CWI Syllabi

CWI
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
Telephone + 31 - 20 592 9333
Telefax + 31 - 20 592 4199
URL http://www.cwi.nl

CWI is the nationally funded Dutch institute for research in Mathematics and Computer Science.

Wijzer in Wiskunde

Een inleiding via logica en verzamelingen

H.C. Doets

1991 Mathematics Subject Classification: 03-01, 04-01, 06-01
ISBN 90 6196 466 0
NUGI-code: 811

Inhoud

Vooraf v

1 Gebruikslogica: Waarheid 1
- 1.1 Vorm . . . 1
- 1.2 Inhoud . . . 3
- 1.3 Propositie-logica . . . 5
  - 1.3.1 Connectieven en Waarheidstafels . . . 6
  - 1.3.2 Geldigheid . . . 9
- 1.4 Kwantoren . . . 11

2 Gebruikslogica: Bewijsbaarheid 15
- 2.1 Kunst van het Bewijzen . . . 15
- 2.2 Bewijsregels . . . 17
- 2.3 Taktiek . . . 24
- 2.4 Voorbeelden uit de Analyse . . . 25

3 Verzamelingen 29
- 3.1 Verzameling-begrip . . . 29
- 3.2 Hoe Noteer Je een Verzameling . . . 31
- 3.3 Bizondere Verzamelingen . . . 33
- 3.4 Algebra . . . 33

4 Relaties 41
- 4.1 Paren en Producten . . . 41
- 4.2 Relaties . . . 43
- 4.3 Equivalenties . . . 45

5 Functies 51
- 5.1 Basisbegrippen . . . 51
- 5.2 Surjectie, Injectie, Bijectie; Compositie . . . 55
- 5.3 Inversen . . . 58
- 5.4 Definiëren van Functies en Relaties op Quotienten . . . 61
- 5.5 Producten en Machten . . . 62

6 Eindig vs. Oneindig **65**
6.1 Volledige Inductie 65
6.2 Gelijkmachtigheid 70
6.3 Kombinatoriek 73
6.3.1 Pigeon-hole Principes 74
6.3.2 Ramsey-stellingen 75
6.3.3 Bomen 76
6.3.4 Wel-quasi-ordeningen 82

7 Formele Bewijzen **89**
7.1 Natuurlijke Deductie 89
7.2 Afleidingen 91
7.3 Afleidbaarheid 96
7.4 Verband tussen Waarheid en Afleidbaarheid 98
7.4.1 Betrouwbaarheid 98
7.4.2 Volledigheid 100

8 Oneindige Verzamelingen **103**
8.1 Ongelijkmachtig 103
8.2 Aftelbaar 104
8.3 Overaftelbaar 105
8.4 Cantor-Bernstein Stelling 107
8.5 Kardinaalgetallen 110
8.6 Keuze-axioma 112

9 Ordeningen **117**
9.1 Eigenschappen van Relaties 117
9.2 Ordeningsrelaties 119
9.3 Isomorfie 122
9.4 Definities en Opgaven 124
9.5 Bomen als Partiële Ordeningen 127
9.6 Isomorfie en Equivalentie 127
9.7 Ordetype 128

10 Ordeningen van $\mathbb{N}$, $\mathbb{Q}$ en $\mathbb{R}$ **133**
10.1 Ordening van $\mathbb{N}$ 133
10.2 Ordening van $\mathbb{Q}$ 134
10.3 Geordende Sommen en Producten 137
10.4 Ordening van $\mathbb{R}$ 141
10.4.1 Ordeningsvolledigheid 141
10.4.2 Separabiliteit 143
10.4.3 Karakterisering 144
10.4.4 Constructie 146
10.5 Welordeningen en Ordinalen 148
10.6 Lemma van Zorn 152

Literatuur **157**

INHOUD

iii

Grieks Alfabet **159**

Index **161**

Notatie **165**

Vooraf

Dit boekje is bestemd voor studenten in het eerste jaar van de studie wiskunde.

Het wil drie dingen.

Het eerste hangt samen met de treurige omstandigheid, dat de wiskunde van het VWO geen aandacht besteedt aan het meest wezenlijke kenmerk van de wiskunde: het *bewijs*. Daarom is de naam *wiskunde* voor het gelijknamige VWO-vak — waar eigenlijk alleen gerekend wordt — tamelijk misplaatst.

Hoofdstuk 2 probeert in deze lacune te voorzien door uit te leggen hoe een wiskundig bewijs eruit ziet; in de volgende hoofdstukken wordt geprobeerd dit in praktijk te brengen in een aantal eenvoudige contexten. De "toegift" Hoofdstuk 7 maakt van een (bescheiden) fragment van het wiskundig deductie apparaat een zelfstandig stukje wiskunde en legt het verband tussen waarheid en bewijsbaarheid.

De tweede ambitie is het behandelen van de verzamelingstheoretische basisbegrippen van de wiskunde. Hierover gaan Hoofdstukken 3, 4 en 5, en delen van Hoofdstukken 6 en 8.

Ten derde is er nog andere, misschien minder nuttige, maar toch belangrijke basiskennis: soorten oneindigheid (Hoofdstukken 6 en 8), ordeningen en hun eigenschappen, de constructie van het continuum (Hoofdstukken 9 en 10), waarvoor in het normale curriculum vaak geen ruimte blijft.

Door de markeringen met * is het mogelijk verschillende selecties van de stof te maken.

- Beginnende eerstejaars kunnen het beste alle zo gemarkeerde passages (secties, stellingen e.d.) over slaan.

- Gevorderde eerstejaars/beginnende tweedejaars moeten in staat geacht worden ook de rest te verwerken, op (delen van) de secties over kombinatoriek (6.3) keuze-axioma (8.6), ordinalen (10.5) en Zorn's lemma (10.6) na. Deze onderwerpen zijn opgenomen omdat ze in de context passen, deze illustreren, of omdat ze relevant zijn voor algebra en topologie.

Bij zelfstandige bestudering en bij het uitwerken van een redelijk gedeelte van de meer dan 300 opgaven — zonder dat heeft bestudering weinig zin — moet je op hulp kunnen rekenen.

Opgaven zijn herkenbaar aan het symbool ♣. Een opgave is voorzien van twee van dergelijke symbolen als van met ster gemarkeerde theorie gebruik moet worden gemaakt, of als hij moeilijker is dan gemiddeld.

Ieder hoofdstuk eindigt met een "samenvatting" die niets anders is dan een opsomming van de belangrijkste begrippen en een serie theorievragen uit de niet-gesterde gedeelten van het hoofdstuk. Het kunnen geven van tekst en uitleg bij ieder van deze begrippen en vragen kan een controle zijn op de verwerking van de inhoud.

Aan het eind van sommige hoofdstukken wordt naar de literatuur verwezen. Maar: het niveau van bijna alle verwijzingen vereist meer voorkennis of vaardigheid dan deze tekst geeft. Alleen Devlin [4] en Velleman [16] vormen hierop uitzonderingen. Deze boeken vormen uitstekende bruggen tussen VWO en Universiteit. De eerste is heel goed zelfstandig leesbaar; iedere beginnende wiskunde student zou het moeten hebben, en liefst ook lezen. Maar het geeft alleen beknopte informatie over wat een bewijs is, terwijl het tweede ook de informatie van het huidige Hoofdstuk 2 uitdiept. Beide overlappen gedeeltelijk met wat hier in de eerste vijf hoofdstukken wordt besproken, maar hun tempo is vriendelijker.

Eerdere versies van dit materiaal, de oudste in 1983 geschreven in samenwerking met A.S. Troelstra, zijn in gebruik geweest bij de opleiding wiskunde aan de Universiteit van Amsterdam.

Naast LaTeX is voor de afleidingsbomen in Hoofdstuk 7 dankbaar gebruik gemaakt van newbussproofs.sty (version 0.5b, 1995) van Samuel R. Buss.

Hoofdstuk 1

Gebruikslogica: Waarheid

Misschien is niets geheel waar, en zelfs dàt niet.
(Multatuli, *Ideeën 1*)

Dit hoofdstuk vertelt iets over de rol van de logica in de wiskunde in de symbolische weergave van wiskundige beweringen.

Sectie 1.1 (*Vorm*) zegt e.e.a. over grammaticaal correct gebruik van de logische basis-uitdrukkingen: voegwoorden of *connectieven*, en *kwantoren*. Sectie 1.2 (*Inhoud*) zegt hoe deze basis-uitdrukkingen zich gedragen in de wiskundige conversatie.

Subsecties 1.3.1, 1.3.2 en Sectie 1.4 gaan gedetailleerder in op de connectieven aan de hand van hun *waarheidstafels* en geven een aantal veel gebruikte logische wetten in propositie-logica (logica van de connectieven) en kwantor-logica.

1.1 Vorm

Bekijk de volgende (ware) bewering:

> tussen twee reële getallen ligt een derde.

Om de logische struktuur duidelijk te maken volgt hier een meer expliciete versie, die gebruik maakt van variabelen en verwijst naar de ordening $<$ van de verzameling van reële getallen $\mathbb{R}$:

> voor alle reële getallen x en y geldt:
> als $x < y$, dan is er een reëel getal z zódat zowel $x < z$ als $z < y$.

('zowel $x < z$ als $z < y$' wordt vaak afgekort tot: $x < z < y$.)

De tekens $\forall$, $\rightarrow$, $\exists$ en $\wedge$ zijn, bij wijze van afkorting, in gebruik voor de zinswendingen *voor alle* (*voor iedere*), *als—dan*, *er is* (*er zijn*) en *en* (*zowel—als*); $\in$ staat voor *is element van* (Notatie 3.1, blz. 30). Onder gebruikmaking van deze notaties kan deze bewering nu korter worden weergeven als volgt:

$$\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [\, x < y \;\longrightarrow\; \exists z \in \mathbb{R}\, (\, x < z \;\wedge\; z < y\,)\,].$$

(De twee kwantor-uitdrukkingen $\forall x \in \mathbb{R}$ en $\forall y \in \mathbb{R}$ kun je ook samentrekken tot: $\forall x, y \in \mathbb{R}$.)

Merk op, hoe de haakjes hier het "bereik" van de uitdrukkingen $\forall x \in \mathbb{R}$, $\forall y \in \mathbb{R}$ en $\exists z \in \mathbb{R}$ bepalen: de eerste twee zijn van kracht tussen de haakjes [en], de tweede is dat tussen (en).

De uitdrukkingen *voor alle* ($\forall$), en *er is* ($\exists$) heten *kwantoren*. De letters x, y en z waarop deze kwantoren betrekking hebben, heten *variabelen*. De kwantorcombinatie $\forall x$ *bindt* ieder optreden van de variabele x in zijn bereik; netzo bindt $\exists z$ ieder optreden van z in zijn bereik.

De uitdrukkingen *en*, afgekort: $\wedge$, en *als—dan*, afgekort: $\rightarrow$, heten *connectieven*. Er zijn nog meer connectieven in geregeld gebruik, nl.: *of* (symbool: $\vee$); *niet*, uitvoeriger: *het is niet zo, dat* (symbool: $\neg$), en *dan en slechts dan als* of *dan en dan alléén*, in de wiskundige omgangstaal meestal afgekort met: *d.e.s.d.a.* (symbool: $\leftrightarrow$).[1]

Kwantoren en connectieven heten wel *logische tekens* omdat hun betekenis niet context-afhankelijk is (voor de kwantoren geldt dit overigens maar in zekere zin). Nog een ander logisch teken is het *identiteitsteken* $=$. Hieronder volgt een overzicht van de notaties voor connectieven en kwantoren, met alternatieven die ook wel worden gebruikt.

omschrijving	*naam*	*symbool*	*alternatieven*
en	conjunctieteken	$\wedge$	$\&$ $\cdot$
of	disjunctieteken	$\vee$	$+$
als—dan	implicatieteken	$\rightarrow$	$\Rightarrow$ $\supset$
d.e.s.d.a.	equivalentieteken	$\leftrightarrow$	$\Leftrightarrow$ $\equiv$
niet	negatieteken	$\neg$	$\sim$
voor alle x	universele kwantor	$\forall x$	$\bigwedge x$ (x)
er is een x	existentiële kwantor	$\exists x$	$\bigvee x$ (Ex)

1.1 Definitionele equivalentie en -gelijkheid. De notatie $:\equiv$ wordt hier gebruikt voor: *is per definitie equivalent met*; netzo wordt $:=$ gebruikt voor: *is per definitie gelijk aan*. Elders zie je ook wel $\equiv_{\text{def}}$ en $=_{\text{def}}$.

Binden van variabelen. Hierboven werd opgemerkt, dat variabelen door kwantoren worden gebonden. Zonder erg precies te zijn kun je zeggen, dat een variabele in een uitdrukking is *gebonden* als de betekenis van de uitdrukking niet van de (waarde van de) variabele afhangt en die variabele alleen is gebruikt om naar plaatsen in de uitdrukking te kunnen verwijzen. Behalve met kwantoren zijn er nog verschillende andere manieren om variabelen te "binden". Voorbeelden:

- *De functie die x afbeeldt op x^2.*

  Hiermee wordt een welbepaalde functie beschreven die niet van de waarde van de variabele x afhangt.

[1] In het Engels wordt het *if and only if* meestal afgekort tot *iff*.

- *Sommatie.*

  Bijvoorbeeld, de uitdrukking $\sum_{i=1}^{5} i$ is niets anders dan een ingewikkelde omschrijving van het getal 15 — nl. als $1+2+3+4+5$ — en die hangt niet af van de waarde van de variabele i.

- *Abstractie.*

  Nog een andere manier van binden van een variabele vindt plaats in de *abstractie-notatie* $\{\, x \mid E \,\}$, zie (3.1), blz. 31.

Slechte Gewoonten. Met een beetje pech zou je de boven aangehaalde bewering ook kunnen aantreffen in de volgende gedaante.

> Voor alle reële getallen x en y,
> als $x < y$, dan gelden $x < z$ en $z < y$ voor een reëel getal z.

Hiermee kan zowel de onware bewering, dat $\exists z \in \mathbb{R}\, \forall x, y \in \mathbb{R}\, (x < y \longrightarrow x < z \wedge z < y)$, worden bedoeld als de ware bewering, dat $\forall x, y \in \mathbb{R}\, \exists z \in \mathbb{R}\, (x < y \longrightarrow x < z \wedge z < y)$. Het zowel vooraan als achteraan plaatsen van kwantoren bevordert kennelijk dubbelzinnigheid: het is hier moeilijker om het bereik van de verschillende kwantoren te bepalen. In het ergste geval kunnen beweringen ontstaan met twee totaal verschillende betekenissen.

Ook is het heel makkelijk om onzorgvuldig te zijn met het aangeven, welke variabelen als — op een of andere manier — gebonden worden bedoeld. Bijvoorbeeld, de afgeleide van $x^2 + 2x$ als functie van x is $2x + 2$, maar de afgeleide van $x^2 + 2x$ als functie van y is 0.

Een minder goede gewoonte is het om een kwantor voor een samengestelde uitdrukking te zetten:

> voor alle getallen $n^2 + 1, \ldots$

Hoewel dit niet altijd tot onduidelijkheid hoeft te leiden, is het toch verstandig deze manier van schrijven te vermijden. Beter is dan nog: voor alle getallen *van de vorm* $n^2 + 1, \ldots$.

Vertaalproblemen. Dankzij grillen van het Nederlands is het niet altijd even vanzelfsprekend hoe je een bewering moet schrijven met behulp van connectieven en kwantoren. Al in het eerste voorbeeld van deze sectie ('tussen twee getallen ligt een derde') is het moeilijk om een universele kwantor en een implicatieteken te ontdekken.

Een ander voorbeeld is 'een goede Vietcong is een dode Vietcong'. De onbepaalde lidwoorden mogen hier dan *existentiële* kwantoren suggereren, maar de ongetwijfeld bedoelde bewering heeft de vorm $\forall m \in VC\, (G(m) \rightarrow D(m))$.

1.2 Inhoud

Eén van de verworvenheden van de logica is de mogelijkheid, om dezelfde formule op verschillende manieren te kunnen interpreteren. (Overigens is dit geen privilege van de logica: in de algebra bijvoorbeeld kan het vermenigvuldigingsteken $\cdot$

staan voor de vermenigvuldigingsoperatie van iedere willekeurige groep.) Bekijk weer dezelfde bewering, nu zonder referentie aan de verzameling $\mathbb{R}$ weergegeven als

$$\forall x \, \forall y \, [\, x < y \;\longrightarrow\; \exists z \, (\, x < z \;\wedge\; z < y \,)\,]$$

of, met het neutralere teken $\mathbf{R}$ i.p.v. $<$ (dat gewoonlijk op een ordening duidt)

$$\forall x \, \forall y \, [\, x\mathbf{R}y \;\longrightarrow\; \exists z \, (\, x\mathbf{R}z \;\wedge\; z\mathbf{R}y \,)\,].$$

Deze uitdrukking heeft alléén betekenis, als duidelijk is afgesproken op welk *domein* de kwantoren betrekking hebben, en wat de betekenis is van het teken $\mathbf{R}$ op dit domein. In het voorafgaande was dit domein de verzameling van reële getallen $\mathbb{R}$ en $\mathbf{R}$ stond voor de gewone ordening van de reële getallen. Kwantoren $\forall x$ en $\exists z$ moeten dan gelezen worden als: *voor alle reële getallen x geldt ...*, resp., *er is een reeël getal z waarvoor geldt ...* In dat geval drukt de formule de *ware* bewering uit, dat tussen iedere twee reële getallen een derde ligt. Maar, je had als domein ook de verzameling $\mathbb{N}$ van natuurlijke getallen $0, 1, 2, \ldots$ kunnen nemen (en $<$ / $\mathbf{R}$ als de gewone ordening hierop), en in dat geval staat de formule voor een *onware* bewering: tussen opvolgende natuurlijke getallen als 2 en 3 ligt immers geen derde natuurlijk getal.

Conclusie: om kwantoren ($\forall x$ of $\exists x$) te kunnen begrijpen, moet een *domein* of *universum* U (dat is e.o.a. collectie van objecten) zijn gespecificeerd, waarop die kwantoren betrekking hebben: $\forall x$ en $\exists x$ betekenen in de context van zo'n domein U dan: *voor alle $x \in U$ ...*, resp., *er is een $x \in U$ ...*

De weergegeven formule is kennelijk voor meerdere interpretaties vatbaar, afhankelijk van het gekozen universum en de betekenis van het teken $<$ of van $\mathbf{R}$. Een dergelijke interpretatie-bepalende context: universum, plus betekenis van *niet-logische* tekens zoals $<$ of $\mathbf{R}$ heet een *struktuur* of *model*:

1.2 Model. Een universum, tezamen met een specificatie, wat met de niet-logische tekens van de gegeven context wordt bedoeld, heet een *struktuur* of *model* (*passend bij* de niet-logische tekens van die context).

Als $\mathbf{R}$, $\mathbf{c}$, ... niet-logische tekens zijn, dan heeft een hierbij passend model de vorm $\mathcal{A} = (A, R, c, \ldots)$; hierin is A het universum, R de relatie[2] op A die de betekenis is van het relatieteken $\mathbf{R}$, c het element van A dat de betekenis is van het teken $\mathbf{c}$, enz.

Voorbeelden van modellen zijn ordeningen als $(\mathbb{N}, <)$, $(\mathbb{R}, <)$, de structuren van de algebra: groepen, ringen, lichamen, de bomen van Subsectie 6.3.3 (blz. 76).

Strukturen/modellen worden vaak aangegeven met de symbolen $\mathcal{A}$, $\mathcal{B}$ en $\mathcal{C}$.

Voorbeeld. Bekijk de bewering

$$\forall x \, \forall y \, (\mathbf{V}(x, y) \longrightarrow \{\mathbf{O}(x, y) \vee \exists z[\mathbf{V}(x, z) \wedge \mathbf{O}(z, y)]\})$$

[2] Relaties vormen het onderwerp van Hoofdstuk 4.

en de struktuur waarvan het universum de wereldbevolking is, $\mathbf{O}(x, y)$ staat voor: x is een ouder van y en $\mathbf{V}(x, y)$ voor: x is een voorouder van y. De interpretatie van de bewering in de context van deze struktuur is: iedere voorouder is een ouder, of een voorouder van een ouder, en dat *is* zo. De bewering is dus *waar* m.b.t. deze struktuur.

Als je van de eerder besproken bewering de eerste kwantorcombinatie $\forall x$ afhaalt, dan houd je de volgende uitdrukking over:

$$\forall y\ [\, x\mathbf{R}y \ \longrightarrow\ \exists z\,(\, x\mathbf{R}z \ \wedge\ z\mathbf{R}y\,)\,].$$

Deze heeft wel de *vorm* van een bewering, maar is zelf geen bewering: als je haar wilt interpreteren — in welke struktuur dan ook — stuit je (de kwantor $\forall x$ is er niet meer) op het ongespecificeerde ding x. In de oorspronkelijke bewering werd de variabele x gebonden door de kwantorcombinatie $\forall x$ aan de kop van de bewering. In de nieuwe versie is deze kwantor weg, en de resterende optredens van x worden niet langer gebonden. Een (in een uitdrukking) niet-gebonden optreden van een variabele heet *vrij* (in die uitdrukking). Vervang je x hier door (de naam van) een specifiek reëel getal, dan is er wèl weer sprake van een bewering.

Een uitdrukking als de bovenstaande, die zich als bewering voordoet maar het niet is, "onaf" is, heet een *beweringsvorm* of een *formule*. Formules zijn kennelijk om te zetten in beweringen op twee manieren: 1. *binden* van *vrije* variabelen door kwantoren; 2. vervanging van vrije variabelen door (namen van) concrete objecten uit het afgesproken universum. (N.B. *namen van*: bijvoorbeeld, in een formule als 'x wordt ingekapseld' kun je de variabele x niet vervangen door de *persoon* Jeltsin —hoe zou dat moeten?— maar wèl door de *naam* 'Jeltsin' van de persoon Jeltsin!)

1 ♣ Opgave. Beschouw de volgende modellen:

a. $(\mathbb{N}, <)$ (universum $\mathbb{N} = \{0, 1, 2, \ldots\}$, met de gewone ordening);

b. $(\mathbb{N}, >)$ (analoog);

b. $(\mathbb{R}, <)$ (universum $\mathbb{R}$, eveneens met de gewone ordening);

c. (V, R), waarin V de collectie van alle verzamelingen $X \subset \mathbb{N}$ is, en R de relatie *echte deelverzameling van*, gedefinieerd op V door: $XRY :\equiv X \subset Y \ \wedge\ X \neq Y$. (Zie zonodig Definitie 3.3 op blz. 33.) Op welke van deze modellen gelden de volgende zinnen? (het niet-logische teken $\mathbf{R}$ staat hier dus achtereenvolgens voor: de gewone ordening $<$ van $\mathbb{N}$, de inverse ordening $>$ van $\mathbb{N}$, de gewone ordening $<$ van $\mathbb{R}$ en de echte inclusie):

1. $\forall x \exists y (x\mathbf{R}y)$,
2. $\exists x \forall y (x = y \ \vee\ x\mathbf{R}y)$,
3. $\forall x \exists y (x\mathbf{R}y \ \wedge\ \neg \exists z (x\mathbf{R}z \ \wedge\ z\mathbf{R}y))$.

1.3 Propositie-logica

De propositie-logica is het onderdeel van de logica dat over de connectieven gaat.

1.3.1 Connectieven en Waarheidstafels

In het voorafgaande heb je gezien, dat met connectieven beweringen en formules kunnen worden gecombineerd tot nieuwe beweringen en formules. De betekenis van de connectieven kan eenvoudig worden beschreven door uit te leggen hoe de waarheid (of onwaarheid) van de combinatie afhangt van de waarheid van de delen.

Voor het vervolg staan de letters W en O voor de twee *waarheidswaarden*. W staat voor $WAAR$, en O voor $ONWAAR$. (Soms worden ook de getallen 1 en 0 gebruikt i.p.v. W en O.)

Bij de waarheidstafel-benadering van de propositie logica wordt nu van twee principes uitgegaan:

1. iedere bewering is óf waar, óf onwaar,

2. de waarheidswaarde van een met connectieven samengestelde bewering hangt af van de waarheidswaarde van zijn delen.

Hoe dat zit wordt beschreven door de *waarheidstafels* van de connectieven.

In het volgende staan de letters P en Q voor willekeurige beweringen.

Negatie

Een uitdrukking van de vorm $\neg P$ (*niet* P) heet de *negatie* van P. Deze uitdrukking is *waar*, of: heeft de waarheidswaarde W, juist ingeval P *onwaar* is, d.w.z., waarheidswaarde O heeft. In tabelvorm:

P	$\neg P$
W	O
O	W

Deze tabel heet de *waarheidstafel* van het negatieteken.

Conjunctie

De uitdrukking $P \wedge Q$ (P *èn* Q) heet de *conjunctie* van P en Q. P en Q heten de *leden* of *conjuncten* van $P \wedge Q$. Deze uitdrukking is waar precies ingeval P en Q *beide* waar zijn. In tabel-vorm:

P	Q	$P \wedge Q$
W	W	W
W	O	O
O	W	O
O	O	O

Dit is de *waarheidstafel* van het conjunctieteken.

Disjunctie

De uitdrukking $P \vee Q$ (P *of* Q) heet de *disjunctie* van P en Q. P en Q heten de *leden* of *disjuncten* van $P \vee Q$.

De interpretatie van disjuncties is niet altijd even vanzelfsprekend. In de omgangstaal zijn twee *of*'s in gebruik: de *inclusieve*, die een disjunctie ook waar rekent als *beide* disjuncten waar zijn, en een *exclusieve*, die dat niet doet. Deze laatste wordt meestal met een accent aangegeven: óf (en vaak verdubbeld tot óf...óf).

In de wiskunde wordt uitsluitend met de inclusieve *versie gewerkt: een disjunctie is waar als* tenminste één *van de disjuncten waar is.*

Dan nog kunnen problemen opduiken.

Voorbeeld. De volgende bewering wordt vermoedelijk door iedereen geaccepteerd als waar:

voor ieder geheel getal x geldt: $x < 1$ of $0 < x$.

Maar, acceptatie hiervan brengt natuurlijk acceptatie van ieder individueel geval met zich mee; bijvoorbeeld, voor $x := 1$:

$$1 < 1 \text{ of } 0 < 1.$$

Sommigen kunnen dit niet als geldend accepteren, of vinden dit een "onzinnige" bewering, omdat er immers iets "beters", t.w.: $0 < 1$, geldt. In de wiskunde zul je met dit soort situaties moeten leren leven.

De waarheidstafel van het disjunctieteken ziet er als volgt uit:

P	Q	$P \vee Q$
W	W	W
W	O	W
O	W	W
O	O	O

Implicatie

Een uitdrukking van de vorm $P \rightarrow Q$ (*als* P *dan* Q, Q *als* P) heet de *implicatie* van P en Q. P en Q heten de *leden* van de implicatie, P is het *linkerlid* of *antecedens* en Q het *rechterlid* of *consequens.*

De waarheidstafel van $\rightarrow$ is misschien de enige die niet vanzelf spreekt, maar ze is heel goed motiveerbaar aan de hand van het volgende voorbeeld. Niemand zal willen ontkennen, dat voor ieder natuurlijk getal n geldt:

$$5 < n \rightarrow 3 < n.$$

Maar dan moet dit i.h.b. gelden voor de getallen 2, 4 en 6. Dus, een implicatie is *waar* als (i) beide leden *onwaar* zijn ($n = 2$); (ii) het linkerlid *onwaar* en het rechter *waar* is ($n = 4$); en (iii) beide leden *waar* zijn ($n = 6$). Natuurlijk is een implicatie tenslotte *onwaar* als zijn linkerlid *waar* en zijn rechter *onwaar* is. Dit levert de volgende waarheidstafel.

P	Q	$P \rightarrow Q$
W	W	W
W	O	O
O	W	W
O	O	W

Implicaties waarvan het *eerste* lid *onwaar*, en die waarvan het *tweede* lid *waar* zijn, zijn dus *waar*. Implicaties die (ongeacht de waarden van eventueel erin voorkomende parameters) één van deze eigenschappen hebben heten wel "triviaal waar". (Wiskundigen hebben de gewoonte om vanzelfsprekendheden *triviaal* te noemen — speciaal in die gevallen waarin ze niet naar nadere uitleg gevraagd willen worden.) Hiervan zijn een aantal, voor de beginner eigenaardige, voorbeelden, zoals het feit dat de *lege verzameling* een deel is van *iedere* verzameling — zie Stelling 3.4 op blz. 34.

Ook het gebruik van implicatie strookt niet altijd met die van de omgangstaal. Daar wordt bijvoorbeeld een zeker *verband* geëist tussen de leden van een implicatie. In het wiskundig gebruik zal zo'n verband in de regel ook bestaan, maar nodig voor de interpretatie is dit niet: de waarheidstafel vertelt alles. En soms sluit de omgangstaal verbluffend goed aan bij de waarheidstafel, bijvoorbeeld in de uitroep: "ik zal doodvallen als Karel zijn belofte niet nakomt". Geuit door een van levenslust stralend type ('ik zal doodvallen' *onwaar*) moet dit worden opgevat — volgens de waarheidstafel! — als een ingewikkelde manier om te zeggen dat op beloftes van Karel gebouwd kan worden.

In de wiskundige praktijk wordt meestal het teken $\Rightarrow$ gebruikt i.p.v. $\rightarrow$, omdat $\rightarrow$ al zoveel andere rollen speelt.

De *omkering* van een implicatie $P \Rightarrow Q$ is $Q \Rightarrow P$; de *contrapositie* is $\neg Q \Rightarrow \neg P$. De omkering van een ware implicatie hoeft niet waar te zijn, maar een implicatie en zijn contrapositie zijn òfwel beide waar, òfwel beide onwaar (zie de contrapositiewetten van Stelling 1.5, blz. 10).

Een conditie P heet wel een *voldoende voorwaarde* voor de conditie Q en Q een *nodige voorwaarde* voor P als de implicatie $P \Rightarrow Q$ waar is.

Equivalentie

De uitdrukking $P \leftrightarrow Q$ (P d.e.s.d.a. Q) heet de *equivalentie* van P en Q. P en Q heten de *leden* van de equivalentie. De waarheidstafel van het equivalentieteken is (in ieder geval na acceptatie van die voor $\rightarrow$) volstrekt onproblematisch; ze bepaalt dat $P \leftrightarrow Q$ waar is ingeval P en Q dezelfde waarheidswaarde hebben. In wiskundige praktijk wordt meestal het teken $\Leftrightarrow$ gebruikt i.p.v. $\leftrightarrow$.

P	Q	$P \leftrightarrow Q$
W	W	W
W	O	O
O	W	O
O	O	W

De conditie P heet een *noodzakelijke en voldoende voorwaarde* voor Q als de equivalentie $P \Leftrightarrow Q$ geldig is.

1.3.2 Geldigheid

Met de connectieven kunnen formules en beweringen herhaald worden samengesteld. Er moeten dan wel haakjes worden gebruikt om de volgorde aan te geven waarin deze samenstelling is gevormd.
Een voorbeeld vormt de uitdrukking

$$\neg P \wedge [(P \rightarrow Q) \leftrightarrow \neg(Q \wedge \neg P)].$$

Met behulp van de waarheidstafels kun je nu de waarheidswaarde van zo'n samenstelling uitrekenen, als waarheidswaarden voor de formules P en Q gegeven zijn. Zijn die waarden W (voor P) resp. O (voor Q), dan krijgt $\neg P$ de waarde O; $P \rightarrow Q$ wordt O; $Q \wedge \neg P$: O; $\neg(Q \wedge \neg P)$: W; $(P \rightarrow Q) \leftrightarrow \neg(Q \wedge \neg P)$: O, en de totale uitdrukking krijgt dus de waarde O. De berekening is eenvoudig in één regel te geven door te beginnen met de gegeven waarheidswaarden onder de letters te zetten, en de waarden voor achtereenvolgende *subformules* (zie Definitie 1.6, blz. 10) onder het bijbehorende connectief te plaatsen. De einduitkomst O van de berekening is onderstreept:

$\neg$	P	$\wedge$	$[(P$	$\rightarrow$	$Q)$	$\leftrightarrow$	$\neg$	$(Q$	$\wedge$	$\neg$	$P)]$
O	W	$\underline{O}$	W	O	O	O	W	O	O	O	W

1.3 Logisch Geldig.

1. Een uitdrukking die (op grammaticaal correcte manier) is samengesteld uit letters $P, Q, R, \ldots$ connectieven en haakjes heet een *formule* van de propositie-logica.

   Formules worden in het vervolg aangegeven met Griekse hoofdletters Φ, $\Psi, \ldots$[3]

2. Een formule heet (propositioneel-) *logisch geldig* als hij altijd de waarheidswaarde W krijgt, ongeacht de waarheidswaarden toegekend aan de erin voorkomende letters.

Voorbeelden van logische geldigheden zijn alle formules van een van de volgende gedaanten: $\Phi \rightarrow \Phi$, $\Phi \vee \neg\Phi$, $\Phi \rightarrow (\Psi \rightarrow \Phi)$ (ga na).

Waarheidstafel van een formule. Als je wilt onderzoeken of een formule van de propositie-logica logisch geldig is stel je z'n *waarheidstafel* op. De in zo'n formule voorkomende letters heten *propositie-letters* of *-variabelen*. Bevat de formule n letters, dan zijn er 2^n mogelijke distributies van de twee waarheidswaarden over deze letters mogelijk, die ieder hun eigen waarheidswaarde voor de formule opleveren. Deze 2^n berekeningen van deze waarheidswaarden vormen de *waarheidstafel* van de betreffende formule. Zijn alle uitkomsten gelijk aan W, dan heb je te maken met een logische geldigheid. Een voorbeeld van zo'n waarheidstafel is te vinden onder Opgave 2 op blz. 11.

[3] Het Griekse alfabet vind je op blz. 159.

Weglaten van haakjes in formules. In de notatie van formules wordt bezuinigd op haakjes door af te spreken dat $\wedge$ en $\vee$ sterker binden dan $\rightarrow$ en $\leftrightarrow$. Dus bijvoorbeeld: $P \wedge Q \rightarrow R$ staat voor: $(P \wedge Q) \rightarrow R$.

1.4 Logisch Equivalent. Formules Φ en Ψ heten (propositioneel-logisch) *equivalent*, notatie: $\Phi \equiv \Psi$, als $\Phi \leftrightarrow \Psi$ logisch geldig is, d.w.z.: als onder iedere toekenning van waarheidswaarden aan variabelen Φ en Ψ dezelfde waarheidswaarde krijgen.

Het volgende is een opsomming van een aantal vaak gebruikte equivalenties van de propositie-logica. Hierin mag je voor de letters P, Q en R desgewenst willekeurige formules lezen.

1.5 Stelling.

1. $P \equiv \neg\neg P$ *(wet van de dubbele negatie),*
2. $(P \rightarrow Q) \equiv \neg P \vee Q$; $\neg(P \rightarrow Q) \equiv P \wedge \neg Q$,
3. $(\neg P \rightarrow \neg Q) \equiv (Q \rightarrow P)$;
   $(P \rightarrow \neg Q) \equiv (Q \rightarrow \neg P)$; $(\neg P \rightarrow Q) \equiv (\neg Q \rightarrow P)$ *(contrapositie wetten),*
4. $(P \leftrightarrow Q) \equiv [(P \rightarrow Q) \wedge (Q \rightarrow P)] \equiv [(P \wedge Q) \vee (\neg P \wedge \neg Q)]$,
5. $P \wedge P \equiv P$; $P \vee P \equiv P$ *(idempotentie van $\wedge$ en $\vee$),*
6. $P \wedge Q \equiv Q \wedge P$; $P \vee Q \equiv Q \vee P$ *(commutativiteit van $\wedge$ en $\vee$),*
7. $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$; $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ *(associativiteit),*
8. $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$; $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ *(distributiviteit),*
9. $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$; $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ *(wetten van DeMorgan).*

Onderdeel 1.5.7 rechtvaardigt het weglaten van haakjes in conjuncties en disjuncties van drie of meer leden.

Voor de praktijk nuttige onderdelen van Stelling 1.5 zijn 2, 3 en 9.

1.6 Subformule. Een formule die als (aaneengesloten) deel voorkomt binnen een andere formule heet een *subformule* van die formule.

Voorbeeld. De subformules van de eerder bekeken formule $\neg P \wedge [(P \rightarrow Q) \leftrightarrow \neg(Q \wedge \neg P)]$ zijn: P, Q, $\neg P$, $P \rightarrow Q$, $Q \wedge \neg P$, $\neg(Q \wedge \neg P)$, $(P \rightarrow Q) \leftrightarrow \neg(Q \wedge \neg P)$ en de formule zelf.

1.7 Stelling. *Als in een formule van de propositie-logica een deelformule wordt vervangen door een equivalent, dan is het resultaat een equivalent van de oorspronkelijke formule.*

Bewijs. Onderstel dat de formule Ψ verkregen is door in de formule Φ het deel φ te vervangen door zijn equivalent ψ. Hoe je ook waarheidswaarden toevoegt aan de letters in Ψ en Φ, het uitrekenen van de waarheidswaarden van deze formules verloopt volledig parallel, behalve waar het de subformules φ en ψ betreft. Maar, voor die subformules is het resultaat per hypothese hetzelfde, en dus krijg je dezelfde waarheidswaarde voor Φ en Ψ. ⊣

Voorbeeld. De formule $P \wedge \neg(\neg Q \vee R)$ is equivalent met (1.5.9) $P \wedge (\neg\neg Q \wedge \neg R)$ en met (1.5.1) $P \wedge (Q \wedge \neg R)$.

Opgaven

2 ♣ Bewijs Stelling 1.5. (Doe één onderdeel van 1.5.2 en één van 1.5.3.)
Aanwijzing. Stel de waarheidstafel van de betreffende formule op.
Bijvoorbeeld, voor de eerste DeMorgan wet uit 1.5.9:

$\neg$	$(P$	$\wedge$	$Q)$	$\leftrightarrow$	$(\neg$	P	$\vee$	$\neg$	$Q)$
O	W	W	W	W	O	W	O	O	W
W	W	O	O	W	O	W	W	W	O
W	O	O	W	W	W	O	W	O	W
W	O	O	O	W	W	O	W	W	O

Omdat onder het hoofdconnectief $\leftrightarrow$ alléén W's optreden, is $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ logisch geldig, en dus heb je dat $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$.

3 ♣♣ Bekijk de volgende twee beweringen over propositionele formules Φ en Ψ:
(a) $\Phi \vee \Psi$ is logisch geldig,
(b) Φ is logisch geldig, of Ψ is logisch geldig.
(i) Geldt, voor alle Φ en Ψ, dat als (a), dan ook (b)?
(ii) Geldt (idem) als (b), dan ook (a)?
Geef een argument of een tegenvoorbeeld.

1.4 Kwantoren

Wat hiervoor aan propositie-logica is behandeld is eigenlijk nogal flauw en voor de wiskunde weinig relevant. Bijvoorbeeld, je zult vermoedelijk zelden het verlangen bij je voelen opkomen om een disjunctie van twee beweringen zoals $3 < 1 \vee 1 < 3$ op te schrijven: het disjunct $1 < 3$ is óók waar, en veel informatiever. Maar worden eenmaal variabelen toegelaten, dan verandert alles, en wordt het vormen van propositionele samenstellingen opeens zinvol.

Voor de context met kwantoren komt Definitie 1.3.1 er als volgt uit te zien.

1.8 Formule, Zin.

1. Een kwantor-logische *formule* is een grammaticaal correcte uitdrukking, opgebouwd uit basistekens (zoals $\mathbf{R}$, $=$, namen van objecten) en variabelen, connectieven en kwantoren (en haakjes).

2. Een *zin* is een formule zonder vrije variabelen.

In Sectie 1.2 is uitgelegd, dat zinnen kunnen worden geïnterpreteerd in verschillende strukturen (Definitie 1.2, blz. 4), en dat de waarheidswaarde van een zin in verschillende strukturen verschillend kan uitvallen.

1.9 Logisch Geldig, Equivalent.

1. Een formule is *logisch geldig* als hij in iedere, bij de formule passende, struktuur geldt onder iedere vervanging van eventuele vrije variabelen door (namen voor) elementen van het universum van die struktuur.

2. Φ en Ψ zijn (logisch) *equivalent* als $\Phi \leftrightarrow \Psi$ logisch geldig is.

Merk op, dat als Φ een formule is met vrije variabelen $x_1, \ldots, x_n$ en $\mathcal{A}$ is een struktuur passend bij Φ, dan geldt Φ in $\mathcal{A}$ d.e.s.d.a. $\forall x_1 \cdots \forall x_n \Phi$ daarin geldt. Dus volgt uit Definitie 1.9.1 dat Φ logisch geldig is d.e.s.d.a. $\forall x_1 \cdots \forall x_n \Phi$ dat is.

Hieronder volgen — zonder bewijs — een aantal veel gebruikte logische geldigheden waarin kwantoren figureren. Van de meeste is de waarheid niet moeilijk in te zien.

1.10 Stelling. *Formules van de volgende gedaanten zijn logisch geldig:*

1. $\exists x \forall y \Phi \longrightarrow \forall y \exists x \Phi$,

2. $\forall x(\Phi \rightarrow \Psi) \longrightarrow (\forall x \Phi \rightarrow \forall x \Psi)$; $\forall x(\Phi \rightarrow \Psi) \longrightarrow (\exists x \Phi \rightarrow \exists x \Psi)$,

3. $\forall x(\Phi \leftrightarrow \Psi) \longrightarrow (\forall x \Phi \leftrightarrow \forall x \Psi)$; $\forall x(\Phi \leftrightarrow \Psi) \longrightarrow (\exists x \Phi \leftrightarrow \exists x \Psi)$,

4. $\forall x \forall y \Phi \longleftrightarrow \forall y \forall x \Phi$; $\exists x \exists y \Phi \longleftrightarrow \exists y \exists x \Phi$,

5. $\neg \forall x \Phi \longleftrightarrow \exists x \neg \Phi$; $\neg \exists x \Phi \longleftrightarrow \forall x \neg \Phi$;
$\neg \forall x \neg \Phi \longleftrightarrow \exists x \Phi$; $\neg \exists x \neg \Phi \longleftrightarrow \forall x \Phi$,

6. $\forall x(\Phi \wedge \Psi) \longleftrightarrow (\forall x \Phi \wedge \forall x \Psi)$; $\exists x(\Phi \vee \Psi) \longleftrightarrow (\exists x \Phi \vee \exists x \Psi)$. ⊣

Voor de praktijk nuttige onderdelen van Stelling 1.10 zijn 1, 4 en 5.

Volgorde van Kwantoren. Onderdeel 4 van Stelling 1.10 zegt, dat de volgorde van *gelijksoortige* kwantoren er niet toe doet. Maar: merk op i.v.m. onderdeel 1, dat de implicatie $\forall x \exists y \Phi \longrightarrow \exists y \forall x \Phi$ *niet* logisch geldt. Voorbeeld: $\forall x \exists y(x < y)$ geldt in het domein van de natuurlijke getallen; maar $\exists y \forall x(x < y)$ doet de foutieve bewering dat er een natuurlijk getal y is dat groter is dan alle natuurlijke getallen. Opdat $\forall x \exists y \Phi$ geldt moet er bij iedere (waarde voor) x een (waarde voor) y bestaan zódat aan Φ wordt voldaan (door die waarden); die waarde van y kan dus heel goed van die van x afhangen. Dat $\exists y \forall x \Phi$ geldt betekent dat er een *vaste* waarde voor y is die, ongeacht de waarde van x, aan Φ voldoet, en dat is natuurlijk een veel sterkere eis.

Stelling 1.7 blijft geldig voor de context met kwantoren en wordt zonder bewijs vermeld.

1.11 Stelling. *Als in een kwantor-logische formule een deelformule wordt vervangen door een equivalent, dan is het resultaat een equivalent van de oorspronkelijke formule.* ⊣

Beperkte Kwantoren. Volgens de "ε-δ-definitie" van continuïteit uit de analyse is een reële functie f *continu* als:

$$\forall x\, \forall \varepsilon > 0\, \exists \delta > 0\, \forall y\, [\, |x - y| < \delta \implies |f(x) - f(y)| < \varepsilon\,]. \qquad (1.1)$$

Deze formule gebruikt de *beperkte* kwantoren '$\forall \varepsilon > 0$' en '$\exists \delta > 0$' die vaak een compactere weergave mogelijk maken. Zo is de zin

$$\forall y \forall x [x < y \implies \exists z (x < z \ \wedge \ z < y)]$$

óók weer te geven als

$$\forall y \forall x < y \exists z < y (x < z)$$

— maar dat voert de compactheid misschien weer te ver.

Beperkte kwantoren worden vaak gebruikt in de context van ordeningen ($\forall x < y$) en verzamelingen ($\forall x \in A$) — zie later. Overigens kun je — zie hiervóór — natuurlijk ook kwantoren beperken met het bedoelde domein.

De versie van Stelling 1.10.5 voor beperkte kwantoren is ook geldig; zo geldt bijvoorbeeld, dat $\neg \forall x \in A\, \Phi$ equivalent is met $\exists x \in A\, \neg \Phi$, etc.

Schuiven met Kwantoren. Met Stelling 1.10.1/2/4 en Stelling 1.11 als "steunen in de rug" kun je inzien, dat $\forall y \exists z \forall x \Phi \to \forall x \forall y \exists z \Phi$ logisch geldt:
$\exists z \forall x \Phi \to \forall x \exists z \Phi$ is logisch geldig, *dus ook* $\forall y (\exists z \forall x \Phi \to \forall x \exists z \Phi)$, en ook $\forall y \exists z \forall x \Phi \to \forall y \forall x \exists z \Phi$. En de twee universele kwantoren in het rechterlid kunnen tenslotte (1.10.4, 1.11) worden omgewisseld. Praktijk-voorbeeld:

Continuïteit en Uniforme Continuïteit. Continuïteit van de reële functie f wil zeggen, dat aan conditie (1.1) hiervoor is voldaan. *Uniforme* continuïteit van f betekent

$$\forall \varepsilon > 0\, \exists \delta > 0\, \forall x\, \forall y\, [\, |x - y| < \delta \implies |f(x) - f(y)| < \varepsilon\,].$$

Vergeleken met (1.1) is de kwantor $\forall x$ twee plaatsen naar achteren verschoven. Volgens het voorafgaande wordt continuïteit geïmpliceerd door *uniforme* continuïteit. Maar zoals bekend: er zijn continue functies die niet uniform continu zijn.

Dat f *niet* continu is betekent

$$\neg \forall x\, \forall \varepsilon > 0\, \exists \delta > 0\, \forall y\, [\, |x - y| < \delta \implies |f(x) - f(y)| < \varepsilon\,].$$

Met behulp van Stelling 1.10.5 en Stelling 1.11 kan dit worden getransformeerd in vier stappen, iedere keer de negatie langs een kwantor werkend, tot:

$$\exists x\, \exists \varepsilon > 0\, \forall \delta > 0\, \exists y\, \neg\, [\, |x - y| < \delta \implies |f(x) - f(y)| < \varepsilon\,].$$

Volgens Stelling 1.5.2 is dit tenslotte equivalent met

$$\exists x\, \exists \varepsilon > 0\, \forall \delta > 0\, \exists y\, [\, |x-y| < \delta \ \wedge\ \neg\, |f(x)-f(y)| < \varepsilon\,],$$

d.w.z., met

$$\exists x\, \exists \varepsilon > 0\, \forall \delta > 0\, \exists y\, [\, |x-y| < \delta \ \wedge\ |f(x)-f(y)| \geqslant \varepsilon\,].$$

Dankzij deze logische transformaties is het dus mogelijk om een duidelijker "beeld" te krijgen, wat niet-continuïteit betekent: er zijn dan kennelijk x en $\varepsilon > 0$ zódat voor iedere $\delta > 0$ ("hoe klein ook") er een y is met $|x-y| < \delta$, terwijl $|f(x)-f(y)| \geqslant \varepsilon$; d.w.z.: er zijn getallen y "willekeurig dicht bij x" waarvoor de functiewaarden $f(x)$ en $f(y)$ minstens ε van elkaar verwijderd blijven.

4 ♣ Opgave. Beargumenteer, dat beweringen van de vorm $(\forall x \Phi \vee \forall x \Psi) \rightarrow \forall x(\Phi \vee \Psi)$ logisch geldig zijn.
Geef een eenvoudig voorbeeld waaruit blijkt dat $\forall x(\Phi \vee \Psi) \rightarrow (\forall x \Phi \vee \forall x \Psi)$ dat niet is.

1.12 Soorten. Vaak spelen verschillende *soorten* objekten tegelijk een rol in dezelfde beschouwing. (Bijvoorbeeld: vectoren in e.o.a. vectorruimte naast reële getallen.) In zo'n geval worden vaak verschillende variabelen gebruikt voor objecten van de verschillende soorten. Bijvoorbeeld: de letters $n, m, k, \ldots$ staan vaak voor natuurlijke getallen, $f, g, h, \ldots$ duiden meestal op functies, enz. De interpretatie van de kwantoren vereist in zo'n geval niet de specificatie van één universum, maar van een aantal: voor iedere soort één.

Samenvatting

Belangrijkste begrippen:

- connectieven: $\neg$, $\rightarrow$, $\leftrightarrow$, $\wedge$, en $\vee$,
- kwantoren: $\forall$ en $\exists$,
- waarheidstafels van connectieven,
- model/struktuur,
- logisch geldig (in propositie- en kwantorlogica).

Vraag:

- hoe maak je de waarheidstafel van een formule?

Literatuur

Sterk aanbevolen is Devlin's op de beginnende wiskunde-student toegesneden boek [4]. Meer over logica is te vinden in van Dalen [1].

Hoofdstuk 2

Gebruikslogica: het Bewijs

Hier wordt beschreven hoe je een bewijs in elkaar zet. Sectie 2.1 geeft stilistische aanwijzingen, Sectie 2.2 beschrijft de formele regels waarmee bewijzen worden opgebouwd, Sectie 2.3 vertelt hoe je die gebruiken moet, en Sectie 2.4 besluit met enkele voorbeelden ontleend aan de analyse.

2.1 De Kunst van het Bewijzen

Het is niet heel duidelijk, wat de objecten van de wiskunde zijn. Bijvoorbeeld, deze bevinden zich niet in de gewone, fysische ruimte. Niemand zag ooit het getal π (of zelfs het getal 0). Je zou zelfs kunnen volhouden, dat wiskunde nergens over gaat.

Over de *methode* van de wiskunde daarentegen bestaat grote overeenstemming: de kern daarvan is het *bewijs*. Een bewijs is een argumentatie die je op een absoluut sluitende manier van de waarheid van een bewering overtuigt, of dat probeert. Een goed bewijs kan een kunstwerk zijn dat esthetische met intellectuele kwaliteiten versmelt tot één moment van doorzicht, en waarvan het vinden, of zelfs maar het begrijpen, diepe voldoening oplevert.

Onder vakgenoten bestaat in concrete gevallen grote eenstemmigheid over wat een bewijs is; democratie in de wiskunde is dan ook, wat dit aspect betreft, geen probleem. Mensen argumenteren in uiteenlopende situaties, maar gewoonlijk levert dat weinig overeenstemming op. De waterdichtheid van wiskundige redeneringen is dus een opvallend verschijnsel, dat waarschijnlijk toch verband houdt met het geïdealiseerde karakter van de wiskundige objecten.

Het wiskundig gehalte van de bewijzen die in de eerste helft van deze inleiding worden gegeven of gevraagd is gering; later noem je zulke bewijzen "routine". De aandacht gaat voorlopig naar de *vorm* van bewijzen. Om te beginnen volgt hier een lijstje met tien stilistische geboden.

Er is al gezegd, dat een bewijs een argumentatie is. De basis-eenheid is dus de (Nederlandse) zin.

1 *Schrijf correct Nederlands.*

(De meeste zinnen hebben onderwerp, gezegde enz.)

Er zijn je symbolische afkortingen voor gangbare zinswendingen corresponderend met logische constanten (connectieven, kwantoren) aangereikt; gebruik die spaarzaam (iets als (1.1), blz. 13 is wel ongeveer het maximum dat de gemiddelde wel-opgevoede wiskundige in één keer tot zich kan laten doordringen) en consistent.

2 *Gebruik zinswendingen niet tegelijk met hun symbolische afkorting in één bewering.*

Een bewijs dat uitsluitend uit symbolen bestaat geeft weinig informatie over je hersen-activiteiten.

3 *Schrijf niet alléén formules. Begin een zin nooit met een formule.*

Spring met formules in een tekst om alsof het zelfstandige naamwoorden zijn. Voorbeeld: "de formule Φ is geldig". Ook goed is: "er geldt dat Φ".

Maak gebruik van verbindingswoordjes als 'dus', 'daarom', e.d. Desgewenst kun je dit afkorten met drie puntjes: $\therefore$

Het is niet bevorderlijk voor de leesbaarheid om het implicatieteken $\Rightarrow$ te gebruiken waar 'dus' op zijn plaats zou zijn. Bedenk dat $\Rightarrow$ een afkorting is voor 'als... dan'. Met dit symbool vorm je implicaties, d.w.z. beweringen. Met 'dus' geef je daarentegen aan een gevolgtrekking te maken. Zo gebruikt vormt dit verbindingswoordje geen beweringen. (Natuurlijk bestaan er wel relaties tussen deze twee. Als 'A, *dus* B' een correcte gevolgtrekking is, dan is de bewering $A \Rightarrow B$ waar, en omgekeerd: dat is zo ongeveer wat de regels $\rightarrow$I en $\rightarrow$E hierna vertellen.)

4 *Vertel een verhaaltje, verbind je formules met wat tekst, wees informatief.*

Maar aan de andere kant moet je ook niet overdrijven.

5 *Wees relevant en beknopt.*

Het is dus zaak, het goede midden te houden.

Als er dan toch symbolen — vaak variabelen — moeten verschijnen, laat die dan niet plompverloren uit de lucht vallen, maar zeg wat je met ze voor hebt (zie de regels $\forall$I en $\exists$E hierna).

6 *Declareer je variabelen: zeg wat ze betekenen.*

In veel gevallen is het een goed idee om aan het begin van een bewijs precies te vermelden, waarvan je uit mag gaan (het *gegeven*) en wat er precies van wordt verwacht (het *te bewijzen*).

7 *Gebruik de volgende drie aanheffen:*

Gegeven: ...
Te bewijzen: ...
Bewijs: ...

Een *bewijs met inductie* maakt nog extra strukturering mogelijk; zie blz. 66.

In zowel *Gegeven* als *Te bewijzen* kunnen begrippen voorkomen waarvan de precieze betekenis door *definities* ondubbelzinnig is vastgelegd. (Zie blz. 29 voor méér over definities.) De bedoeling is dat, door die definities ook daadwerkelijk te gebruiken, met zulke begrippen op de bedoelde, precieze manier wordt omgesprongen.

8 *Zoek definities van gedefineerde begrippen op en gebruik die om* Gegeven *en* Te Bewijzen *uit te schrijven.*

Speciaal het volledig uitschrijven van het *Te Bewijzen* vormt in veel gevallen het halve werk: het laat je precies zien, wat er van je wordt verwacht.

Reken er niet op, dat je het door jou gezochte bewijs in één keer correct zal opschrijven. Verwacht zelfs niet, dat het in twee keer lukt. Ga er maar vanuit dat bevredigende bewijzen voorlopig zullen uitblijven, en blijf desondanks proberen.

9 *Zorg voor een ruime voorraad kladpapier en schrijf je eindproduct — méér of minder gelukt — uiteindelijk in het net.*

Tenslotte: laat je pas gewrochte bewijs *minimaal* een dag liggen, en stel jezelf *dan* pas de hamvragen:

10 *Klopt het allemaal?*
en: *Kan een ander óók begrijpen wat ik heb opgeschreven?*

Het *eerlijke* antwoord zal gewoonlijk negatief uitvallen, om aldus aanleiding te geven tot het wederom aanspreken van de voorraad kladpapier. Er valt heus iets te zeggen voor de opvatting, dat als je iets goed hebt begrepen, je het *uiteindelijk* ook goed op papier kunt krijgen. (Pas hierop eens de contrapositiewet toe van Stelling 1.5, blz. 10.)

Zoals gezegd, veel van de hier gegeven bewijzen zijn "routine", dat is: van het type "loop je neus achterna" (maar dat dat zo is, zul je vaak pas na een tijdje zien). Hier volgt het lijstje met de mooiste exemplaren, waarvoor alleen je neus (dus) niet voldoende is: Cantor's Stellingen 8.10 en 8.9 (blz. 106), 8.12, de karakteriseringen 10.3 (blz. 134), 10.15 (blz. 144), en 10.18 (blz. 147). Moeilijker exemplaren zijn Ramsey's Stelling 6.12 (blz. 75), Stelling 6.17 over het gevecht tussen Hercules en de Hydra, Kruskal's Stelling 6.23, en de Welordeningsstelling 10.22 (blz. 150). Al deze resultaten zijn doorbraken, en aan hun bewijzen liggen fraaie ideeën ten grondslag.

2.2 Bewijsregels

Het is normaal, dat je in je eerste bewijspogingen vastloopt, en ook, dat je zelfs geen begin weet te maken. Deze sectie bespreekt enige regels die het gedrag van de logische operaties in wiskundige bewijzen beschrijven. Zeker als je vastloopt is het een goed idee om te zien of één van deze regels bruikbaar is in jouw situatie. Er worden, in operationele termen, zo'n 15 praktisch bruikbare

bewijsregels beschreven voor alle (7) logische tekens. Hoewel dit op het eerste gezicht misschien wel veel regels zijn is het opmerkelijk dat ze een arsenaal bieden dat tegen iedere situatie is opgewassen.

Overigens zijn de meeste regels tamelijk vanzelfsprekend en in ieder geval makkelijk te onthouden; je kunt dan ook tegen het expliciet beschrijven van de regels aankijken als het opgang brengen van een proces van bewustwording. Zo'n proces gaat natuurlijk gepaard met de nodige verwarring. (Vgl. de chronische slapeloosheid die de man met de baard —uit een verhaal van Alphonse Allais— overviel toen hem gevraagd werd of hij met z'n baard *boven* of *onder* de dekens sliep.)

De verhouding tussen *bewijsregels* en *bewijs* kan vergeleken worden met die tussen de regels van het schaakspel en het schaakspel. Om te kunnen schaken moet je de regels kennen. Maar gaat je kennis niet verder, dan kan je schaken alleen maar slaafs en richtingloos zijn. Leren schaken houdt niet op met leren van de regels, en wat er mooi is aan een partij schaak is in de regels niet terug te vinden. Netzo kunnen de bewijsregels alléén je nooit meer leren dan het uitvoeren van de eenvoudigste typen van bewijzen (maar dat is in het begin al moeilijk genoeg). Het zijn *ideeën* die bewijzen hun charme verlenen, en daarover wordt in de bewijsregels niet gerept.

Klassificatie van regels. Sommige regels (modus ponens, de conjunctieregels) vertellen je, welke conclusies *direct* uit bepaalde premissen kunnen worden getrokken, andere regels (zoals de deductieregel) stellen je in staat om een bewijsprobleem te reduceren tot een nieuw, hopelijk eenvoudiger, bewijsprobleem.

De regels zijn verder ingedeeld naar de logische vorm van het *gegeven* dat je wilt gebruiken (*eliminatie*regels), of de *te bewijzen* bewering (*introductