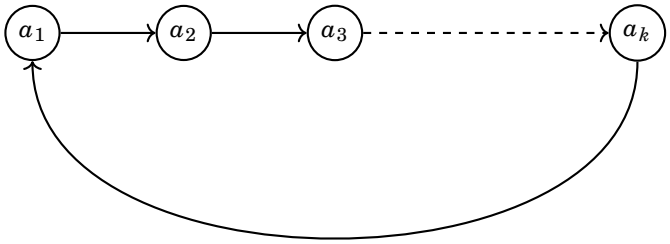
I.5.1 Figuur. Samenstelling van permutaties.

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

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.

cykel

Voor $k \in \mathbb{N}_{\geqslant 1}$ 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.

disjunct

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 $(\sigma\circ\tau)^n = \sigma^n \circ \tau^n$. 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.

disjuncte cykelontbinding

I.5.2 Stelling. Zij A een eindige niet-lege[15] 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 Paragraaf IV.2 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 $0 \leqslant j < k$ 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. ∎

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

[15] De stelling is ook waar voor de lege verzameling A, als we samenstelling van *nul* cykels toestaan. Deze 'lege samenstelling' is dan per definitie gelijk aan id_A, net zoals we eerder $\sigma^0 = \mathrm{id}_A$ definiëerden.

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.[16]

smurfenhints

- 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?
- 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 $f : S \to \{1,\ldots,100\}$ 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

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

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

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

S **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.

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

B **5.** Laat A een eindige verzameling zijn, $r \in \mathbb{N}_{\geqslant 1}$, en $\sigma_1,\ldots,\sigma_r$ 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

Cantor

Georg Cantor (Duits wiskundige, 1845–1918)[17] kwam door zijn werk aan trigonometrische reeksen ($\sum_{n\geqslant 0} a_n \cos(nx) + \sum_{n>0} b_n \sin(nx)$) 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.

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

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

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 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.

ZFC
keuzeaxioma

Gödel liet zien (1940) dat áls ZF consistent is (d.w.z. niet tot een tegenspraak leidt), dat ZFC dan óók consistent is. Ook liet hij zien (1931) dat een bewijs van consistentie van ZF niet binnen ZF te formaliseren is. Paul Cohen bewees (1963) dat als ZF consistent is, dan ook ZF+*niet*C. De conclusie is dat als ZF consistent is, het keuzeaxioma niet afgeleid kan worden uit ZF.

Een belangrijke vraag is of er verzamelingen zijn die strikt groter zijn dan $\mathbb{N}$ en strikt kleiner zijn dan $\mathbb{R}$. De *continuümhypothese* (CH) zegt dat dit niet zo is. De vraag of CH waar of onwaar is, was 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.

continuümhypothese

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

paradox van Banach–Tarski

Opgaven

S **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 [Fr] en [Ha].

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[18]:

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

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 uit deze examenopgaven uit 1968 en 1969:[19]

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:

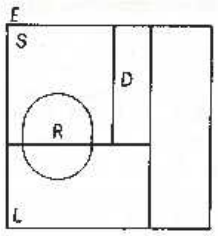
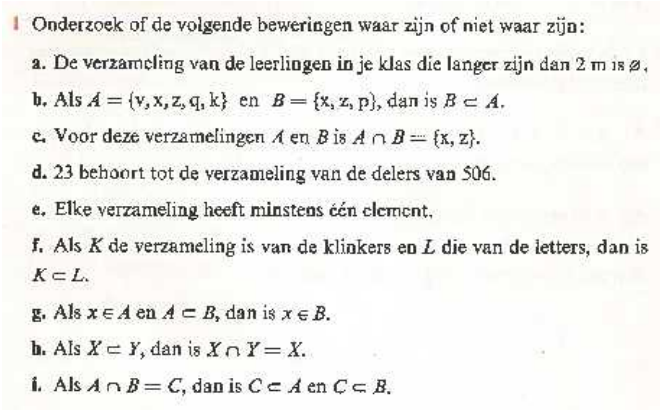


Fig. 8

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.

[18] Uit: Goffree, *Honderd jaar wiskundeonderwijs*.
[19] Ibid.



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 $C \subset B$.

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. We komen functies $f : \mathbb{R}^2 \to \mathbb{R}$, enigszins impliciet, tegen als families van functies f_a. Het begrip inverse functie 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 II.0.2 staan twee interpretaties van deze zin getekend. Je kunt er zelf nog twee verzinnen[1]. ∎

II.0.2 Figuur. Twee interpretaties van de zin "De man zag de piramide op de heuvel met een verrekijker".

II.0.3 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.0.4 Voorbeeld. Ook in niet een niet preciese context is analytisch denken van groot belang. We geven hier een zeer bekend voorbeeld. In de Tweede Wereldoorlog werden vanuit Engeland veel vluchten uitgevoerd om Duitsland te bombarderen, en veel vliegtuigen kwamen niet terug omdat ze door luchtafweergeschut werden getroffen. Iemand die naar de wél teruggekeerde vliegtuigen keek zag vele gaten in de vleugels, maar niet in de motoren, en opperde het idee om daarom de vleugels extra te pantseren. Wat vind je van deze suggestie? ∎

II.1 Propositielogica

propositie

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".

propositievariabele

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

waarheidstabel

waarheid van P en Q. Deze afhankelijkheid kunnen we aangeven in een *waarheidstabel*, waarvan links in Figuur II.1.2 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

II.1.2 Figuur. 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 propositie is de *disjunctie*. Een disjunctie heeft de vorm 'P of Q', hetgeen we noteren als

$$P \vee Q.$$

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

De waarheidstabel van de conjunctie is de middelste in Figuur II.1.2. 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."

II.1.3 Opmerking. In de wiskunde is *afgesproken* het woordje 'of' op deze manier te interpreteren, want in het dagelijks taalgebruik komt regelmatig de interpretatie van *exclusieve-of* voor: of P is waar, of Q is waar, maar niet allebei. Zie Opgave II.1.2.

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 II.1.2. Een ontkenning herken je vaak aan het woordje 'niet', dat soms kan zijn opgenomen in notaties: $2 \neq 3$, $-1 \notin \mathbb{N}$.

logische operator

We noemen negatie, conjunctie en disjunctie *logische operatoren*. Met behulp hiervan kun je willekeurig lange samengestelde proposities 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.1.1 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

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

Bij waarheidstabellen van samengestelde proposities kun je de tabel in stapjes opbouwen. Dat is in Figuur II.1.4 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 $P_1, P_2, \ldots, P_n$.

logisch equivalent

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

implicatie
bi-implicatie

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

II.1.4 Figuur. Links de waarheidstabel van $\neg(\neg P \wedge \neg Q)$ en rechts die van de disjunctie $P \vee Q$. Deze uitspraken zijn logisch equivalent.

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

II.1.5 Figuur. De waarheidstabellen van implicatie en bi-implicatie.

Figuur II.1.5.

als ... dan ...
als en alleen als
precies dan als
equivalent

De implicatie $P \Rightarrow Q$ herken je vaak in de formulering 'als P dan Q.' De bi-implicatie $P \Leftrightarrow Q$ kent meerdere formuleringen, die niet alle even fraai zijn: 'P als en alleen als Q,' 'P dan en slechts dan 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.1.4):

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

De waarheidstabel voor $P \Rightarrow Q$ kan als volgt gemotiveerd worden. We denken aan P als een voorwaarde, en aan Q als een belofte, en aan $P \Rightarrow Q$ als een contract waarin onder de voorwaarde P (bijvoorbeeld: de klant betaalt) de belofte Q (bijvoorbeeld: het bedrijf levert een dienst) zal worden ingelost. Alleen als de klant *wel* heeft betaald en de dienst *niet* is geleverd zal de klant succes hebben bij de rechter wegens contractbreuk. In de overige 3 gevallen zal de rechter oordelen dat aan het contract is voldaan.

Nog een motivatie voor de waarheidstabel voor $P \Rightarrow Q$ is dat we vinden dat voor alle reële getallen x geldt dat $(x > 5) \Rightarrow (x > 2)$ (in woorden: als x groter dan 5 is, dan is x groter dan 2). In het bijzonder is de implicatie waar voor $x \in (2,5]$ en ook voor $x \in (-\infty, 2]$, en natuurlijk ook voor $x \in (5, \infty)$.

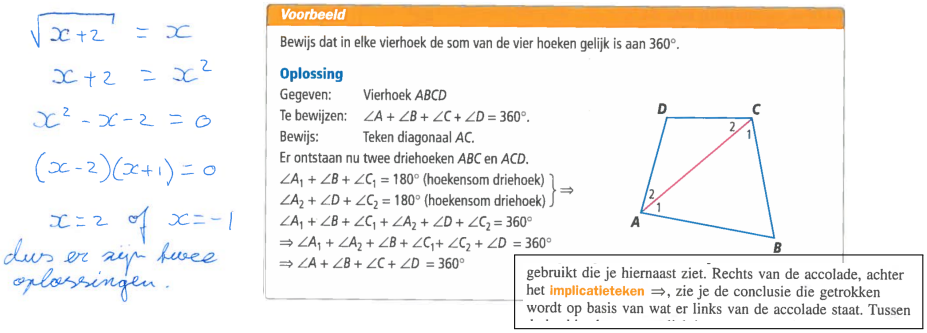
II.1.6 Opmerking. Bij het gebruik van implicaties in de wiskunde zijn er de volgende twee veelvoorkomende aanleidingen tot verwarring.

- 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;

[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.

stel vervolgens dat de gevonden uitspraak ook echt het antwoord is (zie Figuur II.1.7). 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 '⇒' 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 II.1.7).



II.1.7 Figuur. Twee veelgemaakte fouten rondom implicaties. Links: bij het oplossen van vergelijkingen worden vaak impliciet omgekeerde implicaties gebruikt. Rechts (uit *Moderne wiskunde*, editie 9, vwo B): het pijltje krijgt soms de betekenis van 'daaruit volgt,' en wordt binnen de argumentatie als afkorting gebruikt. We zien in het voorbeeld binnen één formule 3 opeenvolgende pijltjes. De lezer snapt wat er bedoeld wordt, maar dit soort slordigheid (door elkaar gebruiken van zinnen en formules) willen we niet aanmoedigen. (Het voorbeeld bevat overigens nog een fout — een meetkundige.)

Opgaven

S

1. 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 $\vee$ en $\wedge$ 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 is er een distributieve wet: $x \cdot (y+z) = x \cdot y + x \cdot z$.

V

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

V ✍

2. 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.

B **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) Bewijs deze wetten van De Morgan voor verzamelingen met behulp van de wetten van De Morgan voor de logica.

V **4.** (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 $P \Rightarrow Q$.

V **5.** 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.

B **6.** Deze opgave gaat over het concept *logische equivalentie*.

(a) Bewijs dat twee proposities P en Q logisch equivalent zijn, als en alleen 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.)

B **7.** We bekijken nog eens Opgave I.2.7. Stel we willen onderdeel (b) bewijzen. Dus gegeven zijn verzamelingen A, B en C, en te bewijzen is dat

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Dat betekent dat we voor iedere $x \in A \cup B \cup C$ moeten bewijzen dat $x \in A \cap (B \cup C)$ equivalent is met $x \in (A \cap B) \cup (A \cap C)$.

(a) Schrijf de uitspraak $x \in A \cap (B \cup C)$ in termen van de uitspraken $x \in A$, $x \in B$ en $x \in C$, en logische operatoren.

(b) Schrijf de uitspraak $x \in (A \cap B) \cup (A \cap C)$ in termen van de uitspraken $x \in A$, $x \in B$ en $x \in C$, en logische operatoren.

(c) Ga nu met een waarheidstabel na dat de 2 uitspraken equivalent zijn.

(d) Denk nu eens na over venndiagrammen, en zie in dat ieder 'bewijs' met venndiagrammen om te schrijven is in een bewijs met waarheidstabellen.

(e) Behandel ook de andere 2 onderdelen van Opgave I.2.7 op deze manier.

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 *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:

universele kwantor
- 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);

existentiekwantor
- 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').

Een ander woord voor propositiefunctie is *predikaat*. De logica die we in deze paragraaf bespreken, om precies te zijn: de uitbreiding van de propositielogica met
predikaatlogica predikaten en de kwantoren $\forall$ en $\exists$, heet dan ook wel *predikaatlogica*.

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:

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

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 $f \subseteq A \times B$ 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

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

unieke existentie waarbij '$\exists!$' uitdrukt dat er een *uniek* element bestaat. Zie verder Opgave II.2.4. ∎

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; je kan je bijvoorbeeld afvragen of *er* $x \in \mathbb{R}$ *is* waarvoor de vergelijking geldt. In literatuur over algebradidactiek vind je meer informatie over de verschillende *rollen van variabelen* in de schoolwiskunde.

volgorde van kwantoren

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

S ✍ **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 x, logische operatoren, kwantoren, variabelen, $\in$, $\mathbb{Z}$, $=$, en $+$, zodat geldt $E = \{x \in \mathbb{Z} : V(x)\}$.

(b) Vind ook een propositiefunctie $W(x)$, uitgedrukt in x, logische operatoren, kwantoren, variabelen, $\in$, $\mathbb{N}$, $=$, 0, 1, en $\cdot$, zodat geldt $P = \{x \in \mathbb{N} : W(x)\}$.

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

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

Hier is een alternatieve formulering:

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

Bewijs dat beide formulering equivalent zijn.

S **3.** 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) $\exists_{x\in\varnothing}(x \neq x)$.

V **4.** 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.

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

V **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.

bewijs

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.

redeneerregels

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* of kortweg *modus ponens*, al zul je dit woord in wiskundeteksten niet snel tegenkomen.)

'$\Rightarrow$'-introductie. Je mag op een kladpapiertje een willekeurige propositie P opnemen, hier vervolgens met de redeneerregels een resultaat Q uit afleiden, en vervolgens $P \Rightarrow Q$ aan je bewijs toevoegen. Vergelijk het kladpapiertje 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 karwei, 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.

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

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.

bewijstheorie

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 wiskundigen 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]

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

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 voorbeeld is gegeven. Je kunt het ook aan de hand van de waarheidstabel van de implicatie (links in Figuur II.1.5) 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

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:

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

[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 medaille, de nobelprijs van de wiskunde. Het artikel is beschikbaar op internet onder `http://arxiv.org/abs/math/9404236`.

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

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.2.9 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

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.
- $a > 3$. Dan $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1$ en zijn er dus geen oplossingen. ∎

equivalentie

Bewijs van 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 $Q \Rightarrow P$.

universaliteit

Bewijs van 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 $a + b \in E$. ∎

existentie

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

1. Je wijst 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.

non-constructief bewijs

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 $a, b \in \mathbb{R}_{\geqslant 0} \setminus \mathbb{Q}$ 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. ∎

Het boek [EV] 'Inzien en bewijzen' van Jan van Eijck en Albert Visser is een aanrader voor wie een uitgebreide behandeling op zeer toegankelijk niveau over bewijzen zoekt (met dank aan Jos Hoevenaars-Pols voor deze referentie).

Opgaven

S **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.

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

(d) Is MU een stelling?

B **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 ${}^{a}\log b \notin \mathbb{Q}$.

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

V **5.** Alice kijkt naar Bob, en Bob kijkt naar Charlotte. Alice is getrouwd, maar Charlotte is niet getrouwd. Is dan de volgende bewering waar, niet waar, of heb je niet voldoende informatie om dit te beslissen?

"Er is hier een getrouwd persoon die naar een ongetrouwd persoon kijkt."

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

II.4 Stellingen en definities

stelling
lemma
gevolg
definitie

Stellingen zijn proposities waarvan door middel van een bewijs de waarheid is vastgesteld. Ook *lemma's* en *gevolgen* zijn stellingen[8] — de enige reden dat er een ander woord wordt gebruikt, is een didactische: een lemma is een hulpstelling, een gevolg 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 Voorbeeld.

(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 definiëer je de eigenschap 'even' van getallen. ∎

II.4.2 Voorbeeld. 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 Voorbeeld.

(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 bepaald is. ∎

equivalente definities

De volgende uitspraak komt soms ook voor in wiskundeteksten:

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

[8] Men ziet ook wel het woord *propositie* als synoniem voor stelling. Pas op dat dit een andere betekenis van de term is dan die wij in paragraaf II.1 gebruikten!

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

S ✍ **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 $(\text{oppervlakte}) = \pi \times (\text{straal})^2$.

V **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?

V **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. (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.

Euclides

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, hebben 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

Aristoteles

kennis, behouden en soms aanzienlijk verrijkt door Perzische geleerden zoals de voor de logica belangrijke Ibn Sina (Avicenna) en Ibn Rushd (Averroës).

Leibniz

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, 1815–1864).

Frege

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 predikaatlogica 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

Russell

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.

Hilbert

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.

Brouwer

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 ingewikkelde 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 gedachten nemen en aan de hand hiervan de notatie doorgronden. Die vertrouwdheid is er mogelijk niet meer bij het laatste gedeelte van dit hoofdstuk over equivalentieklassen 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: zie bijvoorbeeld Figuur III.0.2. ∎

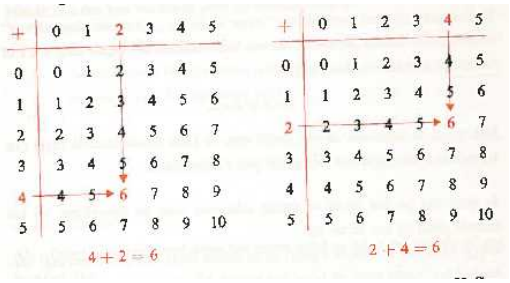
III.1 Operaties

operatie

III.1.1 Definitie. Zij V een verzameling. Een *(binaire) operatie* op 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 $a \bigcirc b$.



III.0.2 Figuur. Een illustratie van de commutatieve eigenschap van optelling uit het de editie van 1968 van *Moderne wiskunde* voor klas 1.

III.1.2 Voorbeeld. 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 vermenigvuldigen. 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 $\mathrm{Sym}(A)$. ∎

partiële operatie

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 $W = \mathbb{R} \times (\mathbb{R} \setminus \{0\})$.

gesloten

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).

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.

associatief

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

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

commutatief

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

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

III.1.5 Voorbeeld. 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.1.3.

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.1.6). ∎

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

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

Bij machtverheffen is er een soortgelijk probleem: a^{a^a} is betekenisloos. Zie verder Opgave III.1.3. 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.

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

neutraal element

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. ∎

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

inverse

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

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 Voorbeeld. 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*:

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 $\boxed{(-)}$ 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 dan 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

delen

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

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). ∎

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.

distributief

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

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

voorrangsregel

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 III.1.8 leidt je het volgende, voor de schoolwiskunde centrale, gevolg van de distributieve eigenschap af:

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

Opgaven

S **1.** 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.)

S ✍ **2.** Zonder de afspraak 'vermenigvuldigen gaat voor optellen', heb je heel veel haakjes nodig.

(a) Zet alle haakjes in de formule $2xy + 5x + 3y + 4$.

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

S **3.** (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 $\mathbb{N} \setminus \{0\}$)?

V (c) En met logaritme $\log_a b$ (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.)

V **4.** 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?

B ✍ **5.** Voor de natuurlijke getallen geldt dat vermenigvuldigen herhaald optellen is en dat machtsverheffen herhaald vermenigvuldigen is. Definieer een nieuwe operatie '↑' 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).

B **6.** In Paragraaf I.5 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 alleen 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.

S ✍ **7.** 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.

V **8.** Zij V een verzameling. Laat $+$ en $\cdot$ twee operaties op V zijn. Neem aan dat $\cdot$ distributief is over $+$. Bewijs dat voor alle $a, b, c, d \in V$ geldt

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

V ✍ **9.** 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. De bedoeling is dat ∞' min oneindig betekent. 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: lineaire ordeningen

Een (binaire) relatie op een verzameling V is een uitspraak $P(x,y)$ over paren (x,y) van elementen x en y van V die, afhankelijk van het paar (x,y), waar of onwaar is. Anders gezegd is P een propositiefunctie op $V \times V$ zoals in Sectie II.2.

Bekende voorbeelden van relaties zijn, voor zeg $V = \mathbb{R}$, x is gelijk aan y ($x = y$), x is ongelijk aan y ($x \neq y$), x is kleiner dan of gelijk aan y ($x \leqslant y$) en x is groter dan y ($x > y$).

Een relatie op een verzameling V ofwel propositiefunctie P op $V \times V$ is dus ook een functie van $V \times V$ naar $\{0,1\}$ (0 voor onwaar, en 1 voor waar). Het is gebruikelijk (zie bijvoorbeeld het begrip 'binary relation' op wikipedia) om relaties niet als functies te definiëren maar als deelverzameling van $V \times V$. Hierbij correspondeert de functie $P : V \times V \to \{0,1\}$ met de deelverzameling $R := \{(x,y) \in V \times V : P(x,y) = 1\}$ van die (x,y) waarvoor $P(x,y)$ waar is. Uit deze deelverzameling kan de functie P weer terugbepaald worden, want voor $(x,y) \in V \times V$ die niet in R zitten geldt $P(x,y) = 0$. Wat hier gebeurt is vergelijkbaar met functies en hun grafieken. We hebben dit ook gezien in Opgave I.4.13.

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 $(a,b) \in R$. Meestal gebruiken we in plaats van een letter (zoals R) een symbool (zoals $<$ of $\sim$). De notatie $a \not R\ b$ staat voor $(a,b) \notin R$.

We bekijken in deze paragraaf een speciaal soort relatie: lineaire ordening. 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:

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

Notatie: $a < b$ betekent $(a \leqslant b) \wedge (a \neq b)$. Verder schrijven we $b \geqslant a$ voor $a \leqslant b$, en evenzo $b > a$ voor $a < b$.

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

Opgaven

S **1.** Laat V het gesloten interval $[0,1]$ in $\mathbb{R}$ zijn. Teken voor elk van de relaties $=$, $\neq$, $\leqslant$ en $>$ op V de daarbij horende deelverzameling van $V \times V$.

V **2.** (a) Bepaal alle lineaire ordeningen op de verzameling $\{1,2,3\}$. Als de gebruikelijke ordening hierbij een hindernis is, vervang dan de getallen 1, 2 en 3 dan door drie verschillende objecten (groenten, zoals spinazie, spruitjes en witlof, bijvoorbeeld) waarbij elke persoon een eigen rangorde heeft voor hoe lekker hij/zij ze vindt. Om eraan te wennen dat er op $\{1,2,3\}$ meerdere ordeningen zijn: denk eens aan 1e klasse, 2e klasse en 3e klasse. Of zelfs: 1egraadsbevoegdheid en 2egraadsbevoegdheid!

B (b) Hoeveel lineaire ordeningen zijn er op een verzameling met n elementen? (Waarom is het antwoord voor elke verzameling met n elementen hetzelfde?)

V **3.** Laat V een verzameling zijn en $\leqslant$ een lineaire ordening op V. Bewijs: $a < b$ als en alleen als $\neg(a \geqslant b)$.

✯ **4.** Is het volgende waar? Voor iedere lineaire ordening op een verzameling V bestaat er een injectieve functie $f : V \to \mathbb{R}$ die de ordening behoudt.

III.3 Equivalentierelaties

Het niveau van abstractie in deze sectie, met name waar het gaat over quotiëntverzamelingen en quotiëntafbeeldingen, is erg hoog. We vragen de lezer niet om dit de eerste keer geheel te begrijpen, maar wel om het geval van modulo n rekenen geheel te doorgronden. Later in dit dictaat spelen quotiëntverzamelingen een belangrijke rol, iedere keer als we iets willen construeren dat we nog niet hebben, zoals bijvoorbeeld de constructie van de gehele getallen vanuit de natuurlijke, van de rationale getallen vanuit de gehele, en van de reële getallen vanuit de rationale. Een ander voorbeeld is dat van projectieve ruimten (zie het vak Meetkunde).

equivalentierelatie **III.3.1 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:

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

representant quotiëntverzameling 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:

$$V/\!\sim\ = \big\{[a] : a \in V\big\}.$$

III.3.2 Voorbeeld.

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 $V/= = \{\{a\} \mid a \in V\}$.

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

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

$$R = \big\{(1,1),(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3),(4,4)\big\} \subseteq V \times V,$$

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.

iv) 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 Voorbeeld III.3.10 voor een uitleg van deze naamgeving.

v) Laat L de verzameling van leerlingen van een school zijn, en noem twee leerlingen equivalent als ze in dezelfde klas zitten. Dat is een equivalentierelatie, en de equivalentieklassen zijn precies de klassen. ▬

III.3.3 Stelling. Laat V een verzameling zijn, en $\sim$ een equivalentierelatie op V. Voor alle $x, y \in V$ geldt:

$$x \sim y \Leftrightarrow [x] = [y], \quad x \not\sim y \Leftrightarrow [x] \cap [y] = \varnothing$$

De verzameling V is dus de disjuncte vereniging van zijn equivalentieklassen, ofwel: V is *gepartitioneerd* door de equivalentieklassen.

Bewijs. Laat x en y in V zijn. Stel dat $x \sim y$. Voor iedere $z \in [x]$ geldt per definitie dat $z \sim x$, en dus dat $z \sim y$ vanwege de transitiviteit van $\sim$. Dus geldt dat $[x] \subseteq [y]$. Maar dan geldt net zo goed dat $[y] \subseteq [x]$, want de situatie is symmetrisch in x en y (symmetrie van $\sim$) en dus dat $[x] = [y]$.

Stel nu dat $[x] = [y]$. Natuurlijk geldt dat $x \in [x]$ (reflexiviteit), en dus $x \in [y]$, en dus ook dat $x \sim y$. De eerste equivalentie is nu bewezen.

Stel nu dat $[x] \cap [y] = \varnothing$. Dan is x geen element van $[y]$, en dus $x \not\sim y$. Als daarentegen $[x] \cap [y] \neq \varnothing$, dan neem $z \in [x] \cap [y]$ en constateer dat $z \sim x$, en dus ook $x \sim z$, en $z \sim y$, en dus (transitiviteit) $x \sim y$. ■

Het belangrijkste wat met een equivalentierelatie $\sim$ op een verzameling V gedaan kan worden is het vormen van een quotiëntafbeelding. In Opgave III.3.1 zien we dat voor $f : V \to W$ de relatie $\sim$ op V gegeven door $x \sim y \Leftrightarrow f(x) = f(y)$ een equivalentierelatie is. We kunnen ons nu afvragen of er, omgekeerd, voor iedere equivalentierelatie er zo'n afbeelding is, en hoe uniek zo'n afbeelding is. De volgende definitie en stelling maken dit alles duidelijk.

quotiëntafbeelding

III.3.4 Definitie. Zij V een verzameling, en $\sim$ een equivalentierelatie op V. Zij W een verzameling. Een afbeelding $q : V \to W$ heet een *quotiënt* voor $\sim$ als:

1. q is surjectief;
2. voor alle $x, y \in V$ geldt $x \sim y \Leftrightarrow q(x) = q(y)$.

III.3.5 Stelling. Zij V een verzameling, en $\sim$ een equivalentierelatie op V.

1. Laat $q : V \to V/\sim$ de afbeelding van V naar de quotiëntverzameling $V/\sim$ zijn gegeven door $q(x) = [x]$. Dan is q een quotiëntafbeelding.
2. Laat $q : V \to W$ en $q' : V \to W'$ quotiëntafbeeldingen zijn. Dan is er een unieke afbeelding $f : W \to W'$ met $q' = f \circ q$. Deze afbeelding f is een bijectie.

Bewijs. 1. Elk element van $V/\sim$ is van de vorm $[x]$ voor een zekere $x \in V$, maar $q(x) = [x]$ dus q is surjectief. Zij nu $x, y \in V$. Als $x \sim y$ dan geldt wegens Stelling III.3.3 dat $[x] = [y]$ en dus $q(x) = q(y)$. Omgekeerd, als $q(x) = q(y)$ dan geldt $[x] = [y]$ en met Stelling III.3.3 dus $x \sim y$.

2. Laat $q : V \to W$ en $q' : V \to W'$ quotiëntafbeeldingen zijn. We produceren eerst een afbeelding $f : W \to W'$ met de eigenschap $q' = f \circ q$. Laat

$$f = \{(q(x), q'(x)) : x \in V\} \subseteq W \times W'.$$

We bewijzen nu eerst dat f de grafiek van een functie van W naar W' is. Laat $b \in W$. Neem een $x \in V$ met $q(x) = b$ (surjectiviteit van q). Dan $(b, q'(x)) \in f$, dus er is minstens één $b' \in B'$ zodat $(b, b') \in f$. Stel nu dat (b, b'_1) en (b, b'_2) allebei in f zitten. Neem $x_1 \in V$ en $x_2 \in V$ met $(b, b'_1) = (q(x_1), q'(x_1))$ en $(b, b'_2) = (q(x_2), q'(x_2))$ (gebruik de definitie van f). Dan geldt $q(x_1) = b = q(x_2)$, en dus $x_1 \sim x_2$ (want q is

een quotiëntafbeelding). Maar dan geldt ook dat $b'_1 = q'(x_1) = q'(x_2) = b'_2$, want q' is ook een quotiëntafbeelding.

Voor alle $x \in V$ geldt nu dat $f(q(x)) = q'(x)$, want $(q(x), q'(x)) \in f$.

We bewijzen dat f een bijectie is. Vanwege de symmetrie in de situatie is f ook de grafiek van een functie van W' naar W, en dus de grafiek van een bijectie.

Tenslotte bewijzen we dat er maar één afbeelding $f : W \to W'$ kan bestaan met de eigenschap $q' = f \circ q$. Dat volgt direct uit de surjectiviteit van q: voor elke $w \in W$ is er een $x \in$ met $w = q(x)$, en dan moet gelden dat $f(w) = f(q(x)) = q'(x)$, dus er is hoogstens één mogelijkheid voor $f(w)$. ■

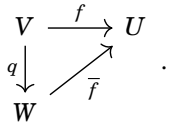
III.3.6 Opmerking. Onderdeel 2 van de bovenstaande stelling zegt dat alle quotiëntafbeeldingen voor een vaste equivalentierelatie alleen op een administratieve wijze verschillen. Iedereen kan zijn/haar eigen favoriete quotiëntafbeeldingen kiezen. Laten we dit illustreren met een flauw voorbeeld. Laat $\sim$ de equivalentierelatie 'mod 0' op $\mathbb{Z}$ zijn. Dan is $\mathrm{id}_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$ een quotiënt, maar ook $q : \mathbb{Z} \to \mathbb{Z}/\!\sim$, met $\mathbb{Z}/\!\sim = \{\{x\} : x \in \mathbb{Z}\}$, en $q : x \mapsto \{x\}$.

compatibel

III.3.7 Definitie. Laat V een verzameling zijn, $\sim$ een equivalentierelatie op V en $f : V \to W$ een afbeelding. Dan heet f *compatibel met* $\sim$ als voor alle x en y in V geldt dat $x \sim y \implies f(x) = f(y)$.

universele eigenschap

III.3.8 Stelling. Laat V een verzameling zijn en $\sim$ een equivalentierelatie op V. Laat $q : V \to W$ een quotiëntafbeelding voor $\sim$ zijn en $f : V \to U$ een een afbeelding die compatibel is met $\sim$. Dan is er een unieke afbeelding $\overline{f} : W \to U$ met $f = \overline{f} \circ q$. In een diagram:



Bewijs. De afbeelding q is surjectief, want een quotiënt. Laat nu $y \in W$. Dan is er een $x \in V$ met $y = q(x)$. De eis dat $f = \overline{f} \circ q$ impliceert dan dat $\overline{f}(y) = f(x)$, er is geen andere mogelijkheid en dat betekent dus dat er hoogstens één zo'n afbeelding $\overline{f}$ bestaat. We zouden $\overline{f}$ graag hiermee definiëren, maar dan moeten we wel nagaan dat het resultaat $f(x)$ niet afhangt van de keuze van x. Stel dus dat ook $x' \in V$ de eigenschap heeft dat $q(x') = y$. Dan geldt $x' \sim x$ (want q is een quotiënt voor $\sim$), en dus $f(x') = f(x)$ (want f is compatibel met $\sim$). We kunnen nu dus definiëren: voor $y \in W$, neem $x \in V$ met $q(x) = y$, dan $\overline{f}(y) = f(x)$. Dan geldt inderdaad dat $f = \overline{f} \circ q$. ■

Een nuttig gevolg van deze stelling is dat afbeeldingen $f : V \to U$ die compatibel zijn met de equivalentierelatie, eenvoudiger 'beschreven' kunnen worden: het zijn in essentie gewoon afbeeldingen $\overline{f} : W \to U$.

Hetzelfde idee kan worden toegepast op operaties. De volgende stelling is de belangrijkste motivatie voor alle moeite die we ons hebben gegeven in de voorgaande paragrafen.

III.3.9 Stelling. Stel dat V een verzameling is, $\bigcirc$ een operatie op V en $\sim$ een equivalentierelatie op 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 operatie $\triangle$ op $V/\!\sim$ 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 $\triangle$.

Bewijs. Zie Opgave III.3.2. ∎

geïnduceerde operatie

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

III.3.10 Voorbeeld. We veralgemeniseren Voorbeeld III.3.2 iv). 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, want elk element van $\mathbb{Z}/n\mathbb{Z}$ bestaat uit die $a \in \mathbb{Z}$ die een gegeven rest na deling door n hebben. In deze quotiëntverzameling is er vanwege compatibiliteit een operatie optellen en vermenigvuldigen. Dat noemen we *modulorekenen*. Zie voor details en concrete voorbeelden Opgaven III.3.3 en III.3.4. Merk overigens op dat de equivalentierelatie vaak als volgt wordt genoteerd:

modulorekenen

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

Modulorekenen of klokrekenen kom je soms in het voortgezet onderwijs tegen, bijvoorbeeld bij Wiskunde D. ∎

Opgaven

S **1.** (a) Laat A en B verzamelingen zijn, en $f : A \to B$ een afbeelding. Bewijs dat de relatie $\sim$ op A gegeven door: $x \sim y \Leftrightarrow f(x) = f(y)$ een equivalentierelatie is.

(b) Laat $f : \mathbb{Z} \to \{0,1\}$ de afbeelding zijn die a stuurt naar de rest na deling van a door 2. Laat zien dat voor alle a en b in $\mathbb{Z}$ geldt: $a \equiv_2 b \Leftrightarrow f(a) = f(b)$.

B **2.** Geef een bewijs van Stelling III.3.9.

V **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 $\mathbb{Z}/4\mathbb{Z}$.

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

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

(b) Zij $A \subseteq \mathbb{Z}$ een deelverzameling. Wat zijn noodzakelijke en voldoende voorwaarden 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.

V

5. (a) In Opgave III.3.4 heb je gezien dat er operaties 'optellen' en 'vermenigvuldigen' op $\mathbb{Z}/2\mathbb{Z}$ zijn. In Opgave II.1.2 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, en denk ook aan de meer recente bankierseed.

> *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 onbegrensd geheugen zouden hebben). De axioma's worden dan als uitgangspunt genomen in het bewijzen van weer andere beweringen over het getalsysteem $\mathbb{N}$.[1]

[1] In dit dictaat werken we met $\mathbb{N} = \{0,1,2,3,\ldots\}$, dat wil zeggen, we beschouwen 0 als een natuurlijk getal. Sommige auteurs laten $\mathbb{N}$ beginnen bij 1. Voor beide varianten zijn argumenten te geven.

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 $+\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, $(a,b)\mapsto a+b$, de optelling;
(d) een operatie $\cdot\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, $(a,b)\mapsto ab$, de vermenigvuldiging.

optelling

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 $a+1=0$ (m.a.w. 0 is het 'kleinst');
inductie
(N6) axioma van *inductie*: als $A\subseteq\mathbb{N}$ voldoet aan de eigenschappen $0\in A$ en $(a\in A)\Rightarrow(a+1\in A)$, 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 $f\colon\mathbb{N}\to\mathbb{N}'$ 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 $2=1+1$, $3=1+1+1$, $4=1+1+1+1,\ldots$.[2]

vermenigvuldiging

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

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.
Peano axioma's

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

IV.1.1 Lemma. 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. ■

[2] Wie hier 'niet-standaard' vragen over heeft mag contact opnemen met Bas.

ordening op $\mathbb{N}$

Uit de optelling op $\mathbb{N}$ kunnen we ook een *lineaire ordening* $\leqslant$ *op* $\mathbb{N}$ definiëren als volgt:

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

In Opgave IV.1.3 wordt bewezen dat deze relatie inderdaad een lineaire ordening is.

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

Opgaven

V ✍ **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 $a = b+1$. (Schrijf steeds expliciet op welk axioma **(N1)**–**(N10)** je gebruikt.)

V **2.** Zij $a, b \in \mathbb{N}$. Neem aan dat $ab = 0$. Bewijs dat $a = 0$ of $b = 0$.
(*Hint*: gebruik de voorgaande opgave.)

B ✍ **3.** Bewijs dat de relatie $\{(a,b) \in \mathbb{N}^2 : \exists_{c \in N}\, a + c = b\}$ op $\mathbb{N}$, die we noteren als $\leqslant$, een lineaire ordening is.

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*.

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:

inductieveronderstelling

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

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 $n \geqslant N$ 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. ∎

Tot slot bekijken we 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 $x^0 = 1$.

faculteit

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 $k \leqslant n$ definiëren

binomiaalcoëfficiënt

we de *binomiaalcoëfficiënt* $\binom{n}{k}$ (spreek uit "*n boven k*") als

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

We beschouwen $\binom{n}{k}$ voor nu als element van $\mathbb{Q}$ zonder al te precies te zijn over wat dat betekent. In Opgave IV.2.16 wordt bewezen dat $\binom{n}{k}$ een geheel getal is.

binomium van Newton

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 $n = 0$:

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

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.2.16:

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

■

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

welordening van $\mathbb{N}$

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 $w \geqslant v$.

Bewijs. We moeten bewijzen: $\exists_{v \in V}\ \forall_{w \in V}\ w \geqslant v$. We doen dit uit het ongerijmde: we nemen aan dat $\neg \exists_{v \in V}\ \forall_{w \in V}\ w \geqslant v$. Volgens de equivalenties aan het eind van Sectie II.2 over het verwisselen van negatie en kwantoren is wat we aannemen equivalent met $\forall_{v \in V}\ \neg \forall_{w \in V}\ w \geqslant v$. Door nogmaals die equivalenties toe te passen is wat we aannemen equivalent met $\forall_{v \in V}\ \exists_{w \in V}\ w < v$. Dus we weten dat voor alle $v \in V$ er een $w \in V$ is met $w < v$. Hieruit volgt dat $0 \notin V$. Zij $A \subseteq \mathbb{N}$ de volgende verzameling:

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

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

S ✍ **1.** Verzin zelf een formule voor

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

en bewijs de formule met behulp van volledige inductie voor elk natuurlijk getal n.

S **2.** Bewijs met behulp van volledige inductie dat voor alle natuurlijke getallen $n \geqslant 1$ de volgende gelijkheden gelden:

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

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

V **3.** Bewijs met behulp van volledige inductie dat voor alle natuurlijke getallen $n \geqslant 1$ de volgende gelijkheden 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) $\dfrac{1}{1\cdot 3}+\dfrac{1}{3\cdot 5}+\dfrac{1}{5\cdot 7}+\cdots+\dfrac{1}{(2n-1)(2n+1)} = \dfrac{n}{2n+1}$.

V **4.** Bewijs met behulp van volledige inductie: voor alle $n \geqslant 1$ geldt

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

V **5.** Doe nog een keer opgaven (a) en (b) van Opgave II.4.4, en vergelijk je uitwerkingen met die van de eerste keer.

S ✍ **6.** 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.

S ✍ **7.** Vind de fout in het volgende 'bewijs met volledige inductie' dat alle mensen op dezelfde dag jarig zijn:
Voor $n \in \mathbb{N}$ met $n \geqslant 1$, 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 $n \geqslant 1$, 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.

S **8.** 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 er precies $n(n-1)/2$ verschillende lijnen zijn die minstens 2 van de n punten bevatten.

S **9.** 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.

V **10.** (Uit de bundel Finaletraining Wiskunde Olympiade) Een aantal steden is verbonden door éénrichtingsverkeerwegen. Tussen elk tweetal steden loopt een directe weg (de ene kant op of de andere kant op). Bewijs dat er een stad is die te bereiken is vanuit alle andere steden (eventueel via andere steden).

V **11.** Bewijs met behulp van volledige inductie dat voor elke $n \in \mathbb{N}$ geldt $2^n > n$.

V **12.** Bewijs met behulp van volledige inductie dat voor elk natuurlijk getal $n \geqslant 4$ geldt $n! > 2^n$.

V ✍ **13.** Bewijs met behulp van volledige inductie dat voor elk natuurlijk getal n het getal $11^n - 4^n$ deelbaar is door 7.

B **14.** Bewijs met behulp van volledige inductie dat de som van de derde machten van drie opeenvolgende natuurlijke getallen deelbaar is door 9.

B **15.** Zij x een reëel getal. Laat zien met behulp van volledige inductie dat voor elke $n \in \mathbb{N}$ geldt

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

B **16.** Bewijs de volgende eigenschappen van de binomiaalcoëfficiënten.

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

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

Deze identiteit wordt mooi vormgegeven in de *Driehoek van Pascal*, zie `https://nl.wikipedia.org/wiki/Driehoek_van_Pascal`.

(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 $\binom{n}{m}$ een positief geheel getal is 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 $1 \leqslant m \leqslant n-1$.

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

✯ **18.** Maak een stapel van speelkaarten aan de rand van een tafel zodat de bovenste zo ver mogelijk uitsteekt over de rand van de tafel. Hoe ver kan je komen met n kaarten? En met oneindig veel kaarten?

IV.3 De recursiestelling

We hebben de faculteit-functie $\mathbb{N} \to \mathbb{N}$, $n \mapsto n!$ al gebruikt in het binomium van Newton (Stelling IV.2.3). De definitie die we daar gaven is: $n! = 1 \cdot 2 \cdot \cdots \cdot n$, met de afspraak dat $0! = 1$. Met deze definitie weten we hoe we, voor elke $n \in \mathbb{N}$, $n!$ kunnen uitrekenen. Maar toch komt de vraag op of we nu wel te maken hebben met een functie zoals gedefinieerd in Definitie I.3.1. Volgens die definitie is de vraag of we een deelverzameling van $\mathbb{N} \times \mathbb{N}$ hebben gedefinieerd waarvan de elementen precies de paren $(n, n!)$ zijn, waar n de natuurlijke getallen doorloopt. Het beste wat we nu kunnen schrijven voor deze verzameling is

$$\{(n, m) \in \mathbb{N} \times \mathbb{N} : m = 1 \cdot 2 \cdot \cdots \cdot n\}.$$

De stippeltjes hierin irriteren ons, want de notatie zegt niet wat er precies wordt bedoeld. We kunnen duidelijkere notatie in te voeren, zoals

$$1 \cdot 2 \cdot \cdots \cdot n = \prod_{k=1}^{n} k\,,$$

maar dan moeten we die notatie weer rechtvaardigen. Het probleem ligt hier niet zozeer in de ZFC axioma's, maar in de *taal* waarmee we verzamelingen kunnen definiëren. Deze taal is exact beschreven in Appendix VIII.2, in slechts een halve pagina, en we raden de lezer aan om de excursie naar die appendix te maken.

recursie

De rigoureuze oplossing voor ons probleem is *recursie*, wat in deze sectie behandeld wordt. De eerste stap is de stippeltjes weg te werken door de definitie van $n!$ *recursief* te maken:

$$0! = 1 \quad \text{en voor } n \in \mathbb{N}: \quad (n+1)! = (n+1) \cdot n!\,.$$

Meer algemeen willen we functies met domein $\mathbb{N}$ *recursief* kunnen definiëren. De volgende stelling legt uit wat we hier precies mee bedoelen. Laten we die stelling eerst eens informeel bespreken. De stelling zegt, dat, gegeven een verzameling X, een functie $F : X \to X$, en een element $x \in X$, er een unieke functie $f : \mathbb{N} \to X$ zodat $f(0) = x$, en zodat, voor alle $n \in \mathbb{N}$, $f(n+1) = F(f(n))$. Bijvoorbeeld geldt dan dat $f(1) = F(x)$, en $f(2) = F(F(x))$, en $F(3) = F(F(F(x)))$, enzovoorts. Dus $f(n) = F^{(n)}(x)$, waarin $F^{(n)} = F \circ F \circ \cdots \circ F$, waarin F precies n keer voorkomt (met de afspraak dat $F^{(0)} = \mathrm{id}_X$). Nu is het wéér zo dat de notatie $F^{(n)}$ die we hier gebruiken niet in de taal van ZFC voorkomt, en dat is waarom er een bewijs van bijna een pagina nodig is om de recursiestelling te bewijzen. Zonder overdrijving kunnen we wel stellen dat het bewijs van deze stelling een conceptuele sprong is van minstens dezelfde orde van grootte als die bij de stelling van Cantor, Stelling I.4.11. We vragen de lezer dus niet om in eerste instantie het bewijs ervan te doorgronden of zelfs te lezen, maar vooral om eerst te leren wat de Stelling IV.3.1 en Gevolg IV.3.2 betekenen, door toepassingen te bekijken, zoals Definitie IV.3.3, en de opgaven in deze sectie. Dit is de eerste keer dat we te maken hebben met het toepassen van een stelling die niet zo makkelijk te begrijpen is.

Nog een laatste opmerking. Wie Stelling IV.3.1 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.

recursiestelling

IV.3.1 Stelling. Laat X een verzameling zijn, $x \in X$, en $F : X \to X$ een afbeelding. Dan is er een unieke $f : \mathbb{N} \to X$ 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. Ter herinnering: we hebben het begrip functie $f\colon \mathbb{N} \to X$ gedefinieerd in Definitie I.3.1 als een deelverzameling (de grafiek van f) van $\mathbb{N} \times X$ die aan de eis voldoet dat voor iedere $n \in \mathbb{N}$ er precies één $y \in X$ is met $(n,y) \in f$. Hieronder gebruiken we deze definitie.

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 $g\colon \mathbb{N} \to X$ 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 $G\colon \mathbb{N} \times X \to X$, en $x \in X$. Dan is er een unieke $f\colon \mathbb{N} \to X$ met:

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

Bewijs. Laat $F\colon \mathbb{N} \times X \to \mathbb{N} \times X$ gegeven zijn door $F(a,y) = (a+1, G(a,y))$. Vanwege de vorige stelling is er een unieke $h\colon \mathbb{N} \to \mathbb{N} \times X$ met $h(0) = (0,x)$, en met, voor alle $n \in \mathbb{N}$, $h(n+1) = F(h(n))$. Laat $h_1\colon \mathbb{N} \to \mathbb{N}$ en $h_2\colon \mathbb{N} \to X$ gedefinieerd zijn als volgt: voor elke $n \in \mathbb{N}$ geldt

$$h(n) = (h_1(n), h_2(n)).$$

Dan geldt:

$$(h_1(0), h_2(0)) = (0,x),$$

en, voor all $n \in \mathbb{N}$,

$$\begin{aligned}(h_1(n+1), h_2(n+1)) = h(n+1) = F(h(n)) = F(h_1(n), h_2(n)) \\ = (h_1(n)+1, G(h_1(n), f(h_1(n)))).\end{aligned}$$

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. ∎

Als eerste toepassing definiëren we de functie 'faculteit' van $\mathbb{N}$ naar $\mathbb{N}$. We gaan Gevolg IV.3.2 toepassen. Dat betekent dat we moeten zeggen welke verzameling X we nemen, welk element x, en welke functie $G\colon \mathbb{N}\times X\to X$. Het gevolg geeft een functie $f\colon \mathbb{N}\to X$, en wij willen een functie $f\colon \mathbb{N}\to\mathbb{N}$, dus voor X moeten we $\mathbb{N}$ nemen. We willen $f(0)=0!=1$, dus voor x moeten we 1 nemen. Verder willen we dat, voor alle $n\in\mathbb{N}$, $f(n+1)=(n+1)\cdot f(n)$, en het gevolg geeft dat $f(n+1)=G(n,f(n))$, dus voor G kunnen we nemen: $(a,b)\mapsto(a+1)\cdot b$. Nu zijn we klaar om de definitie op te schrijven.

faculteit

IV.3.3 Definitie. Laat $n\mapsto n!$ de unieke functie van $\mathbb{N}$ naar $\mathbb{N}$ zijn, genaamd *faculteit*, 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 $G\colon\mathbb{N}\times\mathbb{N}\to\mathbb{N}$, $(a,b)\mapsto(a+1)b$.

IV.3.4 Definitie. Voor $n,k\in\mathbb{N}$ met $k\leqslant n$ definiëren we een rationaal getal door:

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

binomiaalcoëfficiënt

De getallen $\binom{n}{k}$ heten *binomiaalcoëfficiënten*.

Per definitie is $\binom{n}{k}$ in $\mathbb{Q}$, maar uit Opgave IV.2.16 volgt $\binom{n}{k}\in\mathbb{N}$.

Opgaven

S **1.** Vermenigvuldiging van natuurlijke getallen kan worden gedefiniëerd als herhaalde optelling: $n\cdot m=m+\cdots+m$, met n termen m. We willen van de puntjes in deze definitie afkomen. Gebruik Stelling IV.3.1 om te laten zien dat er voor iedere m in $\mathbb{N}$ een functie $v_m\colon\mathbb{N}\to\mathbb{N}$ is met de eigenschappen $v_m(0)=0$, en voor alle $n\in\mathbb{N}$: $v_m(n+1)=v_m(n)+m$.
Doe nog eens hetzelfde, maar dan met Gevolg IV.3.2.
Hierna kan men definiëren, voor n en m in $\mathbb{N}$: $n\cdot m:=v_m(n)$.

S **2.** Voor n en m in $\mathbb{N}$ kan m^n gedefiniëerd worden door herhaald te vermenigvuldigen. Geef een preciese definitie met behulp van Stelling IV.3.1.

V **3.** Laat $a\colon\mathbb{N}\to\mathbb{N}$ een rij in $\mathbb{N}$ zijn. Dan is voor n in $\mathbb{N}$ de som $\sum_{i=0}^{n}a(i)$ recursief gedefiniëerd door:

$$\sum_{i=0}^{0}a(i)=a(0)\quad\text{en voor alle } n\in\mathbb{N}:\quad\sum_{i=0}^{n+1}a(i)=\Big(\sum_{i=0}^{n}a(i)\Big)+a(n+1).$$

Geef aan hoe Gevolg IV.3.2 toegepast kan worden om deze recursieve definitie te rechtvaardigen.

V **4.** Laat $a\colon\mathbb{N}\to\mathbb{N}$ een rij in $\mathbb{N}$ zijn. Dan is voor n in $\mathbb{N}$ het product $\prod_{i=0}^{n}a(i)$ recursief gedefiniëerd door:

$$\prod_{i=0}^{0}a(i)=a(0)\quad\text{en voor alle } n\in\mathbb{N}:\quad\prod_{i=0}^{n+1}a(i)=\Big(\prod_{i=0}^{n}a(i)\Big)\cdot a(n+1).$$

Geef aan hoe Gevolg IV.3.2 toegepast kan worden om deze recursieve definitie te rechtvaardigen.

B **5.** De *rij van Fibonacci* is de functie $f : \mathbb{N} \to \mathbb{N}$ die recursief gedefiniëerd is door

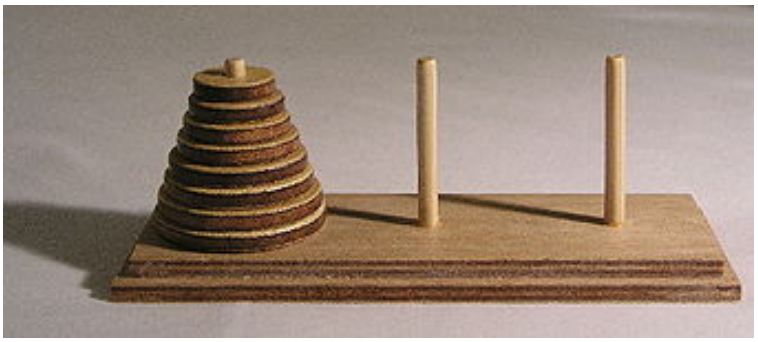
$$\begin{cases} f(0) = 0, \\ f(1) = 1, \\ \forall_{n \geqslant 2}\ f(n) = f(n-1) + f(n-2). \end{cases}$$

(a) Bereken $f(2), \ldots, f(10)$.

(b) Merk op dat de recursie in de definitie van f 2 diep is: $f(n) = f(n-1) + f(n-2)$. Bedenk hoe het toch mogelijk is om Stelling IV.3.1 te gebruiken om f te definiëren. Hint: $(f(n), f(n-1)) = (f(n-1) + f(n-2), f(n-1))$ in $\mathbb{N}^2$.

(c) Denk eens na over de analogie tussen de recursiestelling en functies $y : \mathbb{R} \to \mathbb{R}$ gedefinieerd door 1ste-orde differentiaalvergelijkingen $y' = F(x, y)$ en een beginvoorwaarde $y(0) = a$ (bijvoorbeeld $y' = y$ en $y(0) = 1$), en door 2e-orde differentiaalvergelijkingen $y'' = F(x, y, y')$ en een beginvoorwaarde $y(0) = a$ en $y'(0) = b$ (bijvoorbeeld $y'' = -y$ en $y(0) = 0$ en $y'(0) = 1$).

B **6.** De Torens van Hanoi is een spel of puzzel met een aantal schijven:



Het spel bestaat uit een plankje met daarop drie stokjes. Bij aanvang van het spel is op een van de stokjes een kegelvormige toren geplaatst van schijven met een gat in het midden. De schijven hebben verschillende diameters, in toenemende grootte. Ze zijn zo geplaatst dat de kleinste schijf bovenop en de grootste onderop ligt.
Het doel van het spel is om de complete toren van schijven te verplaatsen naar een ander stokje, waarbij de volgende regels in acht genomen dienen te worden:

1. er mag slechts 1 schijf tegelijk worden verplaatst;
2. nooit mag een grotere schijf op een kleinere rusten.

Bedenk hoe je dit probleem recursief oplost.

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 Perzische wiskundige al-Chwarizmi (Bagdad, 780–850) 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 (met andere woorden, het bestaan van getalssystemen met de gewenste eigenschappen volgt uit ZFC).

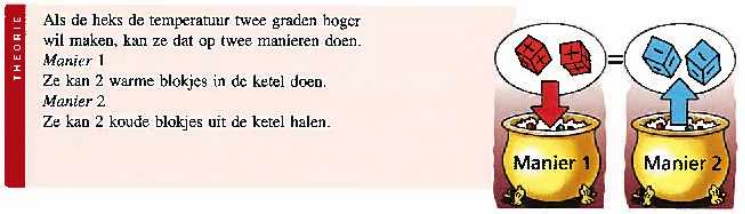
structureel perspectief

constructief perspectief

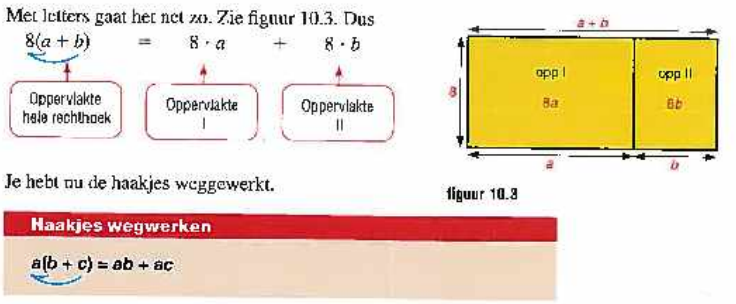
V.0.1 Voorbeeld. Negatieve getallen worden in de onderbouw geïntroduceerd. Je zal als docent hierbij belangrijke didactische keuzes moeten maken. De getallenlijn is een natuurlijke metafoor om negatieve getallen te introduceren, maar enkel op grond hiervan zal het voor leerlingen niet meteen duidelijk zijn hoe met negatieve getallen gerekend kan worden. Schoolboeken gebruiken soms 'denkmodellen' om dit uit te leggen, zoals de heks (zie Figuur V.0.2). Het gebeurt ook dat docenten

rekenregels zoals ‘min keer min is plus’ gewoon poneren.

Ook als leerlingen eenmaal vertrouwd zijn geraakt met negatieve getallen, 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 V.0.3), waarbij de lengtes noodzakelijkerwijs niet negatief zijn. ∎



V.0.2 Figuur. Het denkmodel van de heks voor rekenen met negatieve getallen in het schoolboek *Moderne wiskunde*.



V.0.3 Figuur. De distributieve eigenschap van optelling in het schoolboek *Getal & Ruimte*.

V.0.4 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:

optelling

1. de operatie optelling
   (a) is associatief (dus $a +_R (b +_R c) = (a +_R b) +_R c$ voor alle $a, b, c \in R$),
   (b) is commutatief (dus $a +_R b = b +_R a$ voor alle $a, b \in R$),
   (c) heeft 0_R als neutraal element,
   (d) heeft een inverse (genoteerd met $-_R a$) voor ieder element $a \in R$;

vermenigvuldiging

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 $a, b, c \in R$).

commutatief

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 Voorbeeld. 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.

De verzameling $\{f : \mathbb{R} \to \mathbb{R}\}$ van alle functies van $\mathbb{R}$ naar $\mathbb{R}$ met als optelling de *puntsgewijze optelling* (voor f en g is $f+g$ de functie $x \mapsto f(x)+g(x)$) en de *puntsgewijze vermenigvuldiging* ($f \cdot g$ is de functie $x \mapsto f(x) \cdot g(x)$) is ook een commutatieve ring. Deze operaties worden gebruikt in uitdrukkingen als $\sin^2 + \cos^2$. ∎

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'.

rekenregels in een ring

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) Het is misschien verstandig eerst de opmerking na dit bewijs te lezen, om niet al te verbaasd te zijn over wat volgt. Er geldt

$$a \cdot_R 0_R = a \cdot_R (0_R +_R 0_R) = a \cdot_R 0_R +_R a \cdot_R 0_R.$$

Als toelichting hierbij: de 1e gelijkheid volgt uit het neutraal zijn van 0_R voor de operatie $+_R$, en de 2e gelijkheid volgt uit de distributieve eigenschap van $\cdot_R$ over $+_R$. 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 Lemma IV.1.1 — zie je het subtiele verschil?)

De overige onderdelen zijn onderwerp van Opgave V.1.2. ∎

Laten we een belangrijke **opmerking** maken. De lezer zal waarschijnlijk verbaasd zijn over het bewijs dat hierboven is gegeven: hoe kom je daar nu op? Het antwoord hierop is dat er geen methode bekend is om dit soort bewijzen te vinden, maar dat op een verstandige manier proberen tot resultaat leidt. Men merkt op dat alleen de elementen 0_R en a in de te bewijzen uitspraak voorkomen. En ook dat 0_R het neutrale element van de optelling is, terwijl de uitspraak over vermenigvuldigen gaat. En dat de distributieve eigenschappen de enige axioma's zijn die de optelling en vermeniguldiging met elkaar in verband brengen.

Het wordt niet van de lezer verwacht dat die zelf op dit bewijs komt, maar wel dat hij/zij het bewijs begrijpt, en na het zien van een aantal van dit soort bewijzen, zelfstandig soortgelijke uitspraken kan bewijzen.

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.

lichaam

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}.

V.1.5 Voorbeeld. De systemen van rationale ($\mathbb{Q}$), reële ($\mathbb{R}$) en complexe ($\mathbb{C}$) getallen zijn voorbeelden van lichamen.

In Voorbeeld III.3.10 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.3.3 ontdek je dat deze ring een lichaam is precies 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.1.13. ∎

eindig lichaam

In de volgende stelling gebruiken we de notatie $\frac{a}{c}$ voor ac^{-1} en we laten voor het gemak de subscript $_R$ weg.

rekenregels in een lichaam

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.1.4. ∎

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.

homomorfisme

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 $f(a \cdot_R b) = f(a) \cdot_S f(b)$;
- het neutrale element van vermenigvuldiging blijft behouden: $f(1_R) = 1_S$.

Je zou misschien verwachten dat ook geëist moet worden dat het neutrale element van 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_R^{-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:

$$f(a_R^{-1}) \cdot_S f(a) = f(a_R^{-1} \cdot_R a) = f(1_R) = 1_S. \qquad \blacksquare$$

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.

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 $f : R \to S$ een isomorfisme is, dan vertalen f en f^{-1} alle eigenschappen van R en S als ringen in elkaar. Iets preciezer: R en S hebben dezelfde *structurele* eigenschappen, zoals bedoeld in de inleiding van dit hoofdstuk. 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.

Een isomorfisme $f : R \to S$ van ringen is noodzakelijk een bijectie: de afbeelding f^{-1} in Definitie V.1.9 is, zoals de notatie suggereert, de inverse van f (zie Opgave I.3.18). Omgekeerd geldt:

V.1.10 Stelling. Een bijectief homomorfisme is een isomorfisme.

Bewijs. Zie Opgave V.1.7. $\blacksquare$

V.1.11 Voorbeeld. Beschouw op de verzameling $R = \{0, 1\}$ de operatie $\veebar$ (exclusief of) uit Opgave II.1.2, en de operatie $\wedge$ (conjunctie). Het systeem $(R, \veebar, \wedge, 0, 1)$ is een lichaam.

Zij verder $\mathbb{F}_2$ het lichaam van twee elementen uit Voorbeeld V.1.5. We noteren voor $x \in \mathbb{Z}$ met $\overline{x}$ de restklasse van x in $\mathbb{F}_2$. Dan is de functie $f : R \to \mathbb{F}_2$, $f(0) = \overline{0}$, $f(1) = \overline{1}$ een isomorfisme. Het bewijs van deze beweringen is Opgave V.1.8. $\blacksquare$

geordende ring

V.1.12 Definitie. Een *geordende ring* is een commutatieve ring R met een relatie $\leqslant$ waarvoor geldt:

1. $\leqslant$ is een lineaire ordening;
2. voor alle $a, b, c \in R$ geldt $a \leqslant b \Rightarrow a +_R c \leqslant b +_R c$;
3. voor alle $a, b \in R$ geldt $(0_R \leqslant a \wedge 0_R \leqslant b) \Rightarrow 0_R \leqslant a \cdot_R b$.

Een element $a \in R$ heet *positief* als $0_R < a$ en *negatief* als $a < 0_R$. De deelverzameling van positieve elementen noteren we met R_+ of met $R_{\geqslant 0}$.

geordend lichaam

Als R een lichaam is en een geordende ring, dan noemen we het een *geordend lichaam*.

Het standaardvoorbeeld van een geordende ring is de ring $\mathbb{Z}$ van gehele getallen. Op de verzameling $\mathbb{Z}$ hebben we immers een lineaire ordening ($\mathbb{Z}$ ligt op de getallenlijn), en aan de overige twee eisen in de definitie is voldaan omdat deze lineaire ordening behouden is onder schuiven (de translatie $x \mapsto x + c$), dat is eis 2, en omdat het product van niet-negatieve getallen weer niet-negatief is, dat is eis 3. Op dezelfde manier zie je dat $\mathbb{Q}$ en $\mathbb{R}$ geordende lichamen zijn.

Let op de voorwaarden $0_R \leqslant a$ en $0_R \leqslant b$ in de laatste eigenschap van geordende ringen. Bij vermenigvuldiging met negatieve getallen 'klapt het teken om' (Opgave V.1.11). Merk ook op dat 'niet negatief' niet hetzelfde is als 'positief' — deze fout wordt wel eens gemaakt, hoewel er ook (briljante) wiskundeteksten zijn waarin wordt afgesproken (!) dat 0 ook positief wordt genoemd.[1]

absolute waarde

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.1.11 volgt $0_R \leqslant |a|$.

Opgaven

S **1.** 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.)

V ✍ **2.** Bewijs de nog niet bewezen onderdelen van Stelling V.1.3.

V **3.** In de ring van gehele getallen geldt de volgende eigenschap:

$$ab = 0 \quad \Longrightarrow \quad a = 0 \quad \vee \quad b = 0.$$

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.

V **4.** Bewijs Stelling V.1.6.

B **5.** Laat F een lichaam zijn, en $a \in F$. Bewijs dat er hoogstens 2 elementen $x \in F$ zijn met $x^2 = a$.

S **6.** 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.

V ✍ **7.** Bewijs Stelling V.1.10.

V **8.** Bewijs de beweringen in Voorbeeld V.1.11.

B **9.** Laat A een verzameling zijn. Voor twee deelverzameling $X, Y \subseteq A$ definiëren we het *symmetrisch verschil*

$$X \triangle Y = (X \cup Y) \setminus (X \cap Y).$$

(a) Teken X, Y en $X \triangle Y$ in een venndiagram.

(b) Zij $\mathscr{P}(A)$ de machtsverzameling van A. Bewijs dat $(\mathscr{P}(A), \triangle, \cap, \varnothing, A)$ een ring is. Is het een lichaam?

(c) Zij $\mathscr{F}(A)$ de verzameling van alle functies $f : A \to \mathbb{F}_2$. Bewijs dat $\mathscr{F}(A)$, met puntsgewijze optelling en puntsgewijze vermenigvuldiging, een ring is.

(d) Laat zien dat $\mathscr{P}(A)$ en $\mathscr{F}(A)$ isomorf zijn.

B **10.** Laat R een ring zijn, en g in R een element dat een multiplicatieve inverse heeft.

(a) Laat zien dat de afbeelding $c_g : R \to R$ gegeven door $x \mapsto gxg^{-1}$ een homomorfisme is.

(b) Laat zien dat c_g een isomorfisme is. Hint: gok de inverse en laat dan zien die inderdaad de inverse is.

V **11.** Zij R een geordende ring. We laten voor het gemak de index $_R$ uit de notatie weg. Bewijs de volgende uitspraken.

(a) $\forall_{a,b,c,d \in R}\ (a \leqslant b \wedge c \leqslant d) \implies a + c \leqslant b + d$;

(b) $\forall_{a \in R}\ (a \leqslant 0 \iff 0 \leqslant -a)$;

(c) $\forall_{a \in R}\ (0 \leqslant a \vee 0 \leqslant -a)$;

(d) $\forall_{a \in R}\ 0 \leqslant a^2$;

(e) $0 \leqslant 1$;

(f) $\forall_{a,b,c \in R}\ (a \leqslant b \wedge 0 \leqslant c) \implies ac \leqslant bc$;

(g) $\forall_{a,b,c \in R}\ (a \leqslant b \wedge c \leqslant 0) \implies bc \leqslant ac$.

V **12.** Laat R een ring zijn. 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.

B (e) Algemener: bewijs dat er voor iedere ring R een *uniek* homomorfisme $\mathbb{Z} \to R$ bestaat.

B **13.** Voor deze opgave is Opgave V.1.12 vereist. Gegeven is een lichaam F. Bekijk het inverse beeld $c^{-1}(0)$ van de canonieke afbeelding $c : \mathbb{N} \to F$. Als dit inverse beeld 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 de karakteristiek van F ofwel 0, ofwel 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 alleen als F karakteristiek p heeft.

(c) Laat zien: er bestaat een homomorfisme $\mathbb{Q} \to F$ als en alleen 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.

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 en de lineaire ordening daarop. Een *constructie* vanuit $\mathbb{N}$ stellen we uit tot paragraaf V.5.

Het systeem van gehele getallen is een geordende 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 $\mathbb{N} \subseteq R$ 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 geordende ring $(Z, +, \cdot, 0, 1, \leqslant)$ zodat de canonieke functie $c : \mathbb{N} \to Z$ uit Opgave V.1.12 een bijectie geeft van $\mathbb{N}$ naar $\{x \in Z : 0 \leqslant x\}$. Bovendien geldt:

1. als ook $(Z', +', \cdot', 0', 1', \leqslant')$ aan deze eisen voldoet, dan is er een uniek isomorfisme van geordende ringen $f : Z \to Z'$. Informeel gezegd: elk tweetal van zulke systemen verschilt alleen administratief.
2. Z kan zo gekozen worden dat het een uitbreiding van $\mathbb{N}$ is.

Het bewijs stellen we uit tot Paragraaf V.5.

We noemen een geordende ring als in voorgaande stelling een *geordende ring van gehele getallen*. We kiezen vanaf nu 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

gehele getallen

[1] In Vlaanderen geldt 0 gebruikelijk als positief én negatief getal.

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. Voor $a \in \mathbb{Z}$ geldt $a \in \mathbb{N}$ of $-a \in \mathbb{N}$.

Bewijs. Laat a in $\mathbb{Z}$. Vanwege de tweede eis in de definitie van lineaire ordening geldt dan $0 \leqslant a$ of $a \leqslant 0$. In het eerste geval geldt $a \in \mathbb{N}$, en in het tweede geval dat $-a \in \mathbb{N}$ (zie als nodig Opgave V.1.11). ■

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.1.2. 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). ■

Opgaven

V ✍ **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).

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.

deler
veelvoud

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 $\pm p$.

priemontbinding

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 Paragraaf II.3).

stelling van Euclides

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 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 $q = q'$. ∎

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 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*.

ggd

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. ∎

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.

algoritme van Euclides

V.3.6 Lemma. Zij $a, b \in \mathbb{N}$ met $a > b > 0$. Zij r de rest bij deling van a door b. Dan geldt

$$\text{ggd}(a, b) = \text{ggd}(b, r).$$

Bewijs. Zie Opgave V.3.5. ∎

V.3.7 Voorbeeld. We willen de grootste gemene deler van 2520 en 1100 bepalen. Het euclidisch algoritme gaat als volgt[2]:

$$\begin{array}{rcl@{\quad}l@{\quad}rcl@{\quad}l}
\gcd(2520,1100) & = & \gcd(1100,320), & \text{want} & 2520-2\cdot 1100 & = & 320; & \text{(i)}\\
\gcd(1100,320) & = & \gcd(320,140), & \text{want} & 1100-3\cdot 320 & = & 140; & \text{(ii)}\\
\gcd(320,140) & = & \gcd(140,40), & \text{want} & 320-2\cdot 140 & = & 40; & \text{(iii)}\\
\gcd(140,40) & = & \gcd(40,20), & \text{want} & 140-3\cdot 40 & = & 20; & \text{(iv)}\\
\gcd(40,20) & = & \gcd(20,0), & \text{want} & 40-2\cdot 20 & = & 0; & \text{(v)}\\
\gcd(20,0) & = & 20. & & & & &
\end{array}$$

We lezen hieruit af dat $\gcd(2520,1100) = \cdots = \gcd(40,20) = 20$.

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:

$$\begin{array}{rrcl}
\text{(i)} & 2520 & - 2 \cdot & 1100 = 320\\
\text{(ii)} & 1100 & - 3 \cdot & 320 = 140\\
\text{(iii)} & 320 & - 2 \cdot & 140 = 40\\
\text{(iv)} & 140 & - 3 \cdot & 40 = \boxed{20}\\
\text{(v)} & 40 & - 2 \cdot & 20 = 0
\end{array}$$

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).

$$\begin{aligned}
\text{(iv) is:} \quad & 140-3\cdot 40 = 20\\
\text{gebruikmakend van (iii):} \quad & 140-3\cdot(320-2\cdot 140) = 20\\
& 7\cdot 140-3\cdot 320 = 20\\
\text{gebruikmakend van (ii):} \quad & 7\cdot(1100-3\cdot 320)-3\cdot 320 = 20\\
& 7\cdot 1100-24\cdot 320 = 20\\
\text{gebruikmakend van (i):} \quad & 7\cdot 1100-24\cdot(2520-2\cdot 1100) = 20\\
& 55\cdot 1100-24\cdot 2520 = 20
\end{aligned}$$

uitgebreide algoritme van Euclides

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. ∎

Tot slot komen we terug op de uniciteit van de priemontbinding. We hebben inmiddels de technieken ontwikkeld om het volgende cruciale lemma te bewijzen.

lemma van Gauss

V.3.8 Lemma (Gauss). Zij $a,b \in \mathbb{Z}$ en zij p een priemgetal. Als $p \mid ab$, dan $p \mid a$ of $p \mid b$.

Bewijs. Stel $p \mid ab$ terwijl $p \nmid a$. Omdat p een priemgetal is en $p \nmid a$, geldt $\gcd(p,a) = 1$. Volgens Stelling V.3.5 zijn er dan $m,n \in \mathbb{Z}$ zodat

$$mp + na = 1.$$

Als we links en rechts met b vermenigvuldigen, krijgen we

$$mpb + nab = b.$$

[2] Zie ook een uitwerking op YouTube: `http://youtu.be/7Es4j-0Gf_I` en `http://youtu.be/sEZQwLBEo48`.

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 $p|b$. ■

hoofdstelling van de rekenkunde

V.3.9 Stelling (Hoofdstelling van de rekenkunde). Voor elk positief geheel getal n bestaat er een **unieke** rij priemgetallen $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$ $(r \in \mathbb{N})$ zodat

$$n = p_1 p_2 \cdots p_r.$$

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, …, 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

S **1.** (a) Laat zien dat de relatie | (“is deler van”) géén lineaire ordeningsrelatie is.

(b) Laat zien dat het ook geen equivalentierelatie is.

S **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 $b \neq 0$?

V ✍ **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) $\forall_{a,b,c\in\mathbb{Z}}\ a|(b+c) \implies (a|b \vee a|c)$

V ✍ **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.)

V ✍ **5.** Bewijs Lemma V.3.6.

V **6.** Bepaal steeds met behulp van het euclidische algoritme één paar gehele getallen m, n dat voldoet aan de gegeven vergelijking.

(a) $341m + 259n = 1$;

(b) $503m + 401n = 1$;

(c) $2849m + 791n = \text{ggd}(2849, 791)$;

(d) $689m + 403n = 39$.

V ✍ **7.** Bereken de ggd van $3^{100} + 2^{100}$ en $3^{100} - 2^{100}$.

V **8.** 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.

B **9.** 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?

S ✍ **10.** In de film *Die Hard with a Vengeance* 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?

V ✍ **11.** (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?

B (d) Wat kun je zeggen over het product van de ggd en het kgv?

B ✍ **12.** 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.

S ✍ **13.** (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?

V ✍ **14.** Alle positieve delers van het getal 54 vind je terug in een vermenigvuldigingstabel:

$\times$	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 positieve delers.

(e) Bepaal alle getallen tussen 0 en 200 die precies tien positieve delers hebben.

B **15.** 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?

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.

Ook het bewijs van deze stelling stellen we uit tot Paragraaf V.5; zie Opgave V.5.4, maar ook Opgave V.1.13. 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.

rationale getallen

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 is injectief. (Dit maakt de uitspraak precies dat $\mathbb{Q}$ de kleinste uitbreiding van $\mathbb{Z}$ is.)

Bewijs. We bewijzen eerst onderdeel (ii). 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:

$$1_R = f(1) = f((a-b)(a-b)^{-1}) = f(a-b)f((a-b)^{-1}) = 0_R.$$

Nu bewijzen we onderdeel (i). Voor elke b en c in $\mathbb{Z}$ met $c \neq 0$ hebben we $b/c := b \cdot c^{-1}$ in $\mathbb{Q}$. Laat nu F de deelverzameling van $\mathbb{Q}$ zijn gegeven door al deze b/c. Dan is F een deellichaam van $\mathbb{Q}$, en een uitbreiding van $\mathbb{Z}$. Nu komt de moeilijke stap: we passen Stelling V.4.1 toe op deze F. Dan krijgen we een homomorfisme $f : \mathbb{Q} \to F$. Deze f is surjectief, want elke b/c in F gaat naar zichzelf. Vanwege onderdeel (ii) is f ook injectief, dus bijectief. Dus $F = \mathbb{Q}$, en onderdeel (i) is bewezen. ∎

breuk

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.

De lineaire ordening $\leqslant$ op $\mathbb{Z}$ laat zich uitbreiden tot een lineaire ordening op $\mathbb{Q}$ (zie Opgave V.4.2). 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 $a \leqslant nb$.

Bewijs. Opgave V.4.3. ∎

Opgaven

S **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 $\text{ggd}(b,c) = 1$ en $a = \frac{b}{c}$.

V **2.** 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 definiëren 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.

V **3.** Bewijs Stelling V.4.3.

V **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."

B **5.** We borduren voort op de notatie in Opgave V.3.15. Bewijs dat er voor ieder rationaal getal $a \neq 0$ een unieke functie $e : \mathscr{P} \to \mathbb{Z}$ bestaat waarvoor geldt dat $e^{-1}(\mathbb{Z} \setminus \{0\})$ eindig is en

$$a = \pm \prod_{p \in \mathscr{P}} p^{e(p)}.$$

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.

constructie van $\mathbb{Q}$

We denken over $\mathbb{Q}$ als een verzameling breuken

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z} \wedge b \in \mathbb{Z} \setminus \{0\} \right\}.$$

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 definiëren die compatibel zijn met $\sim$. We kunnen dan immers Stelling III.3.9 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.

constructie van $\mathbb{Z}$

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. 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.3.9. Distributiviteit kun je controleren door definities te ontrafelen; dat gebeurt in Opgave V.5.3. 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.1.12). 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

$$F(a,c)=C(a)-C(c)=C(b)-C(d)=F(b,d).$$

De conclusie is dat F equivalente elementen op hetzelfde element afbeeldt. Vanwege Stelling III.3.8 is er dus een welgedefinieerde afbeelding $f\colon Z\to R$ 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 $g\circ f\colon Z\to Z$. 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[3] 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[4]. ∎

[3] 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.

[4] Er is hier een vervelend technisch detail, namelijk dat we wel zeker moeten weten dat $\mathbb{N}$ en Z

Opgaven

S **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.

V ✍ **2.** Bewijs Stelling V.5.2.

V ✍ **3.** Bewijs dat vermenigvuldigen distributief is over optellen in $(\mathbb{N}\times\mathbb{N})/\sim$ (zie het bewijs van Gevolg V.5.3).

B **4.** In deze paragraaf is gedetailleerd beschreven hoe $\mathbb{Z}$ kan worden geconstrueerd uit $\mathbb{N}$. Ook is in Opmerking V.5.1 een globaal programma beschreven hoe $\mathbb{Q}$ kan worden geconstrueerd uit $\mathbb{Z}$. Voer dit programma in detail uit.

V **5.** 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 gedegenereerd is. De breuknotatie $\frac{a}{c}$ voor rationale getallen is daarentegen wél gedegenereerd. Is er hier niet ook een alternatieve, niet gedegenereerde notatie? En waarom gebruiken we die niet gewoon?

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”.

deellichaam
lichaamsuitbreiding

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.

polynoomring

Zij K een lichaam. We noteren met $K[X]$ de verzameling[5] *polynomen met coëfficiënten in* K. Deze verzameling bestaat dus uit de polynomen

$$f(X)=\sum_{i\in\mathbb{N}} f_iX^i,\qquad \text{waarin } f_i\in K \text{ en } f_i=0 \text{ voor alle } i \text{ op eindig veel na.}$$

graad

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 nulpoly-

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.

[5] Voor een verzamelingstheoretische constructie van zo'n verzameling, uitgaande van de ZFC-axioma's, verwijzen we naar een algebraboek.

noom 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:

deler
- Een polynoom $g(X)$ is een *deler* van een polynoom $f(X)$ als er een polynoom $h(X)$ bestaat zodat $f(X) = g(X) \cdot h(X)$.

irreducibel
- Een polynoom $f(X)$ van positieve graad is *irreducibel* als er geen polynomen van positieve graad $g(X)$ en $h(X)$ bestaan zodat $f(X) = g(X) \cdot h(X)$.

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 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

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_{n-1} X^{n-1} \qquad (a_i \in K \text{ voor } 0 \leqslant i < n).$$

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.

constructie van $\sqrt{2}$

V.6.3 Voorbeeld. 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.

constructie van i

Bekijk het irreducibele polynoom $g(X) = X^2 + 1$ in $\mathbb{R}[X]$. We noteren net als hiervoor $\mathbb{R}(i) = \mathbb{R}[X]/(f(X))$. 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 $a, b, c, d \in \mathbb{Q}$. ∎

algebraïsch

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 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 Voorbeeld. 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 (zie Opgave VI.3.5). ∎

Opgaven

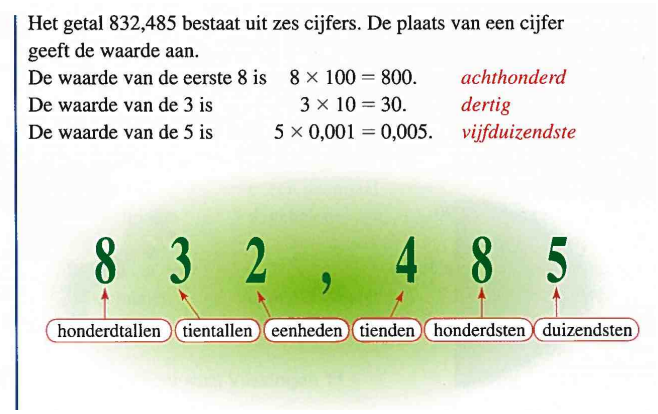
1. (a) Werk de rekenregels voor elementen uit $\mathbb{R}(i)$ uit zoals in Voorbeeld V.6.3.
(b) Doe hetzelfde voor $\mathbb{Q}(\sqrt{2}, i)$.
(c) Doe hetzelfde voor $\mathbb{Q}[X]/(X^3 - 2)$.
(d) Doe hetzelfde voor $\mathbb{Q}[X]/(X^2 + 3X + 1)$.

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 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. Daarnaast staan we stil bij de kommanotatie voor reële getallen en gaan we in op continuïteit van functies. Tot slot zal na al het werk dat we in de reële getallen zullen stoppen, blijken dat de complexe getallen als een eenvoudig 'toegift' verschijnen. We hebben een groot deel van het voorwerk al in het voorgaande hoofdstuk gedaan!

Er zijn verschillende manieren om reële getallen te introduceren. De meest voor de hand liggende lijkt misschien het gebruik van de decimale notatie: een reëel getal 'is' gewoon een 'getal met oneindig veel cijfers achter de komma'. We zullen in het volgende voorbeeld zien dat er bezwaren aan deze zienswijze kleven.



VI.0.1 Figuur. De introductie van de kommanotatie in *Getal & ruimte* (vwo 2).

VI.0.2 Voorbeeld. In de schoolwiskunde wordt veel gebruikt gemaakt van de decimale kommanotatie — zoals in Figuur VI.0.1.

Sommige getallen kun je in decimale 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:

$$\tfrac{1}{6} = 0{,}166666666666666666666666666666666666666666666666666\ldots$$
$$\pi = 3{,}141592653589793238462643383279502884197169399375105 82\ldots$$

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).

decimale ontwikkeling

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!

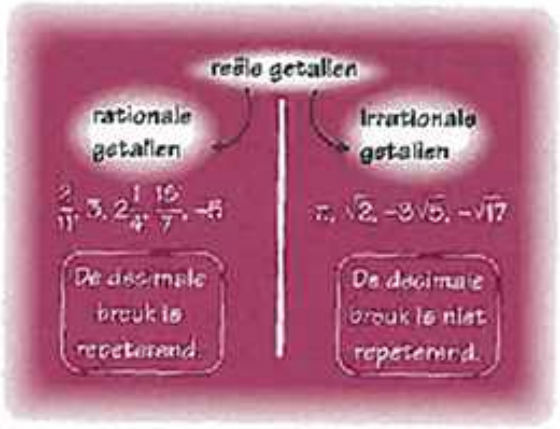
Een ander vervelend technisch detail is dat de decimale ontwikkeling niet altijd uniek is. Zo geldt bijvoorbeeld $1 = 0{,}\overline{9}$, waarbij de streepjesnotatie per definitie staat voor $0{,}99999999\ldots$. Wat zou $1 - 0{,}\overline{9}$ anders moeten zijn dan nul? (Als dit je nog niet overtuigt, bereken dan maar eens $3 \cdot 0{,}\overline{3}$.) 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 *intrinsieke* 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 tot zogenaamde *p-adische getallen* (zie Opgave VI.5.8), dan maakt de basiskeuze wel degelijk uit.) ∎

basis



VI.0.3 Figuur. Verschillende soorten reële getallen, als beschreven in *Getal & ruimte* (vwo 2).

VI.0.4 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. ∎

VI.1 Karakterisering van reële getallen

getallenlijn

We starten met het intuïtieve idee 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:

$$A = \{x \in \mathbb{Q} : x < 0 \text{ of } x^2 \leqslant 2\}.$$

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 $\mathbb{Q}$ hier een 'gat' 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.

bovengrens

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.

supremum

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 $x \leqslant y$;

maximum

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.

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 $A \subseteq \mathbb{Q}$ uit Voorbeeld VI.1.1 is naar boven begrensd (voor de gebruikelijke ordening op $\mathbb{Q}$): 3 is bijvoorbeeld een bovengrens, omdat

$$x < 0 \implies x \leqslant 3 \qquad \text{en} \qquad x^2 \leqslant 2 \implies x \leqslant 3.$$

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.1.3. 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 ook een maximum. ∎

Met behulp van de concepten begrensd en supremum kunnen we de reële getallen karakteriseren. Het bewijs van de existentiestelling die nu volgt, stellen we uit tot Paragraaf VI.5.

existentie van $\mathbb{R}$

VI.1.5 Stelling. Er bestaat een geordend lichaam waarin iedere niet-lege, naar boven begrensde deelverzameling een supremum heeft.

Is R een geordend lichaam, dan zegt Opgave V.1.13 dat er een uniek injectief homomorfisme $\mathbb{Q} \to R$ is. Dit homomorfisme behoudt bovendien de ordening. We zullen in het vervolg $\mathbb{Q}$ simpelweg beschouwen als deelverzameling van R.

Naast existentie zouden we ook graag uniciteit willen bewijzen. Om dit te kunnen doen, leiden we allereerst het volgende resultaat af.

VI.1.6 Stelling. Zij R als in Stelling VI.1.5. Er geldt:

$\mathbb{R}$ is archimedisch

i) R is archimedisch, dat wil zeggen: voor alle $a, b \in R_{>0}$ is er een $n \in \mathbb{N}$ zodat $na > b$ (zie Stelling V.4.3).

$\mathbb{Q}$ is dicht in $\mathbb{R}$

ii) Tussen ieder tweetal $a, b \in R$ met $a < b$ is er een $c \in \mathbb{Q}$ zodat $a < c < b$.

Bewijs. i) Laat $a, b \in R_{>0}$ gegeven zijn en stel dat er geen $n \in \mathbb{N}$ bestaat met $na > b$. Dan geldt dus voor iedere $n \in \mathbb{N}$ dat $n \leqslant \frac{b}{a}$ en dus is $\frac{b}{a}$ een bovengrens van $\mathbb{N}$. Dus is $\mathbb{N}$ naar boven begrensd en omdat $\mathbb{N}$ ook niet leeg is, bestaat er een supremum $s \in \mathbb{R}$. Dat impliceert dat $n \leqslant s$ voor alle $n \in \mathbb{N}$. Hieruit volgt dat ook voor alle $n \in \mathbb{N}$ geldt dat $n \leqslant s - 1$ en dus is s niet de kleinste bovengrens en dus kan s geen supremum zijn. Tegenspraak.

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 $|b| < c < |a|$ 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:

$$\frac{t}{n} \leqslant a + \frac{1}{n} < a + (b - a) = b.$$

∎

uniciteit van $\mathbb{R}$

VI.1.7 Gevolg. Een geordend lichaam waarin iedere niet-lege, naar boven begrensde deelverzameling een supremum heeft, is uniek, op een uniek isomorfisme na.

Bewijs. Stel dat R en S beide aan de voorwaarden voldoen. We beschouwen $\mathbb{Q}$ als een deelverzameling van zowel R als S. Voor $x \in R$ kijken we naar de deelverzameling van $\mathbb{Q}$

$$L_x = \{y \in \mathbb{Q} : y \leqslant x\}.$$

We gebruiken nu drie keer dat $\mathbb{Q}$ dicht ligt in R (Stelling VI.1.6): (i) Merk op dat L_x niet alleen in R, maar zelfs al in $\mathbb{Q}$ naar boven begrensd is: een bovengrens is een

willekeurig rationaal getal tussen x en $x+1$. (ii) Bovendien is L_x niet leeg (neem een rationaal getal tussen x en $x-1$). (iii) Ten slotte geldt $x = \sup_R(L_x)$, waarbij we een R in de notatie gebruiken om aan te geven dat we het supremum in R nemen; x is immers een bovengrens en als x' een kleinere bovengrens zou zijn, dan bestaat er een rationaal getal y met $x' < y < x$ en dat geeft een tegenspraak aangezien $y \in L_x$ en y bovendien groter is dan de 'bovengrens' x'.

Definieer nu een afbeelding $R \to S$ door $x \mapsto \sup_S(L_x)$. In Opgave VI.1.6 wordt bewezen dat dit een uniek isomorfisme tussen R en S is. ■

reële getallen

Stelling VI.1.5 samen met Gevolg VI.1.7 stelt ons in staat te spreken over *hét lichaam van reële getallen* , hetgeen we noteren met $\mathbb{R}$.

Opgaven

S **1.** Definieer, naar analogie met de definitie van supremum, de notie van een *infimum* van een deelverzameling van een geordende verzameling.

S **2.** Bepaal bij de volgende deelverzamelingen V van het gegeven lichaam L steeds of er (i) een bovengrens in L, (ii) een supremum in L en (iii) een maximum in V bestaat.

(a) $L = \mathbb{Q}$ en $V = \{x \in \mathbb{Q} : 0 < x < 1\}$

(b) $L = \mathbb{Q}$ en $V = \{x \in \mathbb{Q} : -2^x < 7\}$

(c) $L = \mathbb{R}$ en $V = \{x \in \mathbb{R} : 2^x < 7\}$

(d) $L = \mathbb{R}$ en $V = \{x \in \mathbb{R} : 2^x \leqslant 7\}$

(e) $L = \mathbb{R}$ en $V = \{x \in \mathbb{R} : \sin(x) < 0\}$

V **3.** Leid in Voorbeeld VI.1.3 uit $y^2 < 2$ een tegenspraak af.

V **4.** Geef een definitie van de wortelfunctie $\sqrt{\ } : \mathbb{R}_{>0} \to \mathbb{R}$ op grond van Stelling VI.1.5.

B **5.** Bewijs dat de verzameling *irrationale getallen* $(\mathbb{R} \setminus \mathbb{Q})$ dicht ligt in $\mathbb{R}$.

B **6.** Maak het bewijs van Gevolg VI.1.7 af. Om een grote hoeveelheid werk te voorkomen, kun je in plaats van te bewijzen dat we met een isomorfisme van lichamen te maken hebben bewijzen dat we een bijectie hebben die de ordening behoudt. (Zodra we weten dat + en · continu zijn, volgt dan vanzelf dat het isomorfisme is.) Twee hints: (i) de inverse $S \to R$ kan ook via de verzameling L_x gedefinieerd worden; (ii) bovendien moet ieder isomorfisme $S \to R$ de suprema van L_x in R en S in elkaar overvoeren.

VI.2 Rijen

rij

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*.

term

index

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 $(1/(2n+1))_{n\geqslant 0}$.

convergent

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

$$\text{voor alle } n \geqslant N: \quad |a_n - a| < \varepsilon.$$

limiet

We noemen a een *limiet* van de rij $(a_n)_{n\geqslant 0}$. Notatie:

$$\lim_{n\to\infty} a_n = a.$$

divergent

Een rij die niet convergent is heet *divergent*.

VI.2.3 Voorbeeld.

(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 $n \geqslant N$:

$$\left|\frac{1}{n} - 0\right| = \frac{1}{n} \leqslant \frac{1}{N} < \varepsilon.$$

(b) Constante rijen zijn convergent, zie Opgave VI.2.3.

(c) De rij $((-1)^n)_{n\geqslant 0}$ 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

$$2 = \left|(1-a) - (-1-a)\right| \leqslant |1-a| + |-1-a| < 1.$$

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. ∎

limiet is uniek

VI.2.4 Opmerking. Een reële rij $(a_n)_{n\geqslant 0}$ kan maximaal één limiet hebben. Stel maar eens dat $\lim_{n\to\infty} a_n = a$ en $\lim_{n\to\infty} a_n = b$ met $a \neq b$. Dan geldt $|a-b| > 0$. We leiden een tegenspraak af. Kies $\varepsilon = \frac{1}{2}|a-b|$. Uit $\lim_{n\to\infty} a_n = a$ volgt dat er een $N_1 \in \mathbb{N}$ bestaat zó dat voor alle $n \geqslant N_1$ geldt $|a_n - a| < \varepsilon$. Uit $\lim_{n\to\infty} a_n = b$ volgt dat er een $N_2 \in \mathbb{N}$ bestaat zó dat voor alle $n \geqslant N_2$ geldt $|a_n - b| < \varepsilon$. Kies een $n \geqslant \max\{N_1, N_2\}$. Dan geldt dat

$$|a-b| = |(a-a_n) + (a_n - b)| \leqslant |a-a_n| + |a_n - b| < \varepsilon + \varepsilon = |a-b|.$$

Ofwel $|a-b| < |a-b|$ en dat is onzin.

begrensd

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 $M \geqslant 0$ 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 Lemma. 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 $M \geqslant 0$ 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

$$|x_n| = \big|x + (x_n - x)\big| \leqslant |x| + |x_n - x| \leqslant |x| + 1 \leqslant M.$$

■

VI.2.7 Voorbeeld. Beschouw de rij $(a_n)_{n\geqslant 0}$ 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 $M \geqslant 0$ 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 $(2n)_{n\geqslant 0}$ divergeert.

divergentie naar ∞

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 $n \geqslant N$: $x_n \geqslant \xi$. *Divergentie naar* $-\infty$ wordt analoog gedefinieerd.

Merk op dat als een $(x_n)_{n\geqslant 0}$ naar ∞ of $-\infty$ divergeert, dat dan in het bijzonder geldt dat $(x_n)_{n\geqslant 0}$ onbegrensd is. Zo'n rij is dus niet convergent wegens Lemma VI.2.6.

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 $n \geqslant 0$. 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 $n \geqslant 0$. 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 $(a_n + b_n)_{n\geqslant 0}$ convergent is met limiet 0. De rij $(a_n + c_n)_{n\geqslant 0}$ is convergent met limiet 1.

(c) Zij $a_n = n$, en $b_n = -n + (-1)^n$ met $n \geqslant 0$. Dan geldt $\lim_{n\to\infty} a_n = \infty$ en $\lim_{n\to\infty} b_n = -\infty$, maar $(a_n + b_n)_{n\geqslant 0}$ is divergent. Immers $a_n + b_n = (-1)^n$.

Blijkbaar kun je dus beter niet rekenen met ∞. ▬

We hebben gezien (Lemma VI.2.6) dat iedere convergente rij begrensd is. We zullen nu een criterium geven waaronder een begrensde rij convergeert.

stijgend
dalend

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 $x_0 \geqslant x_1 \geqslant x_2 \geqslant \cdots$.

Een constante rij is dus zowel dalend als stijgend.

monotone-convergentiestelling

VI.2.11 Stelling (monotoneconvergentiestelling). Zij $(x_n)_{n\geqslant 0}$ 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 Stelling VI.1.5 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

S **1.** Schrijf van elk van de volgende rijen $(a_n)_{n\geqslant 0}$ een paar termen van 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 $n \geqslant N$:

(a) $a_n = \dfrac{1}{2n+1}$;

(b) $a_n = \dfrac{n}{n+1}$;

(c) $a_n = \dfrac{(-1)^n}{n+1}$.

S **2.** Beschouw dezelfde rijen als in de voorafgaande opgave.

(a) Vind voor $\varepsilon \in \{10^{-1}, 10^{-2}, 10^{-3}\}$ een $N \in \mathbb{N}$ zó dat voor alle $n \geqslant N$: $|a_n - a| < \varepsilon$.

✍ (b) Herzie indien nodig je keuze van a, en bewijs dat elke rij naar de gevonden waarde a convergeert.

S **3.** Bewijs dat een constante rij in $\mathbb{R}$ convergent is.

S **4.** 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.

V ✍ **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.

V **6.** (a) Definieer de rij $(a_n)_{n\geqslant 0}$ door $a_n = \frac{1}{\sqrt{n+1}}$. Toon met behulp van de definitie aan dat $\lim\limits_{n\to\infty} a_n = 0$.

(b) Definieer de rij $(a_n)_{n\geqslant 0}$ door $a_n = \sqrt{n}$. Toon met behulp van de definitie aan dat $\lim\limits_{n\to\infty} a_n = \infty$.

V **7.** Toon aan:

(a) voor alle $k \in \mathbb{N}$ met $k \geqslant 1$ geldt $\lim\limits_{n\to\infty} 1/n^k = 0$.

(b) voor alle $n \geqslant 2$ geldt $\lim\limits_{k\to\infty} 1/n^k = 0$.

B **8.** 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 $\lim\limits_{n\to\infty} a_n = \infty$.

V ✍ **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.

V ✍ **10.** Zij $(x_n)_{n\geqslant 0}$ een rij zó dat $(x_{2n})_{n\geqslant 0}$ en $(x_{2n+1})_{n\geqslant 0}$ convergeren naar dezelfde limiet x. Toon aan dat $(x_n)_{n\geqslant 0}$ convergeert en $\lim\limits_{n\to\infty} x_n = x$.

V ✍ **11.** 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 $a < x < b$.

B ✍ **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 $\lim\limits_{n\to\infty} x^n = 0$.

(c) Als $x = 1$ dan $\lim\limits_{n\to\infty} x^n = 1$.

(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.

cijfer

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*.

decimaal

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 $N \in \mathbb{N}$.

decimale ontwikkeling

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 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:

$$
\begin{array}{l|l}
7 & 1{,}0000000\ldots \\
\hline
\quad 30 & 0{,}14285714\ldots \\
\quad 28 & \\
\hline
\quad\ 20 & \\
\quad\ 14 & \\
\hline
\quad\ 60 & \\
\quad\ 56 & \\
\hline
\quad\ 40 & \\
\quad\ 35 & \\
\hline
\quad\ 50 & \\
\quad\ 49 & \\
\hline
\quad\ 10** & \\
\quad\ 7 & \\
\hline
\quad\ 30 & \\
\quad\ 28 & \\
\quad\ \ldots &
\end{array}
$$

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
duivenhokprincipe *duivenhokprincipe*.)

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 $x = \frac{123{,}3}{999} = \frac{1233}{9990}$. ∎

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

S ✍ **1.** Bepaal (zonder rekenmachine) de decimale ontwikkeling van de volgende breuken:
(a) $\frac{3}{11}$
(b) $\frac{3}{13}$
(c) $\frac{313}{495}$
(d) $\frac{15}{3}$

S ✍ **2.** Schrijf de volgende repeterende decimale ontwikkelingen als breuk:
(a) $0{,}4234231 = 0{,}42342310\overline{}$
(b) $0{,}\overline{3211}$
(c) $2{,}12\overline{1}$

V **3.** (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.

B **4.** Geef een formeel bewijs (en dus niet enkel een voorbeeld) van de uitspraak 'Iedere repeterende decimale ontwikkeling definieert een breuk.'

B **5.** (a) Gebruik Stelling VI.3.1 om te laten zien dat alle rijen cijfers $(c_i)_{i \geqslant 1}$ in basis 10, waarin het cijfer 9 niet voorkomt, verschillende reële getallen geven.
(b) Bewijs, met behulp van de Stelling van Cantor (Stelling I.4.11), dat $\mathbb{R}$ overaftelbaar is.

VI.4 Compleetheid

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 definitie een aantal eigenschappen van de intuïtieve notie van afstand extraheren.

metriek

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) $\forall_{a,b,c \in A}\ \mathrm{d}(a,c) \leqslant \mathrm{d}(a,b) + \mathrm{d}(b,c)$.

metrische ruimte

Een verzameling met een metriek noemen we een *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.

omgekeerde driehoeksongelijkheid

VI.4.2 Lemma. Laat (A,d) een metrische ruimte zijn. Dan geldt voor alle a, b en c in A dat:

$$\mathrm{d}(a,b) \geqslant \big|\mathrm{d}(a,c) - \mathrm{d}(b,c)\big|.$$

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 $d : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ 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 enkel 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:

$$\mathrm{d}\big((x_1,y_1),(x_2,y_2)\big) = \sqrt{(x_1-x_2)^2+(y_1-y_2)^2}.$$

euclidische metriek
manhattanmetriek

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. ∎

We kunnen nu algemener definiëren wat convergentie van rijen is.

convergent

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

$$\text{voor alle } n \geqslant N: \quad \mathrm{d}(a_n,a) < \varepsilon.$$

limiet

We noemen a een *limiet* van de rij $(a_n)_{n\geqslant 0}$. Notatie:

$$\lim_{n\to\infty} a_n = a.$$

divergent

Een rij die niet convergent is heet *divergent*.

Net als in Opmerking VI.2.4 volgt dat een rij in een metrische ruimte hoogstens één limiet kan hebben: zie Opgave VI.4.3.

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.

cauchy-rij

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:

$$\text{voor alle } m,n \geqslant N: \quad \mathrm{d}(x_n,x_m) < \varepsilon.$$

VI.4.8 Voorbeeld. We geven twee voorbeelden voor reële rijen.

(a) De rij $(1/(n+1))_{n\geqslant 0}$ 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 $((-1)^n)_{n\geqslant 0}$ 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. ∎

Het omgekeerde van Stelling VI.4.9 is niet altijd waar.

compleet

VI.4.10 Definitie. Zij A een verzameling met een metriek d. De metrische ruimte (A,d) is *compleet* als iedere cauchy-rij convergeert.

$\mathbb{R}$ is compleet

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

$$(g-\varepsilon, g+\varepsilon).$$

Immers, aangezien $(x_n)_{n\geqslant 0}$ cauchy is, bestaat er een $N \in \mathbb{N}$ zodat $|x_m - x_n| < \varepsilon$ voor alle $n,m \geqslant N$; nemen we nu $g = x_N$, dan volgt $|g - x| < \varepsilon$ 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 Voorbeeld.

- $\mathbb{Q}$ 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. ∎

$\mathbb{R}^k$ is compleet

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 cauchy-rij is er een $N \in \mathbb{N}$ zodat voor alle $n, m \geqslant N$:

$$\mathrm{d}(x_n, x_m) = \sqrt{\sum_{i=1}^{k} (x_{n,i} - x_{m,i})^2} < \varepsilon.$$

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 $n \geqslant \max(N_1, N_2, \ldots, N_k)$:

$$\mathrm{d}(x_n, p)^2 = \sum_{i=1}^{k} (x_{n,i} - p_i)^2 < \sum_{i=1}^{k} \left(\frac{\varepsilon}{\sqrt{k}} \right)^2 = \varepsilon^2$$

en dus $\mathrm{d}(x_n, p) < \varepsilon$. ∎

Opgaven

S **1.** Bewijs het eerste deel van Stelling VI.4.3.

V **2.** Bekijk Voorbeeld VI.4.5.

(a) Bewijs dat de 'manhattanmetriek' inderdaad een metriek is op $\mathbb{R}^2$.

(b) Bewijs dat de 'euclidische metriek' inderdaad een metriek is op $\mathbb{R}^2$.

(c) Doe hetzelfde voor $\mathbb{R}^m$ met $m > 2$.

V **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.

V ✍ **4.** Bewijs Stelling VI.4.9.

V **5.** Bewijs dat $\mathbb{R}^m$ (met $m \geqslant 1$) 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.

VI.5 Completeren

Hoewel iedere convergente rij een cauchy-rij is, hebben we in de vorige paragraaf gezien dat het omgekeerde niet geldt. We zullen in deze paragraaf een constructie uitwerken om een metrische ruimte compleet te maken, zodat de omkering wél geldt. Dit noemen we *completeren*. Als toegift zullen we aan het einde van de paragraaf een methode beschrijven om $\mathbb{R}$ te construeren vanuit $\mathbb{Q}$ en zo dus Stelling VI.1.5 bewijzen.

completeren

Zij (A,d) een metrische ruimte. Noteer met C_A de verzameling cauchy-rijen in A. Definieer een relatie op C_A als volgt:

$$(a_n)_{n\geqslant 0} \sim (b_n)_{n\geqslant 0} \qquad \Longleftrightarrow \qquad \lim_{n\to\infty} \mathrm{d}(a_n,b_n) = 0.$$

Merk op dat de limiet genomen wordt van een *reële* rij: de $\mathrm{d}(a_n,b_n)$ zijn reële getallen. We willen twee rijen equivalent noemen als ze dezelfde limiet hebben in de competering van A, maar die zijn we nu juist aan het maken. Gelukkig kunnen we de gewenste equivalentie toch met deze bonafide limiet definiëren. In Opgave VI.5.1 wordt bewezen dat $\sim$ een equivalentierelatie is. Noteer nu met $\widehat{A}$ de verzameling equivalentieklassen van C_A onder deze equivalentierelatie.

Door een element $a \in A$ af te beelden op de constante rij waarvan iedere term gelijk is aan a en hier vervolgens de equivalentieklasse van te nemen, krijgen we een afbeelding $A \to \widehat{A}$. Deze afbeelding is injectief (Opgave VI.5.2) en we noemen hem de *kanonieke inbedding*.

VI.5.1 Lemma. Er is een unieke metriek $\widehat{\mathrm{d}}$ op $\widehat{A}$ die een voortzetting is van de metriek op A en waarvoor geldt dat voor alle cauchy-rijen $(a_n)_{n\geqslant 0}$ en $(b_n)_{n\geqslant 0}$ in A:

$$\widehat{\mathrm{d}}\big([(a_n)_{n\geqslant 0}],[(b_n)_{n\geqslant 0}]\big) = \lim_{n\to\infty} \mathrm{d}(a_n,b_n).$$

geïnduceerde metriek
completering

We noemen deze metriek op $\widehat{A}$ de *geïnduceerde metriek*. De metrische ruimte $\widehat{A}$ noemen we de *completering* van A, om een reden die in de volgende stelling wordt verklaard.

Bewijs. Zij $a,b \in \widehat{A}$. Laat $(a_n)_{n\geqslant 0}$ en $(b_n)_{n\geqslant 0}$ twee cauchy-rijen zijn in A waarvan de equivalentieklassen gelijk zijn aan a respectievelijk b. Bekijk de reële rij $(l_n)_{n\geqslant 0}$ gedefinieerd door $l_n = \mathrm{d}(a_n,b_n)$. We bewijzen dat dit een cauchy-rij is. Laat daartoe $\varepsilon > 0$ gegeven zijn. Er bestaat een $N \in \mathbb{N}$ zodat voor alle $r,s \geqslant N$ geldt

$$\mathrm{d}(a_r,a_s) < \frac{1}{2}\varepsilon \qquad \text{en} \qquad \mathrm{d}(b_r,b_s) < \frac{1}{2}\varepsilon.$$

Laat nu $r \geqslant N$ en $s \geqslant N$. Dan geldt:

$$l_r = \mathrm{d}(a_r,b_r) \leqslant \mathrm{d}(a_r,a_s) + \mathrm{d}(a_s,b_s) + d(b_s,b_r) < \varepsilon/2 + l_s + \varepsilon/2 = l_s + \varepsilon\,.$$

Net zo geldt dat $l_s < l_r + \varepsilon$, en dus:

$$l_s - \varepsilon < l_r < l_s + \varepsilon\,.$$

Dus geldt dat $|l_r - l_s| < \varepsilon$, en we hebben bewezen dat de rij $(l_n)_{n\geqslant 0}$ een cauchy-rij is.

Laat nu l de limiet zijn van de rij $(l_n)_{n\geqslant 0}$, die bestaat omdat $\mathbb{R}$ compleet is (Stelling VI.4.11). In Opgave VI.5.5 wordt aangetoond dat l niet afhangt van de keuze van representanten en dat $\widehat{\mathrm{d}}(a,b) = l$ daarmee een metriek op $\widehat{A}$ definieert die de metriek op A voortzet. ∎

VI.5.2 Stelling. De verzameling $\widehat{A}$ met de geïnduceerde metriek is compleet.

Bewijs. Zij $(\widehat{a_n})_{n\geqslant 0}$ een cauchy-rij in $\widehat{A}$. (Dit is een vrij abstract object: een rij waarvan de termen equivalentieklassen van rijen zijn; een soort 'rij van rijen' dus. Om verwarring te reduceren, noteren we in dit bewijs elementen van $\widehat{A}$ daarom met een hoedje erboven.) We zullen een element $\widehat{a} \in \widehat{A}$ beschrijven waar $(\widehat{a_n})_{n\geqslant 0}$ naar convergeert.

Kies voor iedere n een cauchy-rij $(a_{n,m})_{m\geqslant 0}$ in A die $\widehat{a_n}$ representeert. Door eventueel over te gaan op deelrijen, mogen we aannemen dat voor alle $r,s \geqslant n$ geldt

$$\mathrm{d}(a_{n,r}, a_{n,s}) < \frac{1}{n+1}.$$

De rij $(a_{n,n})_{n\geqslant 0}$ is een cauchy-rij. Om dat in te zien, veronderstellen we $\varepsilon > 0$ gegeven. Omdat $(\widehat{a_n})_{n\geqslant 0}$ een cauchy-rij is, bestaat er een $M \in \mathbb{N}$ zodat voor alle $r,s \geqslant M$ geldt dat

$$\widehat{\mathrm{d}}(\widehat{a_r}, \widehat{a_s}) < \frac{1}{4}\varepsilon.$$

Dat betekent per definitie dat

$$\lim_{u\to\infty} \mathrm{d}(a_{r,u}, a_{s,u}) < \frac{1}{4}\varepsilon.$$

In het bijzonder bestaat er een $U_{r,s} \in \mathbb{N}$ zodat voor alle $u \geqslant U_{r,s}$ geldt

$$\mathrm{d}(a_{r,u}, a_{s,u}) < \frac{1}{3}\varepsilon.$$

Kies nu N zodat $\frac{1}{N+1} < \frac{1}{3}\varepsilon$ en $N \geqslant M$. Zij $r,s \geqslant N$. Kies een $u \in \mathbb{N}$ zo dat u groter is dan $U_{r,s}$, r en s. Dan zien we door twee keer de driehoeksongelijkheid toe te passen dat

$$\mathrm{d}(a_{r,r}, a_{s,s}) \leqslant \mathrm{d}(a_{r,r}, a_{r,u}) + \mathrm{d}(a_{r,u}, a_{s,u}) + \mathrm{d}(a_{s,u}, a_{s,s}) < \varepsilon.$$

We concluderen dat de rij $(a_{n,n})_{n\geqslant 0}$ inderdaad cauchy is.

Laat $\widehat{a}$ nu de equivalentieklasse van $(a_{n,n})_{n\geqslant 0}$ zijn in $\widehat{A}$. Zij $\varepsilon > 0$ gegeven. Omdat $(a_{n,n})_{n\geqslant 0}$ een cauchy-rij is, bestaat er een $M \in \mathbb{N}$ zodat voor alle $n,u \geqslant M$ geldt $\mathrm{d}(a_{n,n}, a_{u,u}) < \frac{1}{2}\varepsilon$. Kies nu $N \in \mathbb{N}$ zo dat $N \geqslant M$ en $\frac{1}{N+1} < \frac{1}{2}\varepsilon$. Dan geldt voor $n \geqslant N$

$$\widehat{\mathrm{d}}(\widehat{a_n}, \widehat{a}) = \lim_{u\to\infty} \mathrm{d}(a_{n,u}, a_{u,u}) \leqslant \lim_{u\to\infty} \mathrm{d}(a_{n,u}, a_{n,n}) + \lim_{u\to\infty} \mathrm{d}(a_{n,n}, a_{u,u}) \leqslant \frac{1}{n+1} + \frac{1}{2}\varepsilon < \varepsilon.$$

Dus is $\widehat{a}$ de limiet van $(\widehat{a_n})_{n\geqslant 0}$. ∎

constructie van $\mathbb{R}$

Voorgaande geeft een idee om $\mathbb{R}$ te construeren op basis van $\mathbb{Q}$: neem gewoon de completering van $\mathbb{Q}$. Er zit echter een addertje onder het gras: in de Definitie VI.4.1 van metriek worden de reële getallen gebruikt en hetzelfde geldt voor de definitie van limiet en cauchy-rij en Lemma VI.5.1 en Stelling VI.5.2. Maar dat

mag natuurlijk niet als we de reële getallen proberen te definiëren — anders krijg je een cirkelredenering!

De oplossing is gelukkig simpel: vervang in voornoemde definities $\mathbb{R}$ door $\mathbb{Q}$ en werk dit consequent door. Op die manier kan, zonder reële getallen te gebruiken, betekenis worden gegeven aan $\widehat{\mathbb{Q}}$ en kunnen we vervolgens $\mathbb{R}$ *definiëren* als $\widehat{\mathbb{Q}}$. Dat programma gaan we nu uitvoeren.

Bewijs (van Stelling VI.1.5). We delen het bewijs op in een aantal stappen.

STAP 1. We geven eerst de constructie van $\mathbb{R}$, zoals hierboven al globaal is beschreven. Daartoe herdefiniëren we een aantal begrippen voor de context van dit bewijs. Onder *rij* zullen we altijd een rij in $\mathbb{Q}$ verstaan. Een *cauchy-rij* is een rij $(a_n)_{n\geqslant 0}$ met de eigenschap dat voor iedere $\varepsilon \in \mathbb{Q}_{>0}$ er een $N \in \mathbb{N}$ is zodat voor alle $m,n \geqslant N$ geldt $|a_n - a_m| < \varepsilon$. (Vergelijk dit met Definitie VI.4.7.) Definieer een equivalentierelatie voor rijen door $(a_n)_{n\geqslant 0} \sim (b_n)_{n\geqslant 0}$ als er voor iedere $\varepsilon \in \mathbb{Q}_{>0}$ een $N \in \mathbb{N}$ is zodat voor alle $n \geqslant N$ geldt $|a_n - b_n| < \varepsilon$. Noteer met $\mathbb{R}$ de verzameling equivalentieklassen onder deze equivalentierelatie. We identificeren het element $a \in \mathbb{Q}$ met het element van $\mathbb{R}$ dat de equivalentieklasse is van de constante rij waarvan iedere term gelijk is aan a.

STAP 2. Nu breiden we de lichaamsstructuur van $\mathbb{Q}$ uit naar $\mathbb{R}$. Dat is niet moeilijk. We geven als voorbeeld de definitie van optelling en verwijzen voor alle overige details naar Opgave VI.5.6. Zij $a,b \in \mathbb{R}$ en kies twee cauchy-rijen $(a_n)_{n\geqslant 0}$ en $(b_n)_{n\geqslant 0}$ die representanten zijn van a respectievelijk b. Dan wordt de *som* $a+b$ per definitie gerepresenteerd door de rij $(a_n + b_n)_{n\geqslant 0}$.

STAP 3. Het uitbreiden van ordening van $\mathbb{Q}$ naar $\mathbb{R}$ is iets ingewikkelder. We kiezen ervoor om $<$ te definiëren omdat die in dit bewijs van belang is. Per definitie is $a < b$ (met $a,b \in \mathbb{R}$ en $(a_n)_{n\geqslant 0}$ en $(b_n)_{n\geqslant 0}$ representanten) als er een $\delta \in \mathbb{Q}_{>0}$ is en een $N \in \mathbb{N}$ is zodat voor alle $n \geqslant N$ geldt $(b_n - a_n) \geqslant \delta$. In Opgave VI.5.6 bewijs je dat dit niet afhangt van de keuze van representanten, dat het inderdaad een lineaire ordening is die de ordening van $\mathbb{Q}$ uitbreidt en dat dit $\mathbb{R}$ de structuur van een geordend lichaam geeft.

Hiermee hebben we de gevraagde structuur gedefinieerd. In de rest van het bewijs gaan we aantonen dat $\mathbb{R}$ aan de eigenschap voldoet dat iedere niet-lege, naar boven begrensde deelverzameling een supremum heeft. Daarvoor bewijzen we eerst een hulpresultaat.

STAP 4. We laten zien dat $\mathbb{Q}$ dicht ligt in $\mathbb{R}$. Neem weer net als hiervoor $a,b \in \mathbb{R}$ met representanten $(a_n)_{n\geqslant 0}$ en $(b_n)_{n\geqslant 0}$. Bovendien veronderstellen we dat $a < b$. Dat betekent dus dat er een $\delta \in \mathbb{Q}_{>0}$ en een $N_1 \in \mathbb{N}$ zijn zodat voor alle $n \geqslant N_1$ geldt $b_n - a_n \geqslant \delta$. Kies zo'n δ en zo'n N_1.

De cauchy-eigenschap geeft ons een $N_2 \in \mathbb{N}$ zodat voor alle $r,s \geqslant N_2$

$$|a_r - a_s| < \frac{1}{3}\delta \qquad \text{en} \qquad |b_r - b_s| < \frac{1}{3}\delta.$$

Definieer

$$c = \frac{1}{2}(a_{N_2} + b_{N_2})$$

en laat N het maximum van N_1 en N_2 zijn. Nu geldt voor alle $s \geqslant N$ dat

$$c - a_s = (c - a_N) + (a_N - a_s) > \frac{1}{6}\delta;$$

deze conclusie is gerechtvaardigd omdat de eerste sommand minimaal $\frac{1}{2}\delta$ is, terwijl de tweede sommand weliswaar negatief zou kunnen zijn, maar kleiner dan $\frac{1}{3}\delta$ is. Hieruit volgt $a < c$ (waar we c identificeren met de constante cauchy-rij met iedere term gelijk aan c). Op dezelfde manier volgt $c < b$. Dus ligt $\mathbb{Q}$ dicht in $\mathbb{R}$.

STAP 5. Neem nu een niet-lege deelverzameling $A \subseteq \mathbb{R}$ die van boven begrensd is. Laat $r' \in \mathbb{R}$ een bovengrens zijn en kies ook een element $l' \in A$. Gebruik nu

Stap 4 om elementen $l_0, r_0 \in \mathbb{Q}$ te vinden met $l'-1 \leqslant l_0 \leqslant l'$ en $r' \leqslant r_0 \leqslant r'+1$. Merk op dat r_0 nog steeds een bovengrens is en dat $l_0 \leqslant r_0$. Het idee is nu om twee rijen $(l_n)_{n\geqslant 0}$ en $(r_n)_{n\geqslant 0}$ te definiëren die het gezochte supremum gaan inklemmen — de een convergeert vanaf links en de andere vanaf rechts ernaartoe. Voor de definitie gebruiken we de notatie $m(x,y) = \frac{1}{2}(x+y)$ voor het midden van $x, y \in \mathbb{Q}$. Definieer de rijen nu met recursie:

$$l_{n+1} = \begin{cases} l_n & \text{als } m(l_n, r_n) \text{ een bovengrens is,} \\ m(l_n, r_n) & \text{anders;} \end{cases}$$

en

$$r_{n+1} = \begin{cases} m(l_n, r_n) & \text{als } m(l_n, r_n) \text{ een bovengrens is,} \\ r_n & \text{anders.} \end{cases}$$

Noteer $C = |r_0 - l_0|$. Voor deze rijen gelden de volgende eigenschappen (zie Opgave VI.5.6):

- $l_0 \leqslant l_1 \leqslant \cdots \leqslant l_n \leqslant \cdots \leqslant r_n \leqslant \cdots \leqslant r_1 \leqslant r_0$;
- voor alle $n \in \mathbb{N}$ geldt $|l_{n+1} - l_n| \leqslant \frac{1}{2^{n+1}} C$ en $|r_{n+1} - r_n| \leqslant \frac{1}{2^{n+1}} C$;
- voor alle $n \in \mathbb{N}$ geldt $|l_n - r_n| \leqslant \frac{1}{2^n} C$;
- voor alle $n \in \mathbb{N}$ geldt dat l_n géén bovengrens van A is, terwijl r_n dat wél is.

Zij nu $\varepsilon \in \mathbb{Q}_{>0}$ gegeven. Kies N zo, dat $\frac{1}{2^N} C < \varepsilon$. Neem $n > m \geqslant N$. Dan geldt

$$\begin{aligned} |r_n - r_m| &= |r_n - r_{n-1} + r_{n-1} - r_{n-2} + \cdots + r_{m+1} - r_m| \\ &\leqslant |r_n - r_{n-1}| + |r_{n-1} - r_{n-2}| + \cdots + |r_{m+1} - r_m| \\ &\leqslant \frac{1}{2^n} C + \frac{1}{2^{n-1}} C + \cdots + \frac{1}{2^{m+1}} C < \varepsilon. \end{aligned}$$

Hiermee is aangetoond dat $(r_n)_{n\geqslant 0}$ een cauchy-rij is. Noteer de equivalentieklasse met r.

STAP 6. Nu bewijzen we dat r een bovengrens is van A. Stel dat dit niet zo is. Dan is er een $a \in A$ zodat $r < a$. Zij $(a_n)_{n\geqslant 0}$ een representant van a. Dan zijn er $\varepsilon \in \mathbb{Q}_{>0}$ en $N_1 \in \mathbb{N}$ zodat voor alle $n \geqslant N_1$ geldt

$$a_n - r_n > \varepsilon.$$

Vanwege de cauchy-eigenschap is er een $N_2 \in \mathbb{N}$ zodat voor alle $r, s \geqslant N_2$

$$|a_r - a_s| < \frac{1}{2}\varepsilon.$$

Zij N nu het maximum van N_1 en N_2 en zij $n \geqslant N$. Dan geldt

$$a_n - r_N > \frac{1}{2}\varepsilon$$

en dus is r_N geen bovengrens van A; tegenspraak.

STAP 7. Tot slot bewijzen we dat r de kleinste bovengrens is. Stel dat $t \in \mathbb{R}$ een kleinere bovengrens is en kies een representant $(t_n)_{n\geqslant 0}$. Dan is er een $\delta \in \mathbb{Q}_{>0}$ en een $N \in \mathbb{N}$ zodat voor alle $n \geqslant N$ dat $|r_n - t_n| \geqslant \delta$. Maar er is ook een $M \in \mathbb{N}$ zodat voor alle $n \geqslant M$ geldt $0 \leqslant r_n - l_M < \frac{1}{2}\delta$. Bijgevolg geldt voor $n \geqslant \max(N, M)$ dat $l_M - t_n = (l_M - r_n) + (r_n - t_n) > \frac{1}{2}\delta$ en dus geldt $l_M > t$. Maar dat betekent dat l_M een bovengrens is en dat is een tegenspraak. ∎

Opgaven

V **1.** Bewijs dat de relatie op C_A die aan het begin van deze paragraaf wordt gedefinieerd een equivalentierelatie is.

V **2.** Bewijs dat de afbeelding $A \to \widehat{A}$ die aan het begin van deze paragraaf wordt gedefinieerd injectief is. Wanneer is de afbeelding ook surjectief?

S **3.** Zij A een niet-lege verzameling. Definieer een metriek op A door $\mathrm{d}(x,x) = 0$ en $\mathrm{d}(x,y) = 1$ als $x \neq y$. Beschrijf $\widehat{A}$.

V **4.** Beschouw $\mathbb{Q}^n$ met de euclidische metriek ("Pythagoras in n dimensies"). Bewijs dat de completering van $\mathbb{Q}^n$ gelijk is aan (of preciezer: kanoniek isomorf met) $\mathbb{R}^n$.

V **5.** Deze opgave betreft het bewijs van Lemma VI.5.1, en vormt een deel daarvan. Er is al bewezen dat voor $(a_n)_{n\geqslant 0}$ en $(b_n)_{n\geqslant 0}$ in C_A de rij $(\mathrm{d}(a_n,b_n))_{n\geqslant 0}$ een cauchy-rij in $\mathbb{R}$ is, en dus een limiet heeft. We definiëren de functie $\mathrm{d}\colon C_A \times C_A \to \mathbb{R}$ door $\mathrm{d}((a_n)_{n\geqslant 0},(b_n)_{n\geqslant 0}) = \lim_{n\to\infty} d(a_n,b_n)$.

(a) Laat $(a_n)_{n\geqslant 0}$, $(a'_n)_{n\geqslant 0}$, $(b_n)_{n\geqslant 0}$ en $(b'_n)_{n\geqslant 0}$ elementen van C_A zijn, en neem aan dat $(a'_n)_{n\geqslant 0} \sim (a_n)_{n\geqslant 0}$ en $(b'_n)_{n\geqslant 0} \sim (b_n)_{n\geqslant 0}$. Bewijs dat

$$\mathrm{d}((a'_n)_{n\geqslant 0},(b'_n)_{n\geqslant 0}) = \mathrm{d}((a_n)_{n\geqslant 0},(b_n)_{n\geqslant 0}).$$

(b) Bewijs dat voor alle $(a_n)_{n\geqslant 0}$ en $(b_n)_{n\geqslant 0}$ in C_A geldt dat

$$\mathrm{d}((a_n)_{n\geqslant 0},(b_n)_{n\geqslant 0}) = \mathrm{d}((b_n)_{n\geqslant 0},(a_n)_{n\geqslant 0}).$$

(c) Bewijs dat voor alle $(a_n)_{n\geqslant 0}$, $(b_n)_{n\geqslant 0}$ en $(c_n)_{n\geqslant 0}$ in C_A geldt dat

$$\mathrm{d}((a_n)_{n\geqslant 0},(c_n)_{n\geqslant 0}) \leqslant \mathrm{d}((a_n)_{n\geqslant 0},(b_n)_{n\geqslant 0}) + \mathrm{d}((b_n)_{n\geqslant 0},(c_n)_{n\geqslant 0}).$$

B (d) Bewijs dat d een metriek op $\widehat{A}$ induceert.

(e) Laat zien dat deze metriek de metriek op A voortzet, door te kijken wat er met constante rijen gebeurt.

V **6.** Maak het bewijs van Stelling VI.1.5 compleet.

S **7.** Beschrijf in tien regels hoe cauchy-rijen gebruikt kunnen worden om $\mathbb{R}$ uit $\mathbb{Q}$ te construeren.

B **8.** Zij p een priemgetal. Voor ieder getal $x \in \mathbb{Q}$ met $x \neq 0$ is er een unieke $r \in \mathbb{Z}$ zodat $x = p^r \frac{t}{n}$, waarbij $t,n \in \mathbb{Z}\setminus\{0\}$ beide niet deelbaar door p zijn. Definieer de *p-adische absolute waarde* door $|x|_p = p^{-r}$ en $|0|_p = 0$.

(a) Toon aan dat $\mathrm{d}(x,y) = |x-y|_p$ een metriek definieert op $\mathbb{Q}$.

(b) Beschrijf aan de hand van concrete voorbeelden wat het betekent dat twee getallen dicht bij elkaar liggen in de p-adische metriek.

(c) Geef een cauchy-rij $(x_n)_{n\geqslant 0}$ die niet convergeert in $\mathbb{Q}$ met de p-adische metriek.

(d) Probeer, naar analogie met de notatie van decimale ontwikkeling in $\mathbb{R}$, een concrete beschrijving te geven van de completering van $\mathbb{Q}$ voor de p-adische metriek.

✯ **9.** (Deze opgave is makkelijker nadat je Paragraaf VI.7 hebt bestudeerd.) In het wiskundige deelgebied van de *functionaalanalyse* wordt veel gebruik gemaakt van verzamelingen van functies en hun completeringen. Heel het formalisme van de quantummechanica is hier bijvoorbeeld op gebaseerd. We geven hier een klein voorbeeld om een beeld te geven.
Bekijk de verzameling $C([0,1])$ van continue functies $[0,1] \to \mathbb{R}$. Voor zo'n functie f noteren we

$$\|f\| = \sup\{|f(x)| : x \in [0,1]\}.$$

Dit leidt tot een metriek op $C([0,1])$ gegeven door

$$\mathrm{d}(f,g) = \|f - g\|.$$

(a) Toon aan dat dit inderdaad een metriek is op $C([0,1])$.

(b) Bewijs dat $C([0,1])$ compleet is.

Definieer nu een rij $(f_n)_{n\geqslant 0}$ in $C([0,1])$ door $f_n(x) = x^n$.

(c) Bewijs dat $(f_n)_{n\geqslant 0}$ geen limiet in $C([0,1])$ heeft.

(d) Laat zien dat $(f_n)_{n\geqslant 0}$ wel *puntsgewijs* convergeert naar de (niet continue) functie $g\colon [0,1] \to \mathbb{R}$ gegeven door $g(1) = 1$ en $g(x) = 0$ voor $x \neq 1$. Dat betekent dat je moet bewijzen dat voor alle $x \in [0,1]$ geldt dat $\lim_{n\to\infty} f_n(x) = g(x)$.

VI.6 Compact en gesloten

In deze paragraaf bestuderen we zogenaamde *topologische* eigenschappen van metrische ruimtes.

deelrij

Laat $(a_n)_{n\geqslant 0}$ en $(a'_n)_{n\geqslant 0}$ rijen zijn in een verzameling A. Per definitie zijn dit afbeeldingen $a, a'\colon \mathbb{N} \to A$. We noemen $(a'_n)_{n\geqslant 0}$ een *deelrij* van $(a_n)_{n\geqslant 0}$ als $a' = a \circ r$ voor een functie $r\colon \mathbb{N} \to \mathbb{N}$ 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, ...

rijcompact

VI.6.1 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 $\mathrm{d}\colon V \times V \to \mathbb{R}$ 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 in W een deelrij heeft die convergeert naar een element *dat bevat is in* W. Dit motiveert de volgende definitie.

gesloten

VI.6.2 Definitie. Zij (A,d) een metrische ruimte. Een deelverzameling $Z \subseteq A$ heet *gesloten* als voor iedere convergente rij $(a_m)_{m\geqslant 0}$ in A met limiet $a \in A$ geldt:

$$\big(\forall_{m\in\mathbb{N}}\ a_m \in Z\big) \quad\Longrightarrow\quad a \in Z.$$

open

Een deelverzameling $U \subseteq A$ heet *open* als $A \setminus U$ 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.

Ons 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.6.3 Definitie. Zij (A, d) een metrische ruimte. De *bol in A met middelpunt $x \in A$ en straal $\varepsilon > 0$* is de deelverzameling

$$B_{x,\varepsilon} = \{y \in A : \mathrm{d}(y,x) < \epsilon\}.$$

bolomgeving

De bol $B_{x,\varepsilon}$ wordt ook een *bolomgeving* van x genoemd.

VI.6.4 Stelling. Een deelverzameling $U \subseteq A$ is open precies dan als iedere $x \in U$ een bolomgeving B heeft zodat $B \subseteq U$.

In Opgave VI.6.3 zul je uit deze stelling afleiden dat de 'open' intervallen $(-\infty, b)$, (a,b) en (a,∞) in $\mathbb{R}$ inderdaad open zijn volgens onze definitie; en dat analoog de intervallen $(-\infty, b]$, $[a,b]$ en $[a,\infty)$ gesloten zijn.

Bewijs. Zij $U \subseteq A$ en noteer $Z = A \setminus U$.

'$\Rightarrow$': 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 $m \in \mathbb{Z}$ een element $x_m \in B_{x,\frac{1}{m+1}} \cap Z$. Dit definieert een rij $(x_m)_{m \geqslant 0}$ 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 $B_{x,\varepsilon} \subseteq U$. Laat $(a_m)_{m \geqslant 0}$ een rij zijn in Z die in A convergeert naar $a \in A$. We zullen laten zien dat $a \in Z$; daarmee is dan aangetoond dat Z gesloten is en U dus open.

Stel $a \notin Z$. Dan $a \in U$. 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 $\mathrm{d}(a_m, a) < \varepsilon$ voor alle $m \geqslant N$. 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.

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.6.7. We beginnen met een elementair lemma.

VI.6.5 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 van lengte kleiner dan $\varepsilon/\sqrt{n}$ (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.6.5. ∎

stelling van Bolzano–Weierstrass

VI.6.6 Stelling (Bolzano–Weierstrass). Iedere begrensde rij in $\mathbb{R}^n$ heeft een convergente deelrij.

Bewijs. Zij $(a_m)_{m\geqslant 0}$ zo'n begrensde rij. We zullen een rij deelverzamelingen

$$\cdots \subset I_{m+1} \subset I_m \subset \cdots \subset I_2 \subset I_1 \subset I_0 = \mathbb{N}$$

definiëren waarbij voor iedere $m \geqslant 1$ geldt:

i) I_m bestaat uit oneindig veel elementen;
ii) het kleinste element van I_{m+1} (dat bestaat volgens welordening) is niet het kleinste element van I_m;
iii) voor alle $m > 0$ en alle $i, j \in I_m$ geldt $\mathrm{d}(a_i, a_j) < \frac{1}{m}$.

Daartoe gebruiken we recursie. We weten al $I_0 = \mathbb{N}$. Stel nu dat I_m gedefinieerd is voor een bepaald $m \in \mathbb{N}$. Herinner je dat de rij in feite een afbeelding $a : \mathbb{N} \to \mathbb{R}^n$ is. Volgens Lemma VI.6.5 kan het beeld $a(I_m)$ overdekt worden met eindig veel deelverzamelingen $V_1, V_2, \ldots, V_r$ waarvan de elementen afstand kleiner dan $\frac{1}{m+1}$ hebben. Dan geldt

$$I_m \subset a^{-1}(V_1) \cup a^{-1}(V_2) \cup \cdots \cup a^{-1}(V_r)$$

en omdat I_m oneindig veel elementen heeft, moet er een index i zijn zodat ook $J = I_m \cap a^{-1}(V_i)$ oneindig is. Laat nu I_{m+1} gelijk zijn aan J met daaruit weggelaten het kleinste element van I_m. Hiermee is de rij deelverzamelingen gedefinieerd.

Definieer nu $r : \mathbb{N} \to \mathbb{N}$ door $r(m) = \min I_m$ en bekijk de rij $a \circ r$ — anders gezegd, de rij $(a_{r(m)})_{m\geqslant 0}$. 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.6.7 Gevolg. Een deelverzameling $Z \subset \mathbb{R}^n$ is rijcompact precies dan als Z begrensd en gesloten is.

Bewijs. '⇒': Stel Z is rijcompact. Zij $(a_m)_{m\geqslant 0}$ een convergente rij in $\mathbb{R}^n$ zodat $a_m \in Z$ voor alle $m \in \mathbb{N}$; zij $a \in \mathbb{R}^n$ de limiet. Iedere deelrij van $(a_m)_{m\geqslant 0}$ 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 $(a_m)_{m\geqslant 0}$ in Z. Laat $a_0 \in Z$ willekeurig (omdat Z niet begrensd is, is het in het bijzonder niet leeg). Kies $a_m \in Z$ voor $m \geqslant 1$ zo, dat $\mathrm{d}(a_0, a_m) > m$; zo'n element bestaat, omdat anders voor alle $z, y \in Z$ zou gelden

$$\mathrm{d}(z, y) \leqslant \mathrm{d}(x, a_0) + \mathrm{d}(a_0, y) \leqslant 2m$$

en dat is in tegenspraak met onbegrensdheid. Volgens rijcompactheid is er een deelrij $(a_{r(m)})_{m\geqslant 0}$ die convergent is en dus (Stelling VI.4.9) cauchy. Voor ieder $\varepsilon > 0$ is er dus een $N \in \mathbb{N}$ zodat $\mathrm{d}(a_{r(N)}, a_{r(k)}) < \varepsilon$) voor alle $k > N$. Maar dan geldt voor al deze k:

$$\mathrm{d}(a_0, a_{r(k)}) \leqslant \mathrm{d}(a_0, a_{r(N)}) + \mathrm{d}(a_{r(N)}, a_{r(k)}) < \mathrm{d}(a_0, a_{r(N)}) + \varepsilon.$$

Het rechterlid van deze ongelijkheid is constant, terwijl het linkerlid variabel is en groter is dan $r(k)$; tegenspraak.

'⇐': Stel Z is begrensd en gesloten. Zij $(a_m)_{m\geqslant 0}$ een rij in Z. Dan is $(a_m)_{m\geqslant 0}$ een begrensde rij en dus geldt volgens Stelling VI.6.6 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

S **1.** Bewijs: Iedere bol in $\mathbb{R}^n$ is open.

S **2.** 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.

S **3.** Bewijs dat voor alle $a, b \in \mathbb{R}$ geldt:

(a) de intervallen $(-\infty, b]$, $[a, b]$ en $[a, \infty)$ zijn gesloten;

(b) de intervallen $(-\infty, b)$, (a, b) en (a, ∞) zijn open.

[Hint: gebruik Stelling VI.6.4.]

V **4.** 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.

V **5.** Bewijs Lemma VI.6.5.

VI.7 Limieten en continuïteit van functies

We beperken ons tot functies van een deelverzameling van $\mathbb{R}^m$ naar $\mathbb{R}^n$. 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.7.1 Definitie.** Zij $V \subseteq \mathbb{R}^m$ en zij $f : V \to \mathbb{R}^n$ een functie. De functie f is *continu in een punt* $a \in V$ als er voor iedere bolomgeving B van $f(a)$ een bolomgeving B' van a is, zodat

$$f(B' \cap V) \subseteq B.$$

De functie heet *continu* als f continu is in a 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.

limiet **VI.7.2 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 limiet b heeft als x naar a nadert* en noteren

$$\lim_{x \to a} f(x) = b,$$

als geldt: voor iedere bolomgeving B van b is er een bolomgeving B' van a zodat

$$f(B' \cap V \setminus \{a\}) \subseteq B.$$

Merk op dat a geen element van het domein van f hoeft te zijn. Zie ook Opgave VI.7.3. De volgende stelling is nu gewoon een herformulering van de definitie:

[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.7.3 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.7.4 Opmerking. De definiërende voorwaarde van $\lim_{x \to a} f(x) = b$ wordt vaak als volgt geformuleerd:

$$\forall_{\epsilon>0} \exists_{\delta>0} \forall_{x \in V} \big(0 < \mathrm{d}(x,a) < \delta \implies \mathrm{d}(f(x),b) < \varepsilon\big).$$

Dat leidt tot de volgende definitie van continuïteit van f in a:

$$\forall_{\epsilon>0} \exists_{\delta>0} \forall_{x \in V} \big(\mathrm{d}(x,a) < \delta \implies \mathrm{d}(f(x),f(a)) < \varepsilon\big).$$

ϵ-δ-definitie

Dit staat in de wandelgangen bekend als de *epsilon-delta-definities*.

VI.7.5 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 gebruiken (zie Gevolg VI.4.4): $\big||x|-|c|\big| \leqslant |x-c|$.

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.7.6 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.7.7 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 $\lim_{x \to 1} f(x) = 2$. 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 $\lim_{x \to 1}(x+1) = 2$. Hieruit volgt het gevraagde. ∎

VI.7.8 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 $\lim_{x \to 0} f(x) = L$. 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. Dit is een heel belangrijke stelling, die wordt gebruikt in de oplossing van ieder optimalisatieprobleem.

De clou van het bewijs kan als volgt onthouden worden. Kies een zogenaamde maximaliserende rij: een rij $a_1, a_2, \ldots$ in Z waarvoor de reële rij $f(a_1), f(a_2), \ldots$ convergeert naar het supremum van de verzameling waarden die f aanneemt. Op dit moment in het bewijs weten we nog niet dat die verzameling begrensd is en we weten dus niet dat het supremum genomen kan worden, maar als dit niet zo zou zijn, dan zouden we de rij $a_1, a_2, \ldots$ zo kiezen dat de rij $f(a_1), f(a_2), \ldots$ naar ∞ divergeert. Dan kiezen we een convergente deelrij $a_{r(1)}, a_{r(2)}, \ldots$. Laat a de limiet zijn. Dan convergeert $f(a_{r(1)}), f(a_{r(2)}), \ldots$ wegens de continuïteit naar $f(a)$ (zie ook Opgave VI.7.12). Hieruit volgt ten eerste dat de rij $f(a_{r(1)}), f(a_{r(2)}), \ldots$ begrensd is, en dat $f(Z)$ begrensd is. Maar dan is $f(a)$ het supremum van $f(Z)$. Dat betekent dat f de maximale waarde aanneemt in a.

VI.7.9 Stelling. Zij $Z \subseteq \mathbb{R}^m$ 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.6.7 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 $(a_n)_{n \geqslant 0}$ heeft een convergente deelrij $(a_{r(n)})_{n \geqslant 0}$ met limiet $a \in Z$. Kies een bolomgeving B van $f(a)$. Aangezien f continu is, bestaat er een bolomgeving B' van a zodat $f(B' \cap Z) \subseteq B$. Vanwege de limieteigenschap bestaat er een $N \in \mathbb{N}$ zodat voor alle $n \geqslant N$ geldt $a_{r(n)} \in B'$. Bijgevolg geldt $f(a_{r(n)}) \in B$, 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 $n \geqslant N$ 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

S

1. 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 $\mathbb{R}$.

S ✍ **2.** Zij $D \subseteq \mathbb{R}$ en $c \in D$, en laat $f : D \to \mathbb{R}$ een 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 $f(x) \geqslant 0$

(b) Als $f(c) \geqslant 0$, dan bestaat er een $\delta > 0$ zó dat voor alle $x \in D$ met $|x-c| < \delta$ geldt dat $f(x) \geqslant 0$

S **3.** 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.

V **4.** Laat $V \subseteq \mathbb{R}$, $f, g : V \to \mathbb{R}$, 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) $\lim_{x \to a}(\alpha \cdot f(x)) = \alpha \cdot L$ 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) $\lim_{x \to a} |f(x)| = |L|$.

V **5.** Zij $V \subseteq \mathbb{R}$. Laat $f : V \to \mathbb{R}$ en $g : V \to \mathbb{R}$ twee functies zijn die continu zijn in het punt $c \in V$, en $\alpha \in \mathbb{R}$ 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.

V **6.** Bewijs dat de samenstelling van continue functies weer continu is.

S **7.** 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.

S ✍ **8.** Is de functie $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ gedefinieerd door

$$f(x) = 1/x$$

continu?

V ✍ **9.** 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.

V ✍ **10.** 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 $f(x) = (x^2 + x)/x$.

V ✍ **11.** 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?

B **12.** 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 $f(a)$.

V ✍ **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.7.12.

V **14.** Laat $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, $x \mapsto x/|x|$. Bepaal of de $\lim_{x\to 0} f(x)$ bestaat.

V **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.

B **16.** Bewijs de *tussenwaardestelling*:
Zij $f : [a,b] \to \mathbb{R}$ een continue functie met $a < b$ reële getallen. Zij $y \in \mathbb{R}$ zo, dat y tussen $f(a)$ en $f(b)$ ligt. Dan bestaat er een $c \in [a,b]$ met $f(c) = y$.

[Hint: stel c gelijk aan het supremum van een slim gekozen verzameling.]

VI.8 Uniforme continuïteit

We beperken ons in deze paragraaf voor het gemak tot functies gedefinieerd op een deelverzameling $D \subseteq \mathbb{R}$. De continuïteit van $f : D \to \mathbb{R}$ betekent dat we voor iedere $c \in D$ en iedere $\varepsilon > 0$ een $\delta > 0$ kunnen vinden met de volgende eigenschap:

$$\text{voor alle } x \in D \text{ met } |x-c| < \delta \text{ geldt } \big|f(x)-f(c)\big| < \varepsilon.$$

Deze δ is afhankelijk van ε en c. We vragen ons nu het volgende af: wanneer bestaat er een δ die *onafhankelijk van c* is?

uniform continu

VI.8.1 Definitie. Zij D een deelverzameling van $\mathbb{R}$. Een functie $f : D \to \mathbb{R}$ heet *uniform continu* als er voor iedere $\varepsilon > 0$ een $\delta > 0$ bestaat zodanig dat

$$\text{voor alle } x,y \in D \text{ met } |x-y| < \delta \text{ geldt } \big|f(x)-f(y)\big| < \varepsilon.$$

Het volgt meteen uit deze definitie dat een uniform continue functie continu is, zie Opgave VI.8.1.

VI.8.2 Voorbeeld. Zij $f : [0,1] \to \mathbb{R}$ gegeven door $f(x) = x^2$. We bewijzen dat f uniform continu is. Laat $\varepsilon > 0$. We nemen $\delta = \varepsilon/2$. Voor alle $x,y \in [0,1]$ met $|x-y| < \delta$ geldt dan

$$\big|f(x)-f(y)\big| = |x^2-y^2| = |x+y|\cdot|x-y| \leqslant 2|x-y| < 2\delta = \varepsilon.$$

Niet iedere continue functie is echter uniform continu.

VI.8.3 Voorbeeld. Zij $f : \mathbb{R} \to \mathbb{R}$ gegeven door $f(x) = x^2$. We beweren dat f niet uniform continu is. Immers, neem $\varepsilon = 1$ en zij $\delta > 0$. Neem nu $x = 1/\delta$ en $y = 1/\delta + \delta/2$. Voor zulke x en y geldt dan $|x - y| < \delta$ en

$$\big|f(x) - f(y)\big| = |x^2 - y^2| = |x + y|\,|x - y| = \frac{1}{2}\delta|x + y| \geqslant \frac{1}{2}\delta \cdot \frac{2}{\delta} = 1 = \varepsilon.$$

De uniforme continuïteit in het eerste voorbeeld is geen toeval: er geldt de volgende algemene stelling.

VI.8.4 Stelling. Laat $a, b \in \mathbb{R}$ met $a < b$. Iedere continue functie $f : [a, b] \to \mathbb{R}$ is uniform continu.

Bewijs. Zij $f : [a, b] \to \mathbb{R}$ continu en stel eens dat f niet uniform continu is. We zullen een tegenspraak afleiden.

Omdat f niet uniform continu is, kunnen we niet voor alle $\varepsilon > 0$ een zodanige $\delta > 0$ vinden dat voor alle $x, y \in [a, b]$ met $|x - y| < \delta$ geldt $\big|f(x) - f(y)\big| < \varepsilon$.

Er is dus een $\varepsilon > 0$ waarvoor géén $\delta > 0$ bestaat zó dat voor alle $x, y \in [a, b]$ met $|x - y| < \delta$ geldt $\big|f(x) - f(y)\big| < \varepsilon$.

Er is dus een $\varepsilon > 0$ zodanig dat voor er voor alle $\delta > 0$ een tweetal punten $x, y \in [a, b]$ bestaat waarvoor wél geldt dat $|x - y| < \delta$, maar niet $\big|f(x) - f(y)\big| < \varepsilon$.

We nemen nu zo'n ε, en voor δ achtereenvolgens 1, 1/2, 1/3, enzovoort. Voor iedere $n \geqslant 0$ vinden we zo een tweetal punten $x_n, y_n \in [a, b]$ met

$$|x_n - y_n| < \frac{1}{n+1} \quad \text{en} \quad \big|f(x_n) - f(y_n)\big| \geqslant \varepsilon. \tag{VI.1}$$

De rij $(x_n)_{n \geqslant 0}$ is begrensd, en met Stelling VI.6.6 van Bolzano-Weierstrass vinden we een convergente deelrij $(x_{n_k})_{k \geqslant 0}$. Zij x de limiet van deze deelrij. Dan is $x \in [a, b]$. Voor alle $k \geqslant 0$ geldt

$$|y_{n_k} - x| \leqslant |y_{n_k} - x_{n_k}| + |x_{n_k} - x| \leqslant \frac{1}{n_k + 1} + |x_{n_k} - x|.$$

Wegens $\lim\limits_{k \to \infty} x_{n_k} = x$ volgt hieruit dat de rij $(y_{n_k})_{k \geqslant 0}$ eveneens convergeert en dat

$$\lim_{k \to \infty} y_{n_k} = x.$$

Omdat f continu is, levert dit

$$\lim_{k \to \infty} f(x_{n_k}) = f(x) = \lim_{k \to \infty} f(y_{n_k}).$$

Uit de definitie van een convergente rij volgt dat er een $N \in \mathbb{N}$ bestaat met de volgende eigenschap: voor alle indices $k \geqslant N$ geldt

$$\big|f(x_{n_k}) - f(x)\big| < \frac{\varepsilon}{2} \qquad \text{en} \qquad \big|f(y_{n_k}) - f(x)\big| < \frac{\varepsilon}{2}.$$

Maar voor deze k volgt dan

$$\big|f(x_{n_k}) - f(y_{n_k})\big| \leqslant \big|f(x_{n_k}) - f(x)\big| + \big|f(x) - f(y_{n_k})\big| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Deze tegenspraak besluit het bewijs. ∎

Opgaven

S **1.** Bewijs dat een uniform continue functie continu is.

S ✍ **2.** Toon aan met behulp van de definitie dat de functie $f : \mathbb{R} \to \mathbb{R}$ gegeven door

$$f(x) = 5x$$

uniform continu is.

S ✍ **3.** Laat zien dat de functie $f : (0,\infty) \to \mathbb{R}$, $x \mapsto 1/x$ niet uniform continu is.

V **4.** Definieer $f : [0,\infty) \to \mathbb{R}$ door $f(x) = \sqrt{x}$. Bewijs, direct met de definities, dat f uniform continu is.

V **5.** Laat $D \subseteq \mathbb{R}$ en $f, g : D \to \mathbb{R}$ uniform continu zijn. Toon aan:

(a) $f + g$ is uniform continu.

✍ (b) Als f en g begrensd zijn, dan is fg uniform continu.

(c) Geef een voorbeeld waarin f en g uniform continu zijn en fg niet.

V **6.** (a) Geef een voorbeeld van een functie $f : \mathbb{R} \to \mathbb{R}$ die continu en begrensd is maar niet uniform continu.

(b) Geef een voorbeeld van een functie $f : (0,1) \to \mathbb{R}$ die continu en begrensd is maar niet uniform continu.

V **7.** Veralgemeniseer deze paragraaf naar functies $D \to \mathbb{R}$ gedefinieerd op een deelverzameling $D \subseteq \mathbb{R}^m$ voor $m \geqslant 1$.

B **8.** Laat $f : (0,1) \to \mathbb{R}$ uniform continu zijn. Toon aan dat f begrensd is.

★ ✍ **9.** Stel $f : (0,1] \to \mathbb{R}$ is uniform continu. Bewijs dat $\lim_{x \to 0} f(x)$ bestaat.

★ **10.** Laat $f : (0,1) \to \mathbb{R}$ uniform continu zijn. Toon aan dat er een unieke continue functie $g : [0,1] \to \mathbb{R}$ bestaat zó dat $g(x) = f(x)$ voor alle $x \in (0,1)$.

VI.9 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*, $\mathbb{C}$. Dit feit heet de hoofdstelling van de algebra. 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 $\mathbb{R}^2$.

complexe getallen

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.

hoofdstelling van de algebra

VI.9.1 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.

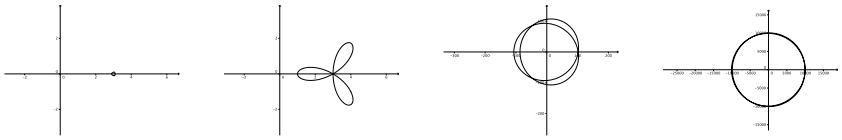
- Als $r = 0$ dan is deze 'cirkel' een punt; het beeld $f(C_r)$ is dus ook een punt A in het complexe vlak. Als $A = 0$ dan zijn we klaar. Neem vanaf nu dus aan dat $A \neq 0$.
- Voor een complex getalen z dat ver van de oorsprong ligt, geldt $f(z) \approx z^n$ (preciezer: $f(z) = z^n + \mathcal{O}(z^{n-1})$). 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!

$r = 0{,}1$ $r = 1$ $r = 10$ $r = 100$



VII LINEAIRE ALGEBRA

In dit hoofdstuk behandelen we de basisresultaten 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 in Paragraaf VII.6.

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'.

F-vectorruimte

VII.1.1 Definitie. Laat $(F, +_F, \cdot_F, 0_F, 1_F)$ een lichaam zijn. Een *vectorruimte over F*, of ook *F-vectorruimte*, is een systeem $(V, 0_V, +_V, \cdot_V)$, met $0_V \in V$, $+_V : V \times V \to V$, $(v,w) \mapsto v +_V w$, en $\cdot_V : F \times V \to V$, $(\lambda, v) \mapsto \lambda \cdot_V v$, dat voldoet aan de volgende axioma's:

V0 $\forall v, w \in V,\ v +_V w = w +_V v$ (optelling is commutatief);
V1 $\forall v, w, x \in V,\ (v +_V w) +_V x = v +_V (w +_V x)$ (optelling is associatief);

V2 $\forall v \in V,\ v +_V 0_V = v$ (0_V is neutraal voor optelling in V);
V3 $\forall v \in V,\ \exists w \in V,\ v +_V w = 0_V$ (bestaan van additieve inverse);
V4 $\forall \lambda, \mu \in F,\ \forall v \in V,\ (\lambda \cdot_F \mu) \cdot_V v = \lambda \cdot_V (\mu \cdot_V v)$ (compatibiliteit $\cdot_F$ en $\cdot_V$);
V5 $\forall v \in V,\ 1_F \cdot_V v = v$ (vermenigvuldiging met 1_F is de identiteit);
V6 $\forall \lambda, \mu \in F,\ \forall v \in V,\ (\lambda +_F \mu) \cdot_V v = \lambda \cdot_V v +_V \mu \cdot_V v$ (distributiviteit in 1e variabele);
V7 $\forall \lambda \in F,\ \forall v, w \in V,\ \lambda \cdot_V (v +_V w) = \lambda \cdot_V v +_V \lambda \cdot_V w$ (distributiviteit in 2e variabele).

vector, scalair

De elementen van V noemen we *vectoren*, en die van F noemen we *scalairen*; het lichaam F zelf is het *lichaam van scalairen*. De vermenigvuldigingsoperatie $\cdot_V$ heet ook wel *scalairvermenigvuldiging* en schrijven we vaak als $F \times V \to V$, $(\lambda, v) \mapsto \lambda v$. Meestal zullen we $(V, 0_V, +_V, \cdot_V)$ als V noteren, als het duidelijk is wat de rest is.

scalair-vermenigvuldiging

De grote hoeveelheid subscripts maakt de voorgaande definitie nogal onprettig om te lezen. In het vervolg zullen we die subscripts dus weglaten. Dat betekent dat je zelf uit de context zal moeten opmaken of het symbool 0 staat voor 0_F of 0_V. Hetzelfde geldt voor + en $\cdot$.

VII.1.2 Opmerking. De axioma's V0–V3 betekenen dat $(V, 0, +)$ een additief genoteerde *commutatieve groep* is. Wie deze term nog niet kent kan het als definitie nemen.

vectorruimte F^n

VII.1.3 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 coördinaatsgewijs:

$$(v_1, \ldots, v_n) + (w_1, \ldots, w_n) = (v_1 + w_1, \ldots, v_n + w_n).$$

De scalairvermenigvuldiging is ook coördinaatsgewijs:

$$\lambda \cdot (v_1, \ldots, v_n) = (\lambda v_1, \ldots, \lambda v_n).$$

De lichaamseigenschappen van F impliceren direct dat aan V0–V7 is voldaan. Iedere $(v_1, \ldots, v_n)$ heeft een unieke additieve inverse, namelijk $(-v_1, \ldots, -v_n)$. ∎

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.1.2).

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.1.3). We zien dus dat het verschil tussen V en F^n slechts 'administratief' is (de vertaling in notatie wordt gedaan door φ).

n-tupel

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. ∎

Alle rekenregels voor F-vectorruimten volgen uit de axioma's. We geven er een paar.

rekenregels in een vectorruimte

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 $v \in V$: $\lambda^{-1}\cdot(\lambda\cdot v) = v$.
7. Voor alle $\lambda \in F$ en alle $v \in V$: $\lambda\cdot v = 0 \implies (\lambda = 0 \vee v = 0)$.

Bewijs. Dat is Opgave VII.1.4. ■

Laat F een lichaam zijn, en V een F-vectorruimte.

deelruimte

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 $\big(\forall w_1, w_2 \in W,\ w_1 + w_2 \in W\big)$ en $\big(\forall \lambda \in F,\ \forall w \in W,\ \lambda w \in W\big)$.

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. ■

Opgaven

S

1. (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 $(\mathbb{C},0,+)$ met $\mathbb{R}$ als lichaam van scalairen.

V ✍

2. 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?

V **3.** Bewijs de uitspraken over φ in Voorbeeld VII.1.4. Dit is vooral een oefening in notatie, er 'gebeurt' eigenlijk niets.

V **4.** Bewijs alle uitspraken in Stelling VII.1.5.

V ✍ **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?

S **6.** 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 $X = R$). 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.

VII.2.1 Definitie. Laat V en W vectorrruimten, en $f : V \to W$ een afbeelding. Dan noemen we f *lineair* als gelden:

lineaire functie

(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.

1. 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.
2. 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).
3. In Opgave VII.2.1 wordt bewezen dat de voorwaarden **L0** en **L1** samen equivalent zijn met de voorwaarde

   (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. 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*.

affiene functie

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).

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.2.2).

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 lineair.

3. Voor iedere $a \in \mathbb{R}$ is de afbeelding 'verschuif de grafiek a naar links', $v_a : V \to V$, gegeven door $(v_a(f))(x) = f(x+a)$ lineair. ▬

kern

VII.2.4 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: $\ker(f)$.

kern en beeld zijn deelruimten

VII.2.5 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. De afbeelding f is injectief precies dan als $\ker(f) = \{0\}$.

Bewijs. Opgave VII.2.4. ■

We gaan nu over op een eenvoudiger soort voorbeeld: 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.

VII.2.6 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

VII.2.7 Definitie. Laat $m, n \in \mathbb{N}$. Een *m-bij-n matrix met coëfficiënten in F* is een functie $a : \{1,\ldots,m\} \times \{1,\ldots,n\} \to F$, $(i,j) \mapsto a_{i,j}$, ook wel genoteerd als

$$a = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix}.$$

De verzameling van m-bij-n matrices met coëfficiënten in F noteren we $\mathrm{M}_{m,n}(F)$, en als $n = m$ ook als $\mathrm{M}_n(F)$.

rij, rijvector

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.

kolom, kolomvector

nulmatrix

identiteitsmatrix

We definiëren de *nulmatrix* $0_{m,n} \in \mathrm{M}_{m,n}(F)$ als de matrix waarvan alle coëfficiënten 0 zijn. Als $n = m$ definiëren de *identiteitsmatrix* $1_n \in \mathrm{M}_n(F)$ door, voor alle $(i,j) \in \{1,\dots,n\} \times \{1,\dots,m\}$, $(1_n)_{i,j} = 1$ 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 *coördinaat* v_i, dus dan geldt:

$$v = (v_1, \dots, v_n).$$

Dan geldt voor iedere v in F^n dat

$$\begin{aligned} v = (v_1,\dots,v_n) &= (v_1,0,\dots,0) + \cdots + (0,\dots,0,v_n) \\ &= v_1 \cdot (1,0,\dots,0) + \cdots + v_n \cdot (0,\dots,0,1). \end{aligned}$$

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

$$\begin{aligned} e_{i,j} &= 1 \quad \text{als } i = j, \\ e_{i,j} &= 0 \quad \text{als } i \neq j. \end{aligned}$$

standaardbasis

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.3.8; hier hebben we die nog niet nodig. Met deze notatie geldt dan

$$\forall v \in F^n, \quad v = v_1 e_1 + \cdots + v_n e_n = \sum_{i=1}^{n} v_i e_i.$$

VII.2.8 Definitie. Laat $m,n \in \mathbb{N}$ en $f : F^n \to F^m$ lineair. Dan definiëren we $\mathrm{mat}_{\mathrm{st}}(f)$ in $\mathrm{M}_{m,n}(F)$ door:

$$\forall (i,j) \in \{1,\dots,m\} \times \{1,\dots,n\}, \quad \mathrm{mat}_{\mathrm{st}}(f)_{i,j} = f(e_j)_i.$$

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*.

matrix t.o.v. standaardbases

VII.2.9 Lemma. 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 $w = (w_1,\dots,w_n) \in W^n$ een unieke lineaire afbeelding $f : F^n \to W$ is zodat voor alle j in $\{1,\dots,n\}$ 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.2.1 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

$$\begin{aligned} f(v+\lambda v') &= f((v_1,\ldots,v_n)+\lambda(v'_1,\ldots,v'_n)) \\ &= f((v_1,\ldots,v_n)+(\lambda v'_1,\ldots,\lambda v'_n)) \\ &= f((v_1+\lambda v'_1,\ldots,v_n+\lambda v'_n)) \\ &= (v_1+\lambda v'_1)w_1+\cdots+(v_n+\lambda v'_n)w_n \\ &= v_1w_1+\lambda v'_1w_1+\cdots+v_nw_n+\lambda v'_nw_n \\ &= v_1w_1+\cdots v_nw_n+\lambda v'_1w_1+\cdots+\lambda v'_nw_n \\ &= v_1w_1+\cdots v_nw_n+\lambda(v'_1w_1+\cdots+v'_nw_n) \\ &= f(v)+\lambda f(v'). \end{aligned}$$

De afbeelding f is dus inderdaad lineair. Duidelijk geldt voor iedere $j \in \{1,\ldots,n\}$ dat $f(e_j) = w_j$.

Neem nu aan dat $g\colon F^n \to W$ 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 lineaire functies en matrices

VII.2.10 Stelling. Laat $m, n \in \mathbb{N}$. Dan is de afbeelding

$$\mathrm{mat}_{\mathrm{st}}\colon \mathrm{Hom}(F^n, F^m) \to \mathrm{M}_{m,n}(F), \quad f \mapsto \mathrm{mat}_{\mathrm{st}}(f)$$

een bijectie.

Bewijs. Dit volgt uit Lemma VII.2.9 toegepast met $W = F^m$. ∎

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.

operaties op lineaire functies

VII.2.11 Stelling.

1. Laat V, W en U vectorruimten zijn, en $f\colon V \to W$ en $g\colon W \to U$ lineaire afbeeldingen. Dan is $g \circ f\colon V \to U$ lineair.
2. Laat V en W vectorruimten zijn, en $f\colon V \to W$ een lineaire afbeelding die bijectief is. Dan is $f^{-1}\colon W \to V$ 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 $f+\lambda g\colon V \to W$, $v \mapsto f(v)+\lambda g(v)$ 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, $f, g\colon V \to W$, $h\colon W \to U$, 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, $h\colon V \to W$, $f, g\colon W \to U$, 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.2.5. We hebben dus de afbeelding $f^{-1}\colon W \to V$, 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

$$\begin{aligned}
w_1 = f(f^{-1}(w_1)) \quad \text{en} \quad w_2 = f(f^{-1}(w_2)) &\quad \text{definitie inverse functie}\\
w_1 + \lambda w_2 = f(f^{-1}(w_1)) + \lambda f(f^{-1}(w_2)) &\quad \text{volgt uit regel 1}\\
f(f^{-1}(w_1)) + \lambda f(f^{-1}(w_2)) = f\left(f^{-1}(w_1) + \lambda f^{-1}(w_2)\right) &\quad \text{lineariteit van } f\\
w_1 + \lambda w_2 = f\left(f^{-1}(w_1) + \lambda f^{-1}(w_2)\right) &\quad \text{regels 2 en 3}\\
f^{-1}(w_1 + \lambda w_2) = f^{-1}\left(f\left(f^{-1}(w_1) + \lambda f^{-1}(w_2)\right)\right) &\quad f^{-1} \text{ op regel 4}\\
f^{-1}\left(f\left(f^{-1}(w_1) + \lambda f^{-1}(w_2)\right)\right) = f^{-1}(w_1) + \lambda f^{-1}(w_2) &\quad \text{definitie inverse functie}\\
f^{-1}(w_1 + \lambda w_2) = f^{-1}(w_1) + \lambda f^{-1}(w_2) &\quad \text{regels 5 en 6}
\end{aligned}$$

■

Laat $n, m, l \in \mathbb{N}$, $a \in \mathrm{M}_{l,m}(F)$ en $b \in \mathrm{M}_{m,n}(F)$. Vanwege Stelling VII.2.10 is er een unieke $f_a\colon F^m \to F^l$ met $\mathrm{mat}_{\mathrm{st}}(f_a) = a$, en is er een unieke $f_b\colon F^n \to F^m$ met $\mathrm{mat}_{\mathrm{st}}(f_b) = b$. Dan is er vanwege Stelling VII.2.11 en Stelling VII.2.10 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

$$\mathrm{M}_{l,m}(F) \times \mathrm{M}_{m,n}(F) \to \mathrm{M}_{l,n}(F), \quad (a, b) \mapsto ab$$

matrix-vermenigvuldiging

heet *matrixvermenigvuldiging*.

VII.2.12 Lemma. In de notatie als hierboven geldt:

$$\forall (i,j) \in \{1,\ldots,l\} \times \{1,\ldots,n\}, \quad (ab)_{i,j} = \sum_{k=1}^{m} a_{i,k} b_{k,j}.$$

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:

$$\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & & \vdots \\ b_{m,1} & b_{m,2} & \cdots & b_{m,n} \end{pmatrix} = b$$

$$a = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & & \vdots \\ a_{l,1} & a_{l,2} & \cdots & a_{l,m} \end{pmatrix} \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & & \vdots \\ c_{l,1} & c_{l,2} & \cdots & c_{l,n} \end{pmatrix} = ab$$

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.2.11.

Laat $m,n \in \mathbb{N}$, en $a,b \in \mathrm{M}_{m,n}(F)$. Vanwege Stelling VII.2.10 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.2.11 en Stelling VII.2.10 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

$$\mathrm{M}_{m,n}(F) \times \mathrm{M}_{m,n}(F) \to \mathrm{M}_{m,n}(F), \quad (a,b) \mapsto a+b$$

matrixoptelling

heet *matrixoptelling*.

VII.2.13 Lemma. In de notatie als hierboven geldt:

$$\forall (i,j) \in \{1,\ldots,m\} \times \{1,\ldots,n\}, \quad (a+b)_{i,j} = a_{i,j} + b_{i,j}.$$

Bewijs. De j-de kolom van $a+b$ is

$$(f_a + f_b)(e_j) = f_a(e_j) + f_b(e_j) = \sum_{i=1}^{n} a_{i,j} e_i + \sum_{i=1}^{n} b_{i,j} e_i = \sum_{i=1}^{n} (a_{i,j} + b_{i,j}) e_i. \qquad \blacksquare$$

In Stelling VII.2.11 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 Stelling VII.2.10 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.2.11 en Stelling VII.2.10 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

$$F \times \mathrm{M}_{m,n}(F) \to \mathrm{M}_{m,n}(F), \quad (\lambda, a) \mapsto \lambda a$$

matrixscalair-vermenigvuldiging

heet *matrixscalairvermenigvuldiging*.

VII.2.14 Lemma. In de notatie als hierboven geldt:

$$\forall (i,j) \in \{1,\ldots,m\} \times \{1,\ldots,n\}, \quad (\lambda a)_{i,j} = \lambda a_{i,j}.$$

Bewijs. De j-de kolom van λa is

$$(\lambda f_a)(e_j) = \lambda f_a(e_j) = \lambda \sum_{i=1}^{n} a_{i,j} e_i = \sum_{i=1}^{n} \lambda a_{i,j} e_i. \qquad \blacksquare$$

Nu kunnen we de vruchten plukken van Stelling VII.2.11 en ons werk aan het verband tussen matrices en lineaire afbeeldingen.

VII.2.15 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 matrixscalairvermenigvuldiging 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.2.11. ■

$\mathrm{M}_n(F)$ is een ring

VII.2.16 Gevolg. Laat $n \in \mathbb{N}$. Dan is de verzameling $\mathrm{M}_n(F)$ 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 $n \leqslant 1$.

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 $n = 2$. 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 $ba = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$. Voor $n > 2$ vind je op vergelijkbare manier niet-commuterende matrices $a,b \in \mathrm{M}_n(F)$. ■

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 $a \in \mathrm{M}_{m,n}(F)$. In het bewijs van Lemma VII.2.9 is de lineaire afbeelding $f_a \colon F^n \to F^m$ waarvoor geldt $\mathrm{mat}_{\mathrm{st}}(f_a) = a$ 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:

$$\forall v \in F^n, \quad \mathrm{kol}_m(f_a(v)) = a \cdot \mathrm{kol}_n(v).$$

commutatief diagram

In de hedendaagse wiskunde geeft men dit soort formules graag weer in de vorm van een *commutatief diagram*:

$$\begin{array}{ccc} F^n & \xrightarrow{f_a} & F^m \\ {\scriptstyle \mathrm{kol}_n}\downarrow & & \downarrow{\scriptstyle \mathrm{kol}_m} \\ \mathrm{M}_{n,1}(F) & \xrightarrow{a\cdot} & \mathrm{M}_{m,1}(F). \end{array}$$

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.

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

$$a\cdot : F^n \to F^m, \quad x \mapsto ax. \tag{VII.1}$$

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.

Opgaven

S **1.** Bewijs dat in Definitie VII.2.1 de voorwaarden **L0** en **L1** samen equivalent zijn met de voorwaarde
(L) $\forall v_1, v_2 \in V,\ \forall \lambda \in F,\ f(v_1 + \lambda v_2) = f(v_1) + \lambda f(v_2)$.

S **2.** Bewijs de claims van Voorbeeld VII.2.3.

V **3.** 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 voor alle $a \in \mathbb{R}$ geldt: $v_a \circ d = d \circ v_a$ en dat $v_a \circ p - p \circ v_a$ de lineaire afbeelding van C naar de deelruimte van constante functies is die f stuurt naar $\int_0^a f(t)\,dt$.

(c) Wat kun je zeggen over $d \circ p$?

(d) En kunnen we praten over $p \circ d$?

V **4.** Bewijs Stelling VII.2.5.

V **5.** Bewijs de overige onderdelen van Stelling VII.2.11

S ✍ **6.** Wat is de reden dat het matrixproduct gegeven wordt door de formule in Lemma VII.2.12?

V **7.** Geef een voorbeeld van een lichaam F, a en b in $\mathrm{M}_2(F)$ met $ab = 0$ en $ba \neq 0$.

V **8.** 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.3.8 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.

VII.3.1 Stelling. Laat V een vectorruimte zijn. Laat I een verzameling zijn, en voor iedere $i \in I$ laat W_i een deelruimte van V zijn. Dan is $\bigcap_{i\in I} W_i$ een deelruimte van V.

Bewijs. Opgave VII.3.4. ∎

VII.3.2 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 deelruimte van V, en $S \subseteq W$.
(b) W is de kleinste deelruimte van V die S bevat: als U een deelruimte van V is met $S \subseteq U$, dan $W \subseteq U$.
(c) W is de doorsnede van alle deelruimten van V die S bevatten.

deelruimte voortgebracht door S

Deze deelruimte W noemen we de *deelruimte voortgebracht door* S, en we noteren haar $\langle S\rangle$.

Bewijs. Opgave VII.3.5. ∎

Uitdrukkingen als $\lambda_1 v_1 + \cdots + \lambda_n v_n$ hebben een speciale naam.

lineaire combinatie

VII.3.3 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 v met coëfficiënten λ*.

eindig voortgebracht

VII.3.4 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.3.5 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 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 $\dim(F^n) \leqslant n$ 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.

VII.3.6 Lemma. Laat V en W eindig voortgebrachte vectorruimten, en $f: V \to W$ een surjectieve lineaire afbeelding. Dan geldt $\dim(W) \leqslant \dim(V)$. 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 $i \in \{1,\ldots,d\}$ laat $w_i = f(v_i)$. Dan is $(w_1,\ldots,w_d)$ een voortbrengend d-tupel van W. Dit bewijst $\dim(W) \leqslant \dim(V)$. 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 $(w_1,\ldots,w_{d-1})$ W voort: lineaire combinaties in $(w_1,\ldots,w_d)$ worden door substitutie van w_d als lineaire combinatie van $(w_1,\ldots,w_{d-1})$ lineaire combinaties van $(w_1,\ldots,w_{d-1})$. Dat geeft $\dim(W) \leqslant d-1 < \dim(V)$. ∎

$\dim F^n = n$

VII.3.7 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 $\dim(F^n) \leqslant n$. Voor $n = 0$: $F^0 = \langle\varnothing\rangle$ dus $0 \leqslant \dim(F^0) \leqslant 0$. Laat $n \in \mathbb{N}$ en laat

$$p: F^{n+1} \to F^n, \quad (x_1,\ldots,x_{n+1}) \mapsto (x_1,\ldots,x_n)$$

de projectie op de eerste n coördinaten zijn. Dan is p een surjectieve lineaire afbeelding die niet injectief is, dus volgens Lemma VII.3.6 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 $n = \dim(F^n) < \dim(F^{n+1}) \leqslant n+1$. Maar dan $\dim(F^{n+1}) = n+1$. ∎

VII.3.8 Definitie. Laat V een vectorruimte, $n \in \mathbb{N}$ en $v \in V^n$. Dan definiëren we

$$\varphi_v: F^n \to V, \quad \lambda \mapsto \sum_{i=1}^{n} \lambda_i v_i.$$

basis

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 $w = \sum_{i=1}^{n} \lambda_i v_i$.

VII.3.9 Definitie. Laat V een vectorruimte zijn, $n \in \mathbb{N}$ en $v \in V^n$. Dan heet v
lineair afhankelijk
lineair onafhankelijk

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 *vlineair onafhankelijk*.

VII.3.10 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.3.8 is 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. Het stelsel v is een basis van V precies dan als v de vectorruimte V voortbrengt en onafhankelijk is.
5. Als $(v_1,\ldots,v_n)$ een basis is van V dan geldt $\dim(V) = n$.
6. Als V voortgebracht is door v dan zijn er een d in $\{0,\ldots,n\}$ en een $w \in V^d$ zodat $\{w_1,\ldots,w_d\} \subseteq \{v_1,\ldots,v_n\}$ 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.2.11 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 geldt dat $\langle\{w_1,\dots,w_j,w_{j+1}\}\rangle = V_{i_{j+1}}$. 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. Het volgt dat $(w_1,\dots,w_j,w_{j+1})$ onafhankelijk is, 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. ∎

VII.3.11 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. $\dim(W) \leqslant \dim(V)$.
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 $n \geqslant 1$, 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.3.10. 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 $\dim(W) \leqslant \dim(V)$.

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*.

dimensiestelling

VII.3.12 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.3.11 is $\ker(f)$ eindig voortgebracht en vanwege Stelling VII.3.10, 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.3.11 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

S **1.** Laat $W = \{(x_1,x_2,x_3) \in F^3 : x_1 + x_2 + x_3 = 0\}$. Geef een basis van W.

S **2.** Laat $n \in \mathbb{N}_{>0}$. Laat $W = \{x \in F^n : x_1 + \cdots + x_n = 0\}$. Bepaal $\dim(W)$.

V ✍ **3.** Laat $W = \{x \in F^2 : x_1 + x_2 = 0 \wedge x_1 - x_2 = 0\}$. Bepaal $\dim(W)$.

V **4.** Bewijs Stelling VII.3.1.

B **5.** Bewijs Stelling VII.3.2.

V **6.** 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.

V **7.** Laat $F = \mathbb{R}$ en V de $\mathbb{R}$-vectorruimte 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.

B **8.** Maak onderdeel (b) van Opgave VII.2.8. Hint: gebruik Stelling VII.3.12 om te bewijzen dat a injectief is.

B **9.** 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 Stelling VII.2.10 al hebben, en v en w per definitie (Definitie VII.3.8) isomorfismen $\varphi_v : F^n \to V$ en $\varphi_w : F^m \to W$ geven, hoeven we deze zaken slechts te combineren.

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.3.8 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:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle\varphi_v}\uparrow & & \uparrow{\scriptstyle\varphi_w} \\ F^n & & F^m \end{array}$$

We kunnen zo nog geen afbeelding van $F^n \to F^m$ maken, maar dat kunnen we wel als we φ_w vervangen door $\varphi_w^{-1} : W \to F^m$:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle\varphi_v}\uparrow & & \downarrow{\scriptstyle\varphi_w^{-1}} \\ F^n & & F^m \end{array}$$

Dit diagram nodigt ons uit om naar $\varphi_w^{-1} \circ f \circ \varphi_v : F^n \to F^m$ te kijken. Deze lineaire afbeelding is volgens Stelling VII.2.10 gegeven door een uniek element

matrix t.o.v. bases

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.1) hebben we dan een commutatief diagram:

$$\begin{array}{ccc} V & \xrightarrow{\quad f \quad} & W \\ {\scriptstyle\varphi_v}\uparrow & & \uparrow{\scriptstyle\varphi_w} \\ F^n & \xrightarrow[{}_w\mathrm{mat}_v(f)\cdot]{} & F^m \end{array}$$

Dit diagram zegt dat f kan worden uitgedrukt in ${}_w\mathrm{mat}_v(f)$, en vice versa:

$$f = \varphi_w \circ {}_w\mathrm{mat}_v(f)\cdot \circ \varphi_v^{-1}, \qquad {}_w\mathrm{mat}_v(f)\cdot = \varphi_w^{-1} \circ f \circ \varphi_v\,. \tag{VII.2}$$

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.

vector t.o.v. basis

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:

$$\forall x \in V, \quad \mathrm{vec}_w(f(x)) = {}_w\mathrm{mat}_v(f)\cdot\mathrm{vec}_v(x), \tag{VII.3}$$

en de j-de kolom van ${}_w\mathrm{mat}_v(f)$ is $\mathrm{vec}_w(f(v_j))$.

matrices en samenstellen

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.2. 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.2 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

$$\big({}_u\mathrm{mat}_w(g) \cdot {}_w\mathrm{mat}_v(f)\big)\cdot = \big({}_u\mathrm{mat}_w(g)\cdot\big) \circ \big({}_w\mathrm{mat}_v(f)\cdot\big)\,.$$

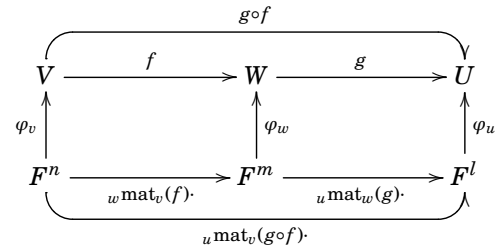
Dit met de voorlaatste gelijkheid combineren geeft:

$$\big({}_u\mathrm{mat}_w(g) \cdot {}_w\mathrm{mat}_v(f)\big)\cdot = {}_u\mathrm{mat}_v(g \circ f)\cdot\,.$$

[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.

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'. ■

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:

$$ {}_{w'}\mathrm{mat}(f)_{v'} = {}_{w'}\mathrm{mat}_w(\mathrm{id}_W) \cdot {}_w\mathrm{mat}_v(f) \cdot {}_v\mathrm{mat}_{v'}(\mathrm{id}_V). $$

matrices van basisverandering

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

$$ \begin{aligned} \forall x \in V \quad & \mathrm{vec}_v(x) = {}_v\mathrm{mat}_{v'}(\mathrm{id}_V) \cdot \mathrm{vec}_{v'}(x), \\ \forall y \in W \quad & \mathrm{vec}_{w'}(x) = {}_{w'}\mathrm{mat}_w(\mathrm{id}_W) \cdot \mathrm{vec}_w(y). \end{aligned} $$

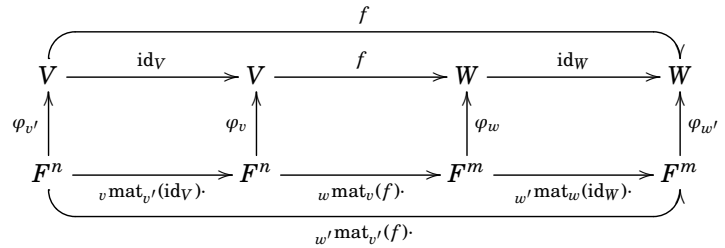
De j-de kolom van ${}_v\mathrm{mat}_{v'}(\mathrm{id}_V)$ is $\mathrm{vec}_v(v'_j)$, en de i-de kolom van ${}_{w'}\mathrm{mat}_w(\mathrm{id}_W)$ is $\mathrm{vec}_{w'}(w_i)$.

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.3) 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:



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 $i = j \leqslant r$ en 0 anders. Met

andere woorden, en met $n = \dim(V)$ en $m = \dim(W)$:

$$ {}_w\mathrm{mat}_v(f) = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} = \left(\begin{array}{c|c} 1_r & 0_{r,n-r} \\ \hline 0_{m-r,r} & 0_{m-r,n-r} \end{array}\right). $$

endomorfisme

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

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

S **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 ${}_w\mathrm{mat}_w(d)$.

B **2.** Laat F een lichaam zijn, V en W twee 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 $i = j \leqslant r$ en 0 anders. Hint: gebruik het bewijs van Stelling VII.3.12.

V **3.** De *rij van Fibonacci* is recursief gedefiniëerd door $F_0 = 0$, $F_1 = 1$, en voor alle $n \geqslant 2$: $F_n = F_{n-1} + F_{n-2}$.

(a) Bereken $F_2, \ldots, F_{10}$.

(b) Een manier om een formule voor F_n te vinden is als volgt. Voor alle $n \geqslant 2$ 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 $n \geqslant 1$ 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 $f\colon \mathbb{R}^2 \to \mathbb{R}^2$, $\binom{x_1}{x_2} \mapsto \left(\begin{smallmatrix}0 & 1\\ 1 & 1\end{smallmatrix}\right)\cdot\binom{x_1}{x_2}$. 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 $f(v_2) = \lambda_2 v_2$.

(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 [SM] argumenteren dat de oorsprong in de genealogie van bijen ligt.

VII.5 Lineaire vergelijkingen, Gauss eliminatie en 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 [vL], dat op zich gedeeltelijk weer is gebaseerd op een dictaat [St1] 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

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n &= 0\\ \quad\vdots & \vdots\ \ \vdots\\ a_{m,1}x_1 + \cdots + a_{m,n}x_n &= 0 \end{cases} \quad \text{met } a_{i,j} \in F.$$

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 $a\cdot\colon F^n \to F^m$, want voor x in F^n zijn de linkerleden van de m vergelijkingen de coördinaten van $a\cdot x$. Stelling VII.2.5 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.3.12, 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-operatie

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.

Gauss eliminatie

elementaire rij-operaties

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

$$\mathrm{rij}_i\colon \mathrm{M}_{m,n}(F) \to F^n, \quad a \mapsto \mathrm{rij}_i(a) = (a_{i,1},\ldots,a_{i,n})$$

die a stuurt naar zijn i-de rij. De 3 typen operaties zijn:

1. $R_1(i,\lambda)$. Voor $i \in \{1,\ldots,m\}$ en $\lambda \in F^\times$ is $R_1(i,\lambda)(a)$ het element van $\mathrm{M}_{m,n}(F)$ verkregen door de i-de rij van a te vermenigvuldigen met λ. In een formule:

$$\mathrm{rij}_l(R_1(i,\lambda)(a)) = \begin{cases} \lambda\cdot\mathrm{rij}_l(a) & \text{als } l = i \\ \mathrm{rij}_l(a) & \text{anders.} \end{cases}$$

2. $R_2(i,j)$. Voor $i,j \in \{1,\ldots,m\}$ met $i \neq j$ is $R_2(i,j)(a)$ het element van $\mathrm{M}_{m,n}(F)$ verkregen door de i-de en j-de rijen van a te verwisselen. In een formule:

$$\mathrm{rij}_l(R_2(i,j)(a)) = \begin{cases} \mathrm{rij}_j(a) & \text{als } l = i \\ \mathrm{rij}_i(a) & \text{als } l = j \\ \mathrm{rij}_l(a) & \text{anders.} \end{cases}$$

3. $R_3(i,j,\alpha)$. Voor $i,j \in \{1,\ldots,m\}$ met $i \neq j$ en $\alpha \in F$ is $R_3(i,j,\alpha)(a)$ 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:

$$\mathrm{rij}_l(R_3(i,j,\alpha)(a)) = \begin{cases} \mathrm{rij}_j(a) + \alpha\cdot\mathrm{rij}_i(a) & \text{als } l = j \\ \mathrm{rij}_l(a) & \text{anders.} \end{cases}$$

rij-operaties zijn inverteerbaar

VII.5.1 Stelling. De bovenstaande rij-operaties zijn inverteerbaar: de inverse van $R_1(i,\lambda)$ is $R_1(i,\lambda^{-1})$, de inverse van $R_2(i,j)$ is $R_2(i,j)$ en de inverse van $R_3(i,j,\alpha)$ is $R_3(i,j,-\alpha)$.

Bewijs. We laten zien dat voor λ en μ in $F^\times$ geldt dat $R_1(i,\lambda)\circ R_1(i,\mu) = R_1(i,\lambda\mu)$; hieruit volgt $R_1(i,\lambda)\circ R_1(i,\lambda^{-1}) = R_1(i,1) = \mathrm{id}$ en $R_1(i,\lambda^{-1})\circ R_1(i,\lambda) = R_1(i,1) = \mathrm{id}$. Voor $l \neq i$ geldt:

$$\mathrm{rij}_l(R_1(i,\lambda)(R_1(i,\mu)a)) = \mathrm{rij}_l(R_1(i,\mu)a) = \mathrm{rij}_l(a) = \mathrm{rij}_l(R_1(i,\lambda\mu)a),$$

en ook

$$\mathrm{rij}_i(R_1(i,\lambda)(R_1(i,\mu)a)) = \lambda\cdot\mathrm{rij}_i(R_1(i,\mu)a)) = \lambda\cdot\mu\cdot\mathrm{rij}_i(a) = \mathrm{rij}_i(R_1(i,\lambda\mu)a).$$

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. ∎

kern invariant onder rij-operaties

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 $l \in \{1,\ldots,m\}$ dat $\sum_j a_{l,j}x_j = 0$. We gaan nu de 3 typen rij-operaties af.

Stel dat $a' = R_1(i,\lambda)(a)$. 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 $l \in \{1,\ldots,m\}$ 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 $a' = R_2(i,j)(a)$. Dan geldt voor iedere $l \in \{1,\ldots,m\}$ 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 $a' = R_3(i,j,\alpha)(a)$. 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 $l \in \{1,\ldots,m\}$ 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.

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. Vóór elke matrix hebben we aangegeven hoe de rijen zijn berekend, door middel van rij-operaties, uit de rijen van de voorgaande matrix.

$$\begin{pmatrix} -1 & 2 & 1 & 1 \\ 1 & -1 & 1 & 0 \\ 2 & -3 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{matrix} -R_1 \\ R_2 \\ R_3 \end{matrix} \begin{pmatrix} 1 & -2 & -1 & -1 \\ 1 & -1 & 1 & 0 \\ 2 & -3 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{matrix} R_1 \\ R_2 - R_1 \\ R_3 - 2R_1 \end{matrix} \begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

$$\rightsquigarrow \begin{matrix} R_1 + 2R2 \\ R_2 \\ R_3 - R_2 \end{matrix} \begin{pmatrix} 1 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \rightsquigarrow \begin{matrix} R_1 \\ R_2 \\ 2^{-1}R_3 \end{matrix} \begin{pmatrix} 1 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\rightsquigarrow \begin{matrix} R_1 - R_3 \\ R_2 - R_3 \\ R_3 \end{matrix} \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

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.

rijtrapvorm

spil

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:

$$\begin{array}{c} 1 \\ 2 \\ \vdots \\ r \\ r+1 \\ \vdots \\ m \end{array} \begin{pmatrix} 0\cdots0 & 1 & *\cdots* & * & *\cdots* & * & *\cdots* \\ 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* & * & *\cdots* \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 1 & *\cdots* \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 & 0 & 0\cdots0 \end{pmatrix}$$
$$\begin{array}{cccccc} & j_1 & & j_2 & \cdots & j_r \end{array}$$

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 $a_{i,j_i} = 1$. Bovendien is $j_1 < j_2 < \ldots < j_r$.

gereduceerde 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 $i \geqslant r$ 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).

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

$$x \in \ker(a\cdot) \quad \Leftrightarrow \quad \begin{cases} x_1 & +2x_2 & & & & +x_6 & -3x_7 & = 0 \\ & & x_3 & -x_4 & & -x_6 & +2x_7 & = 0 \\ & & & & x_5 & +x_6 & +x_7 & = 0 \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} x_1 & = & -2x_2 & +0x_4 & -x_6 & +3x_7 \\ x_3 & = & & x_4 & +x_6 & -2x_7 \\ x_5 & = & & & -x_6 & -x_7 \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} x_1 & = & -2x_2 & +0x_4 & -x_6 & +3x_7 \\ x_2 & = & x_2 & & & \\ x_3 & = & & x_4 & +x_6 & -2x_7 \\ x_4 & = & & x_4 & & \\ x_5 & = & & & -x_6 & -x_7 \\ x_6 & = & & & x_6 & \\ x_7 & = & & & & x_7 \end{cases}$$

$$\Leftrightarrow \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = x_2\cdot \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_4\cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_6\cdot \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} + x_7\cdot \begin{pmatrix} 3 \\ 0 \\ -2 \\ 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}.$$

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

vrije variabele
afhankelijke variabele

$$p\colon F^7 \to F^4, \quad (x_1,x_2,x_3,x_4,x_5,x_6,x_7) \mapsto (x_2,x_4,x_6,x_7)$$

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 $\ker(a\cdot)$ uit rijtrapvorm

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 $n-r$ vectoren

$$w_k = e_k - \sum_{\substack{1 \leqslant i \leqslant r \\ j_i < k}} a_{i,k} e_{j_i}, \qquad \text{voor } k \in \{1,\ldots,n\} \setminus \{j_1,\ldots,j_r\}$$

een basis van $\ker(a\cdot)$.

Bewijs. Het bewijs kan geheel analoog aan het bewijs in Voorbeeld VII.5.7 gevoerd worden. ∎

inhomogeen stelsel lineaire vergelijkingen

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:

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n &= b_1 \\ \quad\vdots & \vdots \quad \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n &= b_m \end{cases} \qquad \text{met de } a_{i,j} \text{ en de } b_i \text{ in } F.$$

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 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*.

strijdig stelsel

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.

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:

$$\begin{array}{cccc} x_1 & & +3x_3 & +x_4 = 1 \\ & x_2 & +2x_3 & +x_4 = 2. \end{array}$$

Een particuliere oplossing is dan $(1,2,0,0)$ (gebruik de *niet* vrije variabelen x_3 en x_4), en een basis van de oplossingsruimte van het homogene stelsel is

$$((-3,-2,1,0),(-1,-1,0,1))$$

(zie Voorbeeld VII.5.3). De oplossingsruimte is dus

$$\{(1,2,0,0) + \lambda\cdot(-3,-2,1,0) + \mu\cdot(-1,-1,0,1) : \lambda,\mu \in \mathbb{Q}\},$$

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. Vervolgens 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:

$$\left(\begin{array}{cccc|c} -1 & 2 & 1 & 1 & 1 \\ 1 & -1 & 1 & 0 & 1 \\ 2 & -3 & 0 & -1 & 1 \end{array}\right) \begin{array}{r} -R_1 \\ R_2 \\ R_3 \end{array} \rightsquigarrow \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 \\ 2 & -3 & 0 & -1 & 1 \end{array}\right)$$

$$\begin{array}{r} R_1 \\ R_2 - R_1 \\ R_3 - 2R_1 \end{array} \rightsquigarrow \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -1 \\ 0 & 1 & 2 & 1 & 2 \\ 0 & 1 & 2 & 1 & 3 \end{array}\right)$$

$$\begin{array}{r} R_1 \\ R_2 \\ R_3 - R_2 \end{array} \rightsquigarrow \left(\begin{array}{cccc|c} 1 & -2 & -1 & -1 & -1 \\ 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

Het stelsel $a \cdot x = b$ is strijdig, want de laatste vergelijking is $0 = 1$. Er zijn dus geen oplossingen. ∎

Opgaven

S **1.** 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.

$$\begin{cases} 2x_1 + 3x_2 - 2x_3 = 0 \\ 3x_1 + 2x_2 + 2x_3 = 0 \\ -x_2 + 2x_3 = 0 \end{cases}$$

$$\begin{cases} 2x_1 + 3x_2 - 2x_3 = 1 \\ 3x_1 + 2x_2 + 2x_3 = -1 \\ -x_2 + 2x_3 = -1 \end{cases}$$

$$\begin{cases} 2x_1 + 3x_2 - 2x_3 = 1 \\ 3x_1 + 2x_2 + 2x_3 = 1 \\ -x_2 + 2x_3 = 1 \end{cases}$$

$$\begin{cases} 3x_1 + x_2 + 2x_3 - 2x_4 = 1 \\ 2x_1 - x_2 + 2x_3 = 2 \\ x_1 + x_3 = 3 \\ -2x_1 - x_2 - x_3 + x_4 = 4 \end{cases}$$

S **2.** 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.

V **3.** Bereken hoeveel rij-operaties maximaal gedaan moeten worden om een m bij n matrix in rijtrapvorm te krijgen. En idem met gereduceerde rijtrapvorm.

S **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:

$$a\cdot C_7H_5N_3O_6 \to b\cdot N_2 + c\cdot H_2O + d\cdot CO + e\cdot C.$$

V **5.** Laat $F = \mathbb{Q}$. Bepaal in F^3 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 $(2,2,2)$.

B **6.** Laat $n \in \mathbb{N}$, 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?)

B **7.** 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 $a'_{1,1}|a'_{2,2}|\cdots|a'_{n,n}$.

✯ **8.** (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...

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 dat het lineaire karakter van een probleem niet meteen duidelijk is. Een voorbeeld daarvan is het spel 'lights out'.

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 diens 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 $(2,2)$:
$$\begin{array}{|ccccc|}\hline 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ \hline\end{array} \quad\rightsquigarrow\quad \begin{array}{|ccccc|}\hline 0&1&0&0&0\\ 1&1&1&0&0\\ 0&1&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ \hline\end{array}$$

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 $f_{i,j}\in V$:

$$\begin{aligned} f_{i,j}(k,l) &= 1 \quad \text{als } |k-i|+|l-j|\leqslant 1\\ &= 0 \quad \text{anders.}\end{aligned}$$

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

Lineaire algebra houdt niet op bij de in dit dictaat behandelde stof, eigenlijk hebben we alleen een flink stuk gedaan van wat vaak in een eerste lineaire algebra college wordt behandeld. We proberen hier een opsomming te geven van de belangrijkste zaken die normaliter in twee colleges lineaire algebra worden behandeld en die hier ontbreken. De dictaten [vL] en [St2] van de Leidse college's 'Linear Algebra I' en 'Linear Algebra II' bevatten dit alles, en de betreffende secties zijn makkelijk te herkennen aan de titels. Suggesties voor een goed boek over dit materiaal dat gratis online beschikbaar is zijn welkom.

som

directe som

Somruimte. Laat F een lichaam zijn en V een F-vectorruimte. De *som* van 2 deelruimten U en W is de deelverzameling $U+W:=\{u+w : u\in U, w\in W\}$. De som heet *direct* als $U\cap W=\{0\}$. Een directe som wordt ook genoteerd als $U\oplus W$, en in dat geval is de afbeelding $U\times W\to U\oplus W$, $(u,w)\mapsto u+w$ een isomorfisme.

Als $V = U \oplus W$ zeggen we dat V ontbonden is als directe som van U en W. In de praktijk kunnen zulke ontbindingen nuttig zijn, omdat de dimensies van U en W kleiner zijn dan die van V (als U en V beide niet nul zijn). Als bijvoorbeeld $f: V \to V$ een lineaire afbeelding is en $V = U \oplus W$ en $f(U) \subseteq U$ en $f(W) \subseteq W$, dan is de matrix van f ten opzichte van een basis van V de afkomt van bases van U en W in blokvorm.

determinant

Determinant. Voor iedere n is er de functie *determinant* $\det: \mathrm{M}_n(F) \to F$ met allerlei wonderlijke en nuttige eigenschappen. Als $F = \mathbb{R}$ dan is $\det(a)$ het georiënteerde volume van het parallellepipedum in $\mathbb{R}^n$ opgespannen door de kolommen van a, en ook is het zo dat voor p een parallellepipedum in $\mathbb{R}^n$ het georiënteerde volume van $a \cdot p$ gelijk is aan $\det(a)$ maal dat van p. Een eerste eigenschap is dat voor $a \in \mathrm{M}_n(F)$ geldt a inverteerbaar is precies dan als $\det(a)$ dat is, en als a inverteerbaar is dan kunnen de coëfficiënten van a^{-1} in determinanten worden uitgedrukt en krijgt men dus een formule voor de oplossing van een inhomogeen stel lineaire vergelijkingen $ax = b$, als a inverteerbaar is:

regel van Cramer

de *regel van Cramer*.

Eigenwaarden. Laat f een endomorfisme zijn van een eindig dimensionale vectorruimte V. Dan wil men graag een basis v van V hebben zodat ${}_v\mathrm{mat}(f)_v$

diagonaliseren

diagonaal is: alle coëfficiënten buiten de diagonaal zijn nul. Dit is het geval precies dan als de basisvectoren v_i de eigenschap hebben dat er $\lambda_i \in F$ bestaan

eigenvector
eigenwaarde

zodat $f(v_i) = \lambda_i v_i$: iedere v_i is een *eigenvector*, met *eigenwaarde* λ_i. Zo'n basis bestaat niet altijd, om 2 verschillende redenen. Ten eerste kan het nodig zijn om F uit te breiden om de nodige λ_i te krijgen: de λ_i zijn de nulpunten, in een

karakteristiek polynoom

algebraïsche afsluiting van F, van het *karakteristieke polynoom* $\det(a - \lambda \mathrm{id}_V)$ in $F[\lambda]$. Ten tweede kan het gebeuren dat zelfs als alle mogelijke eigenwaarden in F zitten, er geen basis van eigenvectoren is. In dat geval is er een andere

Jordanvorm

optimale vorm die men kan krijgen, de zogenaamde *Jordanvorm*: buiten de diagonaal staan overal nullen, behalve wat enen die vlak boven de diagonaal mogen staan.

Standaard inproduct. Vanaf hier is F gelijk aan $\mathbb{R}$ of $\mathbb{C}$. Op $\mathbb{R}^n$ hebben we het

standaard inproduct

standaard inproduct:

$$\langle , \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}, (x, y) \mapsto \langle x, y \rangle = \sum_i x_i y_i.$$

En op $\mathbb{C}^n$ hebben we

$$\langle , \rangle : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}, (x, y) \mapsto \langle x, y \rangle = \sum_i x_i \overline{y_i}.$$

In beide gevallen hebben we dat voor alle x in $\mathbb{R}^n$ (of $\mathbb{C}^n$) $\langle x, x \rangle$ in $\mathbb{R}_{\geqslant 0}$ ligt, en nul is precies dan als x nul is: het inproduct is *positief definiet*. Men definieert

norm, afstand
hoek

dan de *norm* van x als $\|x\| := \sqrt{\langle x, x \rangle}$, alsook de *afstand* tussen x en y als $\|y - x\|$, en (als x en y beide niet 0 zijn) de *hoek* (op teken na) tussen x en y door

$$\cos(\phi) = \frac{\langle x, y \rangle}{\|x\| \cdot \|y\|}.$$

Cauchy–Schwartz ongelijkheid

De *Cauchy–Schwarz ongelijkheid* zegt inderdaad dat $|\langle x, y \rangle| \leqslant \|x\| \cdot \|y\|$. In het bijzonder zegt men dat x en y loodrecht op elkaar staan, ofwel orthogonaal zijn, precies dan als $\langle x, y \rangle = 0$.

orthogonale basis
orthonormale basis

Een basis $v = (v_1, \ldots, v_n)$ heet *orthogonaal*als voor alle i en j met $i \neq j$ geldt dat $\langle v_i, v_j \rangle = 0$, en *orthonormaal* als bovendien voor alle i geldt dat $\|v_i\| = 1$. De standaardbasis is orthonormaal.

Inproducten. Als V een n-dimensionale vectorruimte is, dan definieert men het

inproduct

begrip *inproduct* op V als een functie $\langle , \rangle : V \times V \to F$ die een aantal van de eigenschappen van het standaardinproduct heeft, en alles wat hierboven voor $\mathbb{R}^n$

Gram–Schmidt orthogonalisatie

en $\mathbb{C}^n$ is gezegd kan dan gegeneraliseerd worden. Het *Gram–Schmidt orthogonalisatieproces* geeft het bestaan van orthonormale bases.

Vanaf hier is V een eindig dimensionale F-vectorruimte en is $\langle , \rangle$ een inproduct op V.

orthogonale afbeelding

Een lineaire afbeelding $f : V \to V$ heet *orthogonaal* als voor alle $x, y \in V$ geldt $\langle f(x), f(y)\rangle = \langle x, y\rangle$, dit zijn de lineaire afstandsbehoudende afbeeldingen. Als $F = \mathbb{C}$ dan kunnen zulke f gediagonaliseerd worden met een orthonormale basis van eigenvectoren, en de eigenwaarden hebben absolute waarde 1. Als $F = \mathbb{R}$ kan men een orthonormale basis vinden zodat de matrix van f bestaat uit 1 bij 1 en 2 bij 2 blokken langs de diagonaal.

zelfgeadjungeerd

Een lineaire afbeelding $f : V \to V$ heet *zelfgeadjungeerd* als voor alle $x, y \in V$ geldt $\langle f(x), y\rangle = \langle x, f(y)\rangle$. Dit is equivalent met: de matrix van f ten opzichte van een orthonormale basis is de complex geconjugeerde van zijn getransponeerde. Zo'n endomorfisme kan gediagonaliseerd worden met een orthonormale basis van eigenvectoren, zowel voor $F = \mathbb{R}$ als $F = \mathbb{C}$.

VIII APPENDIX

VIII.1 Redeneerregels

Zoals beloofd in Sectie II.3 geven we hier een verzameling 'redeneerregels' waaruit elk bewijs kan worden opgebouwd. Het zijn zogezegd de basisstappen van bewijzen, ofwel, de atomen van *deductie*. De situatie is als volgt: we hebben een lijst gegeven aannames, en het gaat er nu om wat we daaruit kunnen afleiden.

deductie

We beginnen met de regels waarin geen kwantoren voorkomen, d.w.z., de regels voor deductie in propositielogica. De symbolen die we daar gebruiken zijn $\wedge$, $\vee$, $\neg$, $\Rightarrow$, en $\Leftrightarrow$. Voor elk van deze symbolen krijgen we nu *introductieregels* en *eliminatieregels*. Als we ons hadden beperkt tot minder symbolen (bijvoorbeeld tot $\wedge$ en $\neg$) dan zouden we ook minder redeneerregels nodig hebben.

∧-introductie **$\wedge$-introductie.** Uit P en Q mag je $P \wedge Q$ concluderen: als je in je bewijs al P en Q hebt afgeleid uit de gegeven aannames, dan mag je $P \wedge Q$ toevoegen aan de lijst van gevolgen van de gegeven aannames. De toelichting die je hierbij moet geven zijn de plaatsen waar P en Q staan (zeg hun regelnummers), en dat je een $\wedge$-introductie daarop uitvoert.

∧-eliminatie **$\wedge$-eliminatie.** Uit $P \wedge Q$ mag je P concluderen, en ook Q.

∨-introductie **$\vee$-introductie.** Uit P mag je $P \vee Q$ concluderen, en uit Q mag je $P \vee Q$ concluderen.

∨-eliminatie **$\vee$-eliminatie.** Als je R uit P en de gegeven aannames kan afleiden, en R uit Q en de gegeven aannames kan afleiden, dan volgt R uit $P \vee Q$ en de gegeven aannames: je kan $(P \vee Q) \Rightarrow R$ toevoegen aan de lijst gevolgen van de gegeven aannames. De proposities P en Q worden gezien als tijdelijke extra aannames die je na gebruik weer weggooit. De afleidingen van R uit P en van R uit Q zijn te vergelijken met een subroutine van een programma, ze worden uitgevoerd op een aparte lijst.

¬-introductie **$\neg$-introductie.** Als je uit P en de gegeven aannames een tegenspraak kan afleiden, zeg Q en ook $\neg Q$ voor een bepaalde Q, dan mag je $\neg P$ concluderen.

¬-eliminatie **$\neg$-eliminatie.** Uit $\neg\neg P$ mag je P concluderen. Samen met de vorige regel geeft dit het principe van 'bewijs uit het ongerijmde.' Om P te bewijzen is het voldoende om uit $\neg P$ en de gegeven aannames een tegenspraak af te leiden: pas de vorige regel toe op $\neg P$, dan mogen we $\neg\neg P$ concluderen, en volgens deze regel dus ook P.

⇒-introductie **$\Rightarrow$-introductie.** Als je Q kan afleiden uit P en de gegeven aannames dan mag je $P \Rightarrow Q$ toevoegen aan de lijst gevolgen van de gegeven aannames.

⇒-eliminatie **$\Rightarrow$-eliminatie.** Uit P en $P \Rightarrow Q$ mag je Q concluderen.

⇔-introductie **$\Leftrightarrow$-introductie.** Uit $P \Rightarrow Q$ en $Q \Rightarrow P$ mag je $P \Leftrightarrow Q$ concluderen.

⇔-eliminatie **$\Leftrightarrow$-eliminatie.** Uit $P \Leftrightarrow Q$ mag je $P \Rightarrow Q$ concluderen, en ook $Q \Rightarrow P$.

Dan zijn nu de regels voor de kwantoren $\forall$ en $\exists$ aan de beurt.

∀-introductie **$\forall$-introductie.** Als je uit de gegeven aannames kan afleiden dat $x \in U \Rightarrow P(x)$, dan mag je $\forall_{x \in U} P(x)$ concluderen.
Er is hier wel een beperking: de variabele x moet 'nieuw' zijn, d.w.z., mag niet eerder in het bewijs voorkomen. Zo'n restrictie is nodig, intuïtief gezegd, om ervoor te zorgen dat x alle elementen van U kan doorlopen, anders gezegd, er mogen geen beperkingen op x zijn, x moet een 'willekeurig element van U' zijn. Voor een preciese uitspraak verwijzen we naar het boek [Da, §3.8]. We zitten hier in een situatie waar het formaliseren vrij technisch is.

∀-eliminatie **$\forall$-eliminatie.** Uit $\forall_{x \in U} P(x)$ mag je $t \in U \Rightarrow P(t)$ concluderen.
De intuïtieve betekenis is duidelijk: als we weten dat voor alle $x \in U$ geldt dat $P(x)$, en t is een element van U, dan geldt $P(t)$.
Hier is t een 'term' waarvoor moet gelden dat door de substitutie van x door t in $P(x)$ geen variabele van t 'gebonden' wordt. Hieraan is bijvoorbeeld voldaan als geen enkele variabele die in t voorkomt in $P(x)$ voorkomt.

Er is ook een regel voor $\exists$-introductie, en een regel voor $\exists$-eliminatie. Voor details verwijzen we naar [Da, §3.9].

∃-introductie **$\exists$-introductie.** Uit $t \in U \wedge P(t)$ mag je concluderen dat $\exists_{x \in U} P(x)$.

∃-eliminatie **$\exists$-eliminatie.** Uit $\exists_{x \in U} P(x)$ en $(x \in U \wedge P(x)) \Rightarrow Q$ kan je de conclusie Q trekken.

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 [DDS], waar deze beschrijving deels op is geïnspireerd. Merk op dat we nu heel formeel worden: we beginnen zelfs met een exacte beschrijving van de *taal* van uitspraken (formules) in de verzamelingentheorie.

symbolen

In de verzamelingenleer gebruiken we als *symbolen* 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).

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.

ZFC 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

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

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

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 $\bigcup_{Y \in A} Y$.

machtsverzameling

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

Afscheiding. Dit is een *axiomaschema*. 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

$$\forall_A \exists_B \forall_X (X \in B \Leftrightarrow (X \in A \wedge \varphi)).$$

Deze verzameling noteren we als $\{X \in A : \varphi\}$.

substitutie

Substitutie. Dit is ook een axiomaschema. 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

$$\big(\forall_X \exists!_Y \varphi\big) \Rightarrow \forall_A \exists_B \forall_Y \big(Y \in B \Leftrightarrow \exists_X (X \in A \wedge \varphi)\big).$$

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

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 $S : A \to A$, $X \mapsto X \cup \{X\}$ is injectief maar niet surjectief.

regulariteit

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 verzamelingen van de vorm $X_0 \ni X_1 \ni X_2 \ni \cdots$.

keuzeaxioma

Keuzeaxioma. Elke verzameling S van niet-lege verzamelingen heeft een keuzefunctie, dat wil zeggen, er is een functie $f : S \to \bigcup_{X \in S} X$ 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 $S : \mathbb{N} \to \mathbb{N}$ 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:

opvolger

(a) een verzameling $\mathbb{N}$;
(b) een element $0 \in \mathbb{N}$;
(c) een afbeelding $S : \mathbb{N} \to \mathbb{N}$.

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 $A = \mathbb{N}$.

inductie

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 $f : \mathbb{N} \to \mathbb{N}'$ zodat $f(0) = 0'$, en zodat voor alle $a \in \mathbb{N}$ geldt $f(S(a)) = S'(f(a))$.

Bewijs. Eerst een opmerking: we hebben de recursiestelling (Stelling IV.3.1) bewezen voor de natuurlijke getallen zoals gedefinieerd in Paragraaf IV.1. Deze geldt echter ook voor het Peano-systeem $(\mathbb{N}, 0, S)$, als we overal $n+1$ vervangen door $S(n)$. Het bewijs is hetzelfde.

We definiëren dus een afbeelding $f : \mathbb{N} \to \mathbb{N}'$ 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 $f : \mathbb{N} \to \mathbb{N}'$ 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 $f' : \mathbb{N}' \to \mathbb{N}$ met $f(0') = 0$ en met $\forall_a (a \in \mathbb{N}' \Rightarrow f'(S'(a)) = S(f'(a)))$.

Voor de samenstelling $f' \circ f : \mathbb{N} \to \mathbb{N}$ 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. ∎

constructie van $(\mathbb{N}, 0, 1, +, \cdot)$

Voorts kan men dan, gebruikmakend van de recursiestelling, bewijzen dat er unieke afbeeldingen $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ en $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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.

optelling

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 $s_b(a)$:

$$a + b := s_b(a).$$

■

vermenigvuldiging

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 '$\forall_{a\in\mathbb{N}}\ a+b=b+a$'. 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

$$\begin{aligned} 1{\cdot}b = S(0){\cdot}b &\quad \text{definitie van } 1\\ S(0){\cdot}b = 0{\cdot}b + b &\quad \text{P6 met } 0 \text{ en } b\\ 0{\cdot}b + b = 0 + b &\quad \text{P5 met } b, \text{ dan } +b\\ 0 + b = b &\quad \text{P3 met } b. \end{aligned}$$

■

constructie van $(\mathbb{N},0,S)$

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 met de eigenschap 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

$$\varnothing A \text{ en } \forall_X,\ X \in A \Rightarrow X \cup \{X\} \in A$$

geldt dat $\mathbb{N} \subseteq A$, dus $A = \mathbb{N}$ want de andere inclusie hadden we al. ∎

Antwoorden en uitwerkingen

Paragraaf I.1.

1. (a) 12;
(b) 3;
(c) 1;
(d) 1;
(e) 2.

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.

6. (a) $\{0,1\}$, $\{0\}$, $\{1\}$, $\varnothing$;
(b) $\{0,1,2\}$, $\{0,1\}$, $\{0,2\}$, $\{1,2\}$, $\{0\}$, $\{1\}$, $\{2\}$, $\varnothing$;
(c) $\{0,1,2,3\}$, $\{0,1,2\}$, $\{0,1,3\}$, $\{0,2,3\}$, $\{1,2,3\}$, $\{0,1\}$, $\{0,2\}$, $\{0,3\}$, $\{1,2\}$, $\{1,3\}$, $\{2,3\}$, $\{0\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\varnothing$.
(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 A verdubbelt als je een element toevoegt aan A.

7. $\mathscr{P}(A) = \{\{0,1\},\{0\},\{1\},\varnothing\}$ ($2^2 = 4$ 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).

8. De voorwaarde is: $A = \varnothing$ 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 $B \neq \varnothing$).

Paragraaf I.2.

3. (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 $\bigcap_{k\in K} A_k = (4,\infty)$.

4. (a) $[1,2] = \{x \in \mathbb{R} : 1 \leqslant x \leqslant 2\}$.
(b) $(0,3) = \{x \in \mathbb{R} : 0 < x < 3\}$.

5. (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:

$$\begin{aligned} x &\in \Omega \setminus (A \cup B) \\ x &\notin A \cup B && \text{vanwege definitie van complement,} \\ x \notin A \quad &\text{en} \quad x \notin B && \text{definitie vereniging,} \\ x \in \Omega \setminus A \quad &\text{en} \quad x \in \Omega \setminus B && \text{definitie complement,} \\ x &\in (\Omega \setminus A) \cap (\Omega \setminus B) && \text{definitie doorsnede.} \end{aligned}$$

6. (a) $\Omega \setminus (A \cap B \cap C) = (\Omega \setminus A) \cup (\Omega \setminus B) \cup (\Omega \setminus C)$.
(b) $\Omega \setminus (A \cup B \cup C) = (\Omega \setminus A) \cap (\Omega \setminus B) \cap (\Omega \setminus C)$.

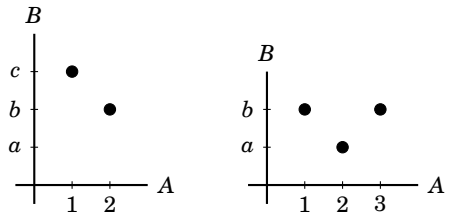
8. (a) Deze vraag is niet precies geformuleerd. Maar er geldt dat $(A \cup B) \setminus (A \cup C) \subseteq A \cup (B \setminus C)$, en dat $(A \cup (B \setminus C)) \setminus ((A \cup B) \setminus (A \cup C)) = A$ (gebruik een venndiagram).
(b) Precies dan als $A = \varnothing$.

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:

$$\begin{aligned} & x \in (A \cap B \cap C^c) \cup (A \cap B \cap D^c) \cup (A \cap B \cap C \cap D) \\ & \big(x \in A \cap B \wedge x \in C^{\mathrm{c}}\big) \vee \big(x \in A \cap B \wedge x \in D^{\mathrm{c}}\big) \vee \big(x \in A \cap B \wedge x \in C \cap D\big) \\ & \big(x \in A \cap B\big) \wedge \big(x \in C^{\mathrm{c}} \vee x \in D^{\mathrm{c}} \vee x \in C \cap D\big) \\ & (x \in A \cap B) \wedge x \in \big((C^{\mathrm{c}} \cup D^{\mathrm{c}} \cup (C \cap D)\big) \\ & (x \in A \cap B) \wedge x \in \Omega \\ & x \in A \cap B\,. \end{aligned}$$

Paragraaf I.3.

1.



2. $f(0) = 1$, $f(1/x) = (x-1)/(x+1)$, $1/f(x) = (1+x)/(1-x)$.

3. (a) $f(x) = x^2 - 7x + 7$;
(b) $f(x) = 1/x + \sqrt{1+x^2}/|x|$.

4. $\{\pm\sqrt{k\pi} : k \in \mathbb{N}\}$; $\{\pm\sqrt{3\pi/2 + 2k\pi} : k \in \mathbb{N}\}$; $\varnothing$.

5. (a) nee;
(b) ja;
(c) nee;
(d) ja.

6. (a) 9.
(b) 1.
(c) 0 als A niet leeg is en 1 als A wel leeg is.

10. (a) waar;
(b) niet waar;
(c) niet waar;
(d) waar.

14. (b) $B = (-5, -4]$, $g^{-1}(x) = 1/(x+5)$

15. (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.

2. (a) $(P \vee Q) \wedge \neg(P \wedge Q)$, bewijs: waarheidstabel.
(b) $(P \veebar Q) \veebar (P \wedge Q)$, bewijs: waarheidstabel.

Paragraaf II.2.

1. (a) $\exists_{n\in\mathbb{Z}}(x = n + n)$.
(b) $(\neg(x = 0)) \wedge (\neg(x = 1)) \wedge (\forall_{r\in\mathbb{N}} \forall_{s\in\mathbb{N}}(x = r{\cdot}s \Rightarrow (r = 1 \vee s = 1)))$.

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.

2. (a) $(2xy) + (5x) + (3y) + 4$.
(b) Nu moet je een volgorde kiezen, bijvoorbeeld van links naar rechts:

$$((((2x)y) + (5x)) + (3y)) + 4.$$

5. (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 $a \uparrow b = a^{(a^{b-1})}$ en dit kan dus gewoon in de bekende notatie worden uitgedrukt.

7. $(a + b)^c = a^c + b^c$. 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!)

9. 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 III.3.

Paragraaf IV.1.

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 $b = b'$.

3. De transitiviteit is het makkelijkst. Laat a, b en c in $\mathbb{N}$, met $a \leqslant b$ en $b \leqslant c$. Dan zijn er n en m in $\mathbb{N}$ met $a+n = b$ en $b+m = c$. Dan ook $n+m \in \mathbb{N}$, en $a+(n+m) = (a+n)+m = b+m = c$, dus $a \leqslant c$. Laat nu a en b in $\mathbb{N}$ met $a \leqslant b$ en $b \leqslant a$. Dan zijn er n en m in $\mathbb{N}$ met $a+n = b$ en $b+m = a$. Dan hebben we $a+(n+m) = (a+n)+m = b+m = a = a+0$, dus de schrapwet **(N3)** en de commutativiteit van de optelling geven $n+m = 0$. Hieruit volgt dat $n = 0$ en $m = 0$: want als $n \neq 0$ dan geeft Opgave IV.1.1 een n' met $n = n'+1$ en dan is $0 = n+m = (n'+m)+1$ in tegenspraak met Axioma **(N5)**, en net zo als $m \neq 0$. Dus $a = b$. Voor $a \in \mathbb{N}$, laat $P(a)$ de uitspraak zijn: $\forall_{b \in \mathbb{N}}\, b \leqslant a \vee a \leqslant b$. We bewijzen dat $P(a)$ voor alle $a \in \mathbb{N}$ waar is, met inductie. De uitspraak $P(0)$ is waar, want voor alle $b \in \mathbb{N}$ geldt dat $0+b = b$, dus $0 \leqslant b$. Laat nu $a \in \mathbb{N}$ en neem aan dat $P(a)$ geldt. We bewijzen $P(a+1)$. Laat $b \in \mathbb{N}$. Dan $b \leqslant a$ of $a \leqslant b$. Als $b \leqslant a$ dan ook $b \leqslant a+1$. Als $b = a$ dan $b \leqslant a+1$. Als $a \leqslant b$ en $b \neq a$, dan is er een $n \in \mathbb{N}$ met $a+n = b$ en $n \neq 0$. Opgave IV.1.1 geeft een $n' \in \mathbb{N}$ met $n = n'+1$. Dan geldt $(a+1)+n' = a+n = b$, dus $a+1 \leqslant b$. We hebben $P(a+1)$ bewezen, en het inductiebewijs is af.

Paragraaf IV.2.

1. $(n+1)^2$.

6. Nee.

7. 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.

13. 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. Het volgt dat ook het getal $7 \cdot 11^n + 4 \cdot (11^n - 4^n)$ deelbaar is door 7.

Paragraaf IV.3.

Paragraaf V.1.

2. 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).

7. Zij $f : R \to S$ een bijectief homomorfisme van ringen. Omdat f bijectief is, bestaat er een inverse functie $f^{-1} : S \to R$; 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.

5. 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 $D_b \cap D_r = D_a \cap D_b$.

7. 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.

10. 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.

11. (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 $i + j = \min(i,j) + \max(i,j)$.

12. 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.

13. (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}).

14. (a) Er geldt $54 = 2 \cdot 3^3$. Iedere positieve 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) Er geldt $200 = 2^3 5^2$.

$\times$	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.

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 $(a,c) \sim (e,f)$.

3. 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.

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 de 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 $1/(n+1) \leqslant 1/(N+1) < \varepsilon$. 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. Zij $\varepsilon > 0$. Kies $N_1 \in \mathbb{N}$ zó dat voor alle $n \geqslant N_1$ geldt dat $|x_{2n} - x| < \varepsilon$. Kies $N_2 \in \mathbb{N}$ zó dat voor alle $n \geqslant N_2$ geldt dat $|x_{2n+1} - x| < \varepsilon$. Kies $N = 1 + 2\max\{N_1, N_2\}$. Kies $k \geqslant N$ 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 $n \geqslant N/2 \geqslant N_1$ en dus

$$|x_k - x| = |x_{2n} - x| < \varepsilon.$$

(2): Laat $k = 2n+1$ met $n \geqslant 1$, dan geldt $n \geqslant N/2 \geqslant N_2$ en dus

$$|x_k - x| = |x_{2n+1} - x| < \varepsilon.$$

Dit bewijst dat $\lim_{k\to\infty} x_k = x$.

11. (a) *Aanwijzing*: Redeneer uit het ongerijmde.

12. (a) Neem aan dat $|x| > 1$. We definiëren $h := |x| - 1$. Dan geldt $h > 0$ en $|x| = 1 + h$. Uit het binomium van Newton (Stelling IV.2.3) volgt dat

$$|x^n| = |x|^n = (1+h)^n \geqslant 1 + nh.$$

Hier volgt dat $(x^n)_{n\geqslant 0}$ niet begrensd is, en dus divergent.
(b) Vergelijk Opgave VI.2.8.
(c) Zie Opgave VI.2.3.
(d) Zie Voorbeeld VI.2.3(c).

Paragraaf VI.3.

1. (a) $0,\overline{27}$; (b) $0,\overline{230769}$; (c) $0,6\overline{32}$; (d) $5,\overline{0}$

2. (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.

Paragraaf VI.6.

Paragraaf VI.7.

1. (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

$$|x^2 - c^2| < 3c \cdot |x - c| < 3c \cdot \delta \leqslant 3c \cdot \frac{\varepsilon}{3c} = \varepsilon.$$

2. (a) Waar.
(b) Niet waar.

8. Ja.

11. (a) 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) We laten zien dat f niet continu is in 0. We moeten een $\varepsilon > 0$ geven, zodat voor alle $\delta > 0$ er een $x \in (-1,1)$ is met $|x| < \delta$ en $|f(x) - f(0)| \geqslant \varepsilon$. Omdat f in de buurt van 0 '1 verspringt,' nemen we $\varepsilon = 1/2$ (als we het echt scherp wilden spelen dan konden we $\varepsilon = 1$ nemen). Laat nu $\delta > 0$. We nemen $x = \min(\delta/2, 1/2)$. Dan geldt dat

$$|f(x) - f(0)| = |0 - 1| = 1 \geqslant \frac{1}{2} = \varepsilon\,.$$

13. Beschouw de rij $(1/(n+1))_{n\geqslant 0}$. De rij is in $\mathbb{R} \setminus \{0\}$ en convergeert naar 0 maar

$$(f\left(\frac{1}{n+1}\right))_{n\geqslant 0} = (n+1)_{n\geqslant 0}$$

is niet convergent. Conclusie de limiet bestaat niet.

Paragraaf VI.8.

2. Zij $\varepsilon > 0$ willekeurig. Neem $\delta = \varepsilon/5$. Dan is $\delta > 0$ en voor elke $x, y \in \mathbb{R}$ geldt: als $|x - y| < \delta$ dan

$$\big|f(x) - f(y)\big| = |5x - 5y| = 5|x - y| < 5\delta = 5\frac{\varepsilon}{5} = \varepsilon.$$

3. Voor iedere $\delta > 0$ bestaan twee elementen $x, x' \in (0,\infty)$ zodanig dat $|x - x'| < \delta$ en $|1/x - 1/x'| \geqslant 1$. Inderdaad, gegeven $\delta > 0$ kiezen we $N \geqslant 1$ zo groot dat $1/N < \delta$ en nemen we $x = 1/(N+1)$ en $x' = 1/(N+2)$. Hieruit volgt dat de functie $1/x$ niet uniform continu is op $(0,\infty)$.

5. (b) Aangezien f en g begrensd zijn kunnen we $M_1, M_2 > 0$ vinden zó dat voor alle $x \in A$ geldt dat $|f(x)| \leqslant M_1$ en $|g(x)| \leqslant M_2$. Zij $\varepsilon > 0$ willekeurig. Aangezien f uniform continu is kunnen we een $\delta_1 > 0$ vinden zó dat voor alle $x, y \in A$ met $|x - y| < \delta_1$ geldt dat $|f(x) - f(y)| < \frac{\varepsilon}{2M_2}$. Wegens de uniforme continuïteit van g vinden we een $\delta_2 > 0$ zó dat voor alle $x, y \in A$ met $|x - y| < \delta_2$ geldt dat $|f(x) - f(y)| < \frac{\varepsilon}{2M_1}$. Definieer $\delta = \min\{\delta_1, \delta_2\}$. Kies $x, y \in A$ met $|x - y| < \delta$. Uit de driehoeksongelijkheid en bovenstaande volgt dat

$$\begin{aligned}
|h(x) - h(y)| &= |f(x)g(x) - f(y)g(y)| \\
&\leqslant |f(x)g(x) - f(x)g(y)| + |f(x)g(y) - f(y)g(y)| \\
&= |f(x)|\,|g(x) - g(y)| + |g(y)|\,|f(x) - f(y)| \\
&< M_1\,\frac{\varepsilon}{2M_1} + M_2\,\frac{\varepsilon}{2M_2} = \varepsilon.
\end{aligned}$$

9. Aanwijzing: Neem een rij $(x_n)_{n\geqslant 1}$ in $(0,1]$ met $\lim\limits_{n\to\infty} x_n = 0$. Toon aan dat $(f(x_n))_{n\geqslant 1}$ een cauchy-rij is. Met de compleetheid van $\mathbb{R}$ geeft dit een kandidaat voor een limiet.

Paragraaf VII.1.

2. (a) Dit is recht-toe-recht-aan.
(b) Voor alle $f \in V$ en voor alle $x \in X$: $(-f)(x) = -f(x)$.
(c) Als $V \neq \{0\}$ (dus als $X \neq \varnothing$) 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 $f^{-1} : \mathbb{R} \to V$, $x \mapsto x + 1$. Er geldt $f(0_V) = 0$, voor alle v en w in V geldt $v +_V w = f^{-1}(f(v) + f(w))$, en voor alle $\lambda \in \mathbb{R}$ en $v \in V$ geldt $\lambda \cdot_V v = f^{-1}(\lambda f(v))$. Dus V is gewoon de vectorruimte $\mathbb{R} = \mathbb{R}^1$, op wat administratie na.

Paragraaf VII.2.

6. Dat is de unieke formule die ervoor zorgt dat het matrix product correspondeert met samenstelling van lineaire afbeeldingen.

Paragraaf VII.3.

3. 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.

Tentamen januari 2016

Tentamen Fundamenten, 6 januari 2016, 17:30–20:30
Theo van den Bogaart, Bas Edixhoven

Tentamenstof Fundamenten, najaar 2015

Het hele dictaat, behalve:

- I.5 (smurfenprobleem),
- IV.3 (de recursiestelling),
- VIII (de appendix).

De eerste vereiste is dat je de definities van de gebruikte begrippen kent, en dat je directe toepassingen daarvan beheerst (bv. het geven van eenvoudige bewijzen en voorbeelden). De tweede vereiste is dat je de belangrijkste stellingen kent (de preciese voorwaarden en de conclusie). Als je aan deze twee eisen voldoet dan haal je zeker een voldoende. Om een hoog cijfer te halen moet je ook bewijzen van de moeilijkere stellingen kunnen geven.

Tentamen Fundamenten, 6 januari 2016, 17:30–20:30

Bewijs al je beweringen, dat wil zeggen, geef duidelijke argumenten en schrijf alle stappen op. Schrijf kort, duidelijk en net. Rekenmachines en documenten (bijvoorbeeld het dictaat) zijn niet toegestaan. **Er zijn 7 opgaven**.
Indicatieve normering: 90=10+10+10+15+15+15+15 (de eerste 10 punten zijn gratis).
Tijdsduur: 3 uur. Succes!

1. Laat $A = \{1,2,3\}$.
   (a) Geef een lijst van de elementen van de machtsverzameling $\mathscr{P}(A)$.
   (b) Geef een functie $f : A \to \mathscr{P}(A)$ waarvoor geldt
   $$\{a \in A : a \notin f(a)\} = \{2,3\}.$$

2. (a) Geef een voorbeeld van een propositie $P(x,y)$ zodat geldt
   $$\big(\forall_{x\in\mathbb{R}}\,\exists_{y\in\mathbb{R}}\,P(x,y)\big) \wedge \big(\neg\exists_{y\in\mathbb{R}}\,\forall_{x\in\mathbb{R}}\,P(x,y)\big).$$
   (b) Leg uit dat er geen propositie $Q(x,y)$ bestaat waarvoor geldt
   $$\big(\forall_{x\in\mathbb{R}}\,\exists_{y\in\mathbb{R}}\,\neg Q(x,y)\big) \wedge \big(\exists_{x\in\mathbb{R}}\,\forall_{y\in\mathbb{R}}\,Q(x,y)\big).$$

3. (a) Laat zien dat de operatie $/ : \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} \to \mathbb{Q}_{>0}$ gegeven door $(a,b) \mapsto a/b$ *niet* associatief is.
   (b) Geef een voorbeeld van een verzameling A en een operatie $\bigcirc : A \times A \to A$ die *wel* associatief maar *niet* commutatief is (hint: van welke operaties weet je dat ze associatief zijn?).

4. Bewijs met volledige inductie dat voor alle $n \in \mathbb{N}$ geldt
   $$\sum_{i=0}^{n} i(3i-1) = n^2(n+1).$$

5. (a) Bepaal met het euclidisch algoritme gehele getallen x en y zodat $259x + 217y = 7$.
   (b) Schets in hoogstens 10 regels een bewijs voor de stelling van Euclides dat er oneindig veel priemgetallen bestaan.

6. Voor een niet lege, gesloten en begrensde deelverzameling $Z \subset \mathbb{R}$ geldt dat iedere continue functie $f : Z \to \mathbb{R}$ een maximum heeft. (Deze stelling is in het dictaat bewezen.)
   (a) Laat met een voorbeeld zien dat de eis dat Z *gesloten* is noodzakelijk is.
   (b) Laat met een voorbeeld zien dat de eis dat f *continu* is noodzakelijk is.

7. We bekijken de $\mathbb{R}$-vectorruimte V van functies $f : \mathbb{R} \to \mathbb{R}$ met puntsgewijze optelling en met scalairvermenigvuldiging, zoals in het dictaat. Laat W de deelruimte zijn voortgebracht door de elementen $a : x \mapsto 2x - 1$, $b : x \mapsto x + 2$ en $c : x \mapsto -x + 3$.
   (a) Zijn a, b en c afhankelijk?
   (b) Geef een basis van W.
   (c) Laat zien dat de lineaire afbeelding $v_1 : V \to V$, gegeven door $v_1(f) : x \mapsto f(x+1)$ de deelruimte W naar W afbeeldt.
   (d) Geef de matrix van $v_1|_W : W \to W$ ten opzichte van de basis die je in onderdeel (b) hebt gegeven.

Uitwerking Tentamen Fundamenten, 6 januari 2016

1. (a) $\mathscr{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

   (b) We zoeken een $f : A \to \mathscr{P}(A)$ met $1 \in f(1)$, $2 \notin f(2)$ en $3 \notin f(3)$. We mogen zelf kiezen wat $f(1)$, $f(2)$ en $f(3)$ zijn, zolang het maar elementen van $\mathscr{P}(A)$ zijn en aan de drie genoemde voorwaarden is voldaan. Bijvoorbeeld: $f(1) = \{1\}$, $f(2) = \varnothing$ en $f(3) = \varnothing$.

2. (a) We kunnen voor $P(x,y)$ nemen: "$y = x$". Dan is er voor iedere $x \in \mathbb{R}$ een $y \in \mathbb{R}$ (namelijk: $y = x$) zodat $P(x,y)$. En ook is er voor iedere $y \in \mathbb{R}$ een $x \in \mathbb{R}$ met $\neg P(x,y)$ (neem bijvoorbeeld $x = y+1$), dus is er geen $y \in \mathbb{R}$ waarvoor $\forall_{x\in\mathbb{R}} P(x,y)$.

   (b) De negatie van $\exists_{x\in\mathbb{R}} \forall_{y\in\mathbb{R}} Q(x,y)$ is $\forall_{x\in\mathbb{R}} \exists_{y\in\mathbb{R}} \neg Q(x,y)$, dus aan de conjunctie van deze twee is onwaar.
   We kunnen het ook uitwerken, als een bewijs uit het ongerijmde. Stel dat $Q(x,y)$ een propositie is zodat geldt:

   $$\big(\forall_{x\in\mathbb{R}} \exists_{y\in\mathbb{R}} \neg Q(x,y)\big) \wedge \big(\exists_{x\in\mathbb{R}} \forall_{y\in\mathbb{R}} Q(x,y)\big).$$

   Vanwege de rechterkant is er dan een $a \in \mathbb{R}$ zodat voor alle $y \in \mathbb{R}$ geldt dat $Q(a,y)$. Maar volgens de linkerhelft is er voor ieder $x \in \mathbb{R}$ een $y \in \mathbb{R}$ zodat geldt $\neg Q(x,y)$. Dus in het bijzonder is er een $b \in \mathbb{R}$ zodat $\neg Q(a,b)$ geldt. Maar ook geldt $Q(a,b)$ omdat voor alle $y \in \mathbb{R}$ geldt dat $Q(a,y)$. Tegenspraak, en klaar.

3. (a) We hoeven alleen een voorbeeld te geven. Wel, $(1/1)/2 = 1/2$, en $1/(1/2) = 2$, en $1/2 \neq 2$, dus de operatie is niet associatief.

   (b) We kunnen nemen $A = \mathrm{M}_2(\mathbb{R})$ (2 bij 2 matrices met coëfficiënten in $\mathbb{R}$), en als operatie matrixvermenigvuldiging. Dat is associatief (stelling dictaat), maar niet commutatief: $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, terwijl $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$.
   Ook een goed voorbeeld $A = \{f : \mathbb{R} \to \mathbb{R}\}$ (alle functies van $\mathbb{R}$ naar $\mathbb{R}$, met de operatie samenstelling. Een minimaal voorbeeld is $A = \{0,1\}$ met als operatie $a \circ b = a$.

4. Laat, voor $n \in \mathbb{N}$, $P(n)$ de uitspraak zijn: $\sum_{i=0}^{n} i(3i-1) = n^2(n+1)$.

   Stap 1. We bewijzen $P(0)$. $\sum_{i=0}^{0} i(3i-1) = 0\cdot(3\cdot 0 - 1) = 0$. En $0^2(0+1) = 0$. Dus $P(0)$ is waar.

   Stap 2. Laat $n \in \mathbb{N}$, en neem aan dat $P(n)$ geldt. We bewijzen dat $P(n+1)$ geldt.

   $$\begin{aligned}\sum_{i=0}^{n+1} i(3i-1) &= \left(\sum_{i=0}^{n} i(3i-1)\right) + (n+1)(3(n+1)-1) = n^2(n+1) + (n+1)(3n+2)\\ &= (n+1)(n^2+3n+2) = (n+1)(n+1)(n+2) = (n+1)^2((n+1)+1).\end{aligned}$$

   Hier hebben we bij het tweede gelijkheidsteken de inductiehypothese gebruikt. Dus $P(n+1)$ is waar, en het inductiebewijs is af.

5. (a) $259 - 217 = 42$, $217 - 5\cdot 42 = 7$, $42 - 6\cdot 7 = 0$, dus $\gcd(259,217) = 7$. We hebben:

   $$7 = 217 - 5\cdot 42 = 217 - 5\cdot(259 - 217) = 6\cdot 217 - 5\cdot 259.$$

   Controle: $6\cdot 217 = 1302$, $5\cdot 259 = 1295$, $1302 - 1295 = 7$.

   (b) Er zijn priemgetallen, bijvoorbeeld 2, 3. Een manier om te zeggen dat er oneindig veel zijn is dat als je er eindig veel, zeg n, neemt, zeg $p_1, \ldots, p_n$, dat er dan een priemgetal p is dat verschillend is van al deze p_i. Laat p nu de kleinste deler groter dan 1 zijn van $N = p_1 \cdot p_2 \cdots p_n + 1$. Dan is N een veelvoud van p, dus ook van iedere deler d van p, dus iedere deler d van p deelt N. De minimaliteit van p impliceert dat 1 en p de enige delers van p zijn, dus p is een priemgetal. Voor iedere i in $\{1, \ldots, n\}$ is N een p_i-voud plus 1, dus geen van de p_i deelt N, dus geen van de p_i is gelijk aan p.

6. (a) Laat $Z = (0,1]$ (links-open, rechts-gesloten), en laat $f : Z \to \mathbb{R}$, $x \mapsto 1/x$. Dan is f continu, maar niet begrensd (als x van boven naar 0 gaat, dan gaat $f(x)$ naar oneindig). Dus f heeft geen maximum.

   (b) Neem $Z = [0,1]$ en $f : Z \to \mathbb{R}$ gegeven door $f(x) = 1/x$ als $x \neq 0$ en $f(0) = 0$. Nu is Z gesloten, maar f is niet continu in 0. Ook hier is f niet begrensd (op $(0,1]$ is het dezelfde als in het vorige onderdeel). Dus heeft f geen maximum.

7. (a) De vraag is of er $(\lambda,\mu,\nu) \neq (0,0,0)$ in $\mathbb{R}^3$ zijn met $\lambda a + \mu b + \nu c = 0$. Voor alle (λ,μ,ν) in $\mathbb{R}^3$ is de gelijkheid $\lambda a + \mu b + \nu c = 0$ equivalent met:

$$\forall_{x\in\mathbb{R}} (\lambda a + \mu b + \nu c)(x) = 0,$$

   en dat is equivalent met:

$$\forall_{x\in\mathbb{R}}\, \lambda a(x) + \mu b(x) + \nu c(x) = 0,$$

   en dat is na invullen van de definities van a, b en c hetzelfde als:

$$\forall_{x\in\mathbb{R}}\, (-\lambda + 2\mu + 3\nu)\cdot 1 + (2\lambda + \mu - \nu)\cdot x = 0,$$

   en dat is equivalent met:

$$\begin{cases} -\lambda + 2\mu + 3\nu = 0 \\ \quad 2\lambda + \mu - \nu = 0. \end{cases}$$

   Oplossen geeft bijvoorbeeld de oplossing $\lambda = 1$, $\mu = -1$, $\nu = 1$. De elementen a, b en c van V zijn dus afhankelijk (we hebben bijvoorbeeld $b = a + c$).

   (b) W wordt voortgebracht door a en c, en die zijn onafhankelijk want $\lambda a + \nu c = 0$ is equivalent met het stelsel dat we uit het vorige krijgen door $\mu = 0$ in te vullen, en dat heeft alleen $(0,0)$ als oplossing. Dus (a,c) is een basis van W.

   (c) Eerst de rechtstreekse manier. Voor alle $x \in \mathbb{R}$ hebben we

$$(v_1(a))(x) = a(x+1) = 2(x+1) - 1 = 2x + 1.$$

   We zoeken (λ,ν) in $\mathbb{R}^2$ zodat voor alle $x \in \mathbb{R}$ geldt: $2x + 1 = \lambda a(x) + \nu c(x)$. Oplossen geeft $\lambda = 7/5$ en $\nu = 4/5$. Dus $v_1(a) = (7/5)a + (4/5)c$. Net zo vinden we $v_1(c) = -(1/5)a + (3/5)c$. Dus $v_1(a)$ en $v_1(b)$ zijn beide in W. Omdat (a,c) een basis is van W is ieder element van W van de vorm $\alpha a + \beta c$ met α en β in $\mathbb{R}$. Omdat v_1 lineair is geldt: $v_1(\alpha a + \beta c) = \alpha v_1(a) + \beta v_1(c) \in W$. Dus $v_1(W) \subseteq W$.

   Een meer gelikte manier is om op te merken dat W de deelruimte is van alle functies $f : \mathbb{R} \to \mathbb{R}$ van de vorm $x \mapsto \alpha x + \beta$, want W is hier een deelruimte van en heeft dezelfde dimensie. Het is dan duidelijk dat $v_1(W) = W$. Met deze benadering ligt het voor de hand de basis (d,e) van W te kiezen, met $d(x) = 1$ en $e(x) = x$.

   (d) We hebben al het rekenwerk al gedaan:

$${}_{(a,c)}\mathrm{mat}_{(a,c)}(v_1) = \begin{pmatrix} 7/5 & -1/5 \\ 4/5 & 3/5 \end{pmatrix}.$$

   Voor de andere basis is het resultaat eenvoudiger:

$${}_{(d,e)}\mathrm{mat}_{(d,e)}(v_1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Herkansing januari 2016

Tentamen Fundamenten, 27 januari 2016, 17:30–20:30
Theo van den Bogaart, Bas Edixhoven

Tentamenstof Fundamenten, najaar 2015

Het hele dictaat, behalve:

- I.5 (smurfenprobleem),
- IV.3 (de recursiestelling),
- VIII (de appendix).

De eerste vereiste is dat je de definities van de gebruikte begrippen kent, en dat je directe toepassingen daarvan beheerst (bv. het geven van eenvoudige bewijzen en voorbeelden). De tweede vereiste is dat je de belangrijkste stellingen kent (de preciese voorwaarden en de conclusie). Als je aan deze twee eisen voldoet dan haal je zeker een voldoende. Om een hoog cijfer te halen moet je ook bewijzen van de moeilijkere stellingen kunnen geven.

Herkansing Fundamenten, 27 januari 2016, 17:30–20:30

Bewijs al je beweringen, dat wil zeggen, geef duidelijke argumenten en schrijf alle stappen op. Schrijf kort, duidelijk en net. Rekenmachines en documenten (bijvoorbeeld het dictaat) zijn niet toegestaan. **Er zijn 7 opgaven**.
Indicatieve normering: 90=10+10+10+15+15+15+15 (de eerste 10 punten zijn gratis).
Tijdsduur: 3 uur. Succes!

1. (a) Geef een definitie van equivalentierelatie op een verzameling.
   (b) Laat $n \in \mathbb{Z}$. Leg uit wat $\mathbb{Z}/n\mathbb{Z}$ is.
   (c) Leg uit hoe optelling en vermenigvuldiging op $\mathbb{Z}/n\mathbb{Z}$ zijn gedefiniëerd.
   (d) Geef een n waarvoor $\mathbb{Z}/n\mathbb{Z}$ een lichaam is, en een n waarvoor dat niet zo is.

2. (a) Geef de waarheidstabellen voor
      i. $P \vee Q$,
      ii. $\neg(P \Rightarrow Q)$.
   (b) Schrijf de zin 'Het is niet waar dat er a, b en c in $\mathbb{Z}$ bestaan met ($a^3 + b^3 = c^3$ en $abc \neq 0$)' in een formule met alleen de symbolen $\forall$, $\exists$, $\neg$, $\wedge$, $\vee$, $\in$, $\mathbb{Z}$, a, b, c, $+$, $\cdot$ (voor vermenigvuldiging), $=$, 0, en haakjes '(' en ')'.
   (c) Geef een formule met alleen dezelfde symbolen die logisch equivalent is met die van het vorige onderdeel en die niet begint met '$\neg$'.

3. (a) Geef een voorbeeld van een verzameling A en een functie $f : A \to A$ die injectief is, maar niet surjectief is.
   (b) Bestaat er voor iedere verzameling A een f als in het vorige onderdeel?
   (c) Bestaat er een bijectieve functie f van het gesloten interval $[0,\infty) \subseteq \mathbb{R}$ naar het open interval $(0,\infty) \subseteq \mathbb{R}$? Zo ja, geef zo'n f. Zo nee, waarom niet?

4. Bewijs met volledige inductie dat voor alle n in $\mathbb{N}$ geldt dat
$$\sum_{i=0}^{n} (2i+1) = (n+1)^2.$$

5. Zij F een lichaam. Voor $x, y \in F$ met $y \neq 0$ noteren we $\frac{x}{y} = xy^{-1}$, waarbij y^{-1} de multiplicatieve inverse van y is. Bewijs op grond van de axioma's van een lichaam dat voor alle x en y in F met $x \neq 0$ en $y \neq 0$ geldt dat $\frac{1}{(\frac{x}{y})} = \frac{y}{x}$. (Zie verderop voor de lichaamsaxioma's.)

6. Gegeven is de functie $f : \mathbb{R} \to \mathbb{R}$ met
$$f(x) = \begin{cases} 0 & \text{als } x \in \mathbb{Q}, \\ x & \text{als } x \notin \mathbb{Q}. \end{cases}$$
   (a) Bewijs dat f continu is in 0.
   (b) Bewijs dat voor alle $a \neq 0$ de functie f *niet* continu is in a.

7. We brengen in herinnering dat $M_{2,2}(\mathbb{R})$ (de verzameling 2×2-matrices met reële coëfficiënten met matrixoptelling en -vermenigvuldiging) een ring is. Met optelling en scalaire vermenigvuldiging heeft $M_{2,2}(\mathbb{R})$ ook de structuur van een $\mathbb{R}$-vectorruimte.
   We beschouwen de deelverzameling V van matrices van de vorm

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad \text{met } a, b \in \mathbb{R}.$$

   (a) Laat zien dat vermenigvuldiging in $M_{2,2}(\mathbb{R})$ niet commutatief is.

   (b) Toon aan dat V gesloten is onder vermenigvuldiging – anders gezegd: voor alle x en y in V is ook xy in V.

   (c) Bewijs dat V een deelruimte is van $M_{2,2}(\mathbb{R})$.

   (d) Geef een basis van V.

   (e) Geef een isomorfisme van ringen $\mathbb{C} \to V$.

Definitie. Een lichaam is een verzameling F, met operaties + en $\cdot$, en elementen 0 en 1, zodat de volgende eigenschappen gelden

1. + en $\cdot$ zijn associatief en commutatief,
2. voor alle a, b en c in F geldt dat $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
3. 0 is neutraal voor +, en 1 is neutraal voor $\cdot$,
4. elke a in F heeft een additieve inverse,
5. elke $a \neq 0$ in F heeft een multiplicatieve inverse,
6. $1 \neq 0$.

Uitwerking Herkansing Fundamenten, 27 januari 2016

1. (a) 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* $\forall_{a,b,c\in V}\ (a \sim b \wedge b \sim c) \implies a \sim c$.

   (b) Definieer een equivalentierelatie op $\mathbb{Z}$ als volgt: $a \sim b$ precies dan als $a-b$ deelbaar is door n. Nu is $\mathbb{Z}/n\mathbb{Z}$ de verzameling restklassen onder deze equivalentierelatie: de elementen zijn de niet-lege deelverzamelingen A van $\mathbb{Z}$ die voldoen aan de volgende voorwaarde: voor alle $a \in A$ en $b \in \mathbb{Z}$ geldt

$$b \in A \iff a \sim b.$$

   (c) Zij $A, B \in \mathbb{Z}/n\mathbb{Z}$. Kies representanten $a \in A$ en $b \in B$ en laat $A+B$ [resp. $A\cdot B$] de restklasse zijn die het element $a+b$ [resp. $a\cdot b$] bevat. Deze definitie is alleen correct als deze restklasse niet afhangt van de keuze van representanten, hetgeen volgt uit

$$a \sim a' \text{ en } b \sim b' \qquad \implies \qquad a+b \sim a'+b'$$

   en de analoge implicatie voor vermenigvuldiging.

   (d) $\mathbb{Z}/n\mathbb{Z}$ is een lichaam precies dan als n of $-n$ een priemgetal is. Bijvoorbeeld is $\mathbb{Z}/2\mathbb{Z}$ is lichaam en $\mathbb{Z}/4\mathbb{Z}$ niet.

2. (a)

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

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

   (b) $\neg\exists_{a\in\mathbb{Z}}\exists_{b\in\mathbb{Z}}\exists_{c\in\mathbb{Z}}(a\cdot a\cdot a + b\cdot b\cdot b = c\cdot c\cdot c \wedge \neg a\cdot b\cdot c = 0)$

   (c) Bijvoorbeeld $\forall_{a\in\mathbb{Z}}\neg\exists_{b\in\mathbb{Z}}\exists_{c\in\mathbb{Z}}(a\cdot a\cdot a + b\cdot b\cdot b = c\cdot c\cdot c \wedge \neg a\cdot b\cdot c = 0)$

3. (a) Neem bijvoorbeeld $A = \mathbb{Z}$ en $f(x) = 2x$ voor $x \in \mathbb{Z}$. Deze is injectief (want $2x = 2y$ impliceert $x = y$), maar niet surjectief (bijvoorbeeld is er geen $x \in \mathbb{Z}$ waarvoor $1 = 2x$).

   (b) Nee, als A eindig is, bestaat zo'n f niet. Als zo'n f wel bestaat, dan zouden A en $f(A)$ gelijkmachtig zijn; maar een eindige verzameling kan niet gelijkmachtige zijn met een strikte deelverzameling.

   (c) Ja, want de verzamelingen zijn gelijkmachtig. Hier is een voorbeeld:

$$f(x) = \begin{cases} x, & \text{als } x \notin \mathbb{Z}, \\ x+1, & \text{als } x \in \mathbb{Z}. \end{cases}$$

4. Zij $P(n)$ de propositie

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

   Omdat $2\cdot 0 + 1 = (0+1)^2$ is $P(0)$ waar.
   Stel nu dat $P(n)$ geldt voor een zekere $n \in \mathbb{N}$. Dan geldt:

$$\sum_{i=0}^{n+1}(2i+1) = \sum_{i=0}^{n}(2i+1) + (2(n+1)+1) = (n+1)^2 + 2(n+1) + 1,$$

   volgens de inductiehypothese. Maar

$$(n+1)^2 + 2(n+1) + 1 = ((n+1)+1)^2$$

   en dus is ook $P(n+1)$ waar. Met volledige inductie volgt nu $P(n)$ voor alle $n \in \mathbb{N}$.

5. Zij $x, y \in F \setminus \{0\}$. We moeten laten zien dat $(xy^{-1})^{-1} = yx^{-1}$. Nu is $(xy^{-1})^{-1}$ per definitie het unieke element $c \in F$ waarvoor geldt $c(xy^{-1}) = 1$ (dan volgt $(xy^{-1})c = 1$ uit commutativiteit van vermenigvuldiging) en dat betekent dat we moeten nagaan dan $(yx^{-1})(xy^{-1}) = 1$. Welnu:

$$\begin{array}{lll} (yx^{-1})(xy^{-1}) & = ((yx^{-1})x)y^{-1} & \text{(associativiteit } \cdot) \\ & = (y(x^{-1}x))y^{-1} & \text{(associativiteit } \cdot) \\ & = (y \cdot 1)y^{-1} & \text{(multiplicatieve inverse)} \\ & = yy^{-1} & \text{(1 is eenheid voor } \cdot) \\ & = 1 & \text{(multiplicatieve inverse).} \end{array}$$

6. (a) Zij $B_{f(0)} \subset \mathbb{R}$ een bolomgeving van $f(0)$. Anders gezegd: $B_{f(0)}$ is gelijk aan het interval $(-\varepsilon, \varepsilon)$ voor een zekere $\varepsilon > 0$. Definieer nu $B_0 = B_{f(0)}$; dan is B_0 een bolomgeving van 0 en voor $x \in B_0$ geldt $f(x) = 0$ of $f(x) = x$ en daarom ook $f(x) \in B_{f(0)}$. Dus is f continu in 0.

   (b) Zij $a \in \mathbb{R} \setminus \{0\}$ en stel dat f wél continu is in a. Wegens continuïteit bestaat er een bolomgeving B van a zodat $|f(b) - f(a)| < \frac{1}{2}|a|$ voor alle $b \in B$. We onderscheiden nu twee situaties.
   Als a irrationaal is kiezen we $b \in B$ rationaal – zo'n element bestaat omdat de rationale getallen dicht liggen in $\mathbb{R}$. Dan geldt $|a| = |f(b) - f(a)| < \frac{1}{2}|a|$ en dat is een tegenspraak.
   Als a rationaal is kiezen we $b \in B$ irrationaal zodat $|b - a| < \frac{1}{2}|a|$ – zo'n element bestaat omdat de irrationale getallen dicht liggen in $\mathbb{R}$ en B een bolomgeving is van a. Dan geldt $|a| = |a - b + b| \leqslant |a - b| + |b| < \frac{1}{2}|a| + |b|$ en dus $|b| > \frac{1}{2}|a|$. Ook geldt $|b| = |f(b) - f(a)| < \frac{1}{2}|a|$ en dat geeft een tegenspraak.

7. (a) Bijvoorbeeld

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

   terwijl

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

   (b) Voor $a, b, c, d \in \mathbb{R}$ geldt:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -ad - bc \\ bc + ad & -bd + ac \end{pmatrix} = \begin{pmatrix} e & -f \\ f & e \end{pmatrix},$$

   met $e = ac - bd$ en $f = bc + ad$.

   (c) De nulmatrix is een element van V en bovendien geldt voor alle $a, b, c, d, \lambda \in \mathbb{R}$:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a + c & -(b + d) \\ b + d & a + c \end{pmatrix}$$

   en

$$\lambda \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \lambda a & -\lambda b \\ \lambda b & \lambda a \end{pmatrix}.$$

   (d) Bijvoorbeeld:

$$v_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ en } v_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

   Dit zijn elementen van V die V voortbrengen:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a \cdot v_1 + b \cdot v_2$$

   en onafhankelijk zijn:

$$\lambda_1 v_1 + \lambda_2 v_2 = 0 \iff \lambda_1 = \lambda_2 = 0.$$

(e) Definieer een afbeelding $f : \mathbb{C} \to V$ door $f(a+bi) = av_1 + bv_2$ (met v_1, v_2 als in het vorige antwoord). Omdat v_1, v_2 een basis is, is dit een bijectie. We moeten laten zien dat f de optellings- en vermenigvuldigingsstructuur behoudt (en volgens de definitie uit het dictaat ook dat $f(1) = 1$). Voor optelling is dit makkelijk:

$$\begin{aligned} f((a+bi)+(c+di)) &= (av_1 + bv_2) + (cv_1 + dv_2) \\ &= (a+c)v_1 + (b+d)v_2 \\ &= f((a+c)+(b+d)i); \end{aligned}$$

voor vermenigvuldiging gebruiken we de formules uit het antwoord van onderdeel b hierboven:

$$\begin{aligned} f((a+bi)\cdot(c+di)) &= (av_1 + bv_2)\cdot(cv_1 + dv_2) \\ &= (ac-bd)v_1 + (bc+ad)v_2 \\ &= f((ac-bd)+(ad+bc)i). \end{aligned}$$

Bibliografie

[Da] D. van Dalen. *Logic and structure.* Fifth edition. Universitext. Springer, London, 2013. x+263 pp. ISBN: 978-1-4471-4557-8; 978-1-4471-4558-5. Online: http://link.springer.com/book/10.1007%2F978-1-4471-4558-5

[DDS] D. van Dalen, H.C. Doets en H.C.M. de Swart. *Verzamelingen; naïef, axiomatisch en toegepast.* Oosthoek, Scheltema & Holkema, Utrecht, 1975.

[EV] J. van Eijck en A. Visser. *Inzien en bewijzen.* Online: http://homepages.cwi.nl/~jve/qed/

[Fr] R.M. French. *The Banach-Tarski theorem.* Math. Intelligencer 10 (1988), no 4, 21–28. Online: http://leadserv.u-bourgogne.fr/files/publications/000293-the-banach-tarski-theorem.pdf

[Ha] K.P. Hart. *Kreatief met sinaasappels.* Kennislink, 2007. Online: http://www.kennislink.nl/publicaties/een-sinaasappel-erbij-toveren

[HHP] J. Hilgert. M. Hoffman, A. Panse. *Einführung in mathematisches Denken und Arbeiten.* Springer Spektrum, 2015. ISBN: 978-3-662-45511-1. DOI: 10.1007/978-3-662-45512-8

[Ho] K. Houston. *How to think like a mathematician.* Cambridge University Press, 2009. 279 pages. ISBN: 978-0-511-50645-1 (e-book), 978-0-521-89546-0 (hardback), 978-0-521-71978-0 (paperback).

[La] S.R. Lay. *Analysis. An introduction to proof.* Prentice Hall, Inc., Englewood Cliffs, NJ, 1986. xii+285 pp. ISBN: 0-13-032996-7

[vL] R. van Luijk. *Linear algebra I.* Online: http://websites.math.leidenuniv.nl/algebra/linalg1.pdf

[SM] T.C. Scott en P. Marketos. *On the origin of the Fibonacci Sequence*. Online: http://www-history.mcs.st-andrews.ac.uk/Publications/fibonacci.pdf

[St1] M. Stoll. *Linear algebra I.* Online: http://www.mathe2.uni-bayreuth.de/stoll/lecture-notes/LinearAlgebraI.pdf

[St2] M. Stoll, with some additions by R. van Luijk. *Linear algebra II.* http://pub.math.leidenuniv.nl/~luijkrmvan/linalg2/2015/LinAlg2-2015.pdf

[WIMS] WIMS: WWW Interactieve Multipurpose Server. http://wims.unice.fr/wims/wims.cgi?lang=nl

Index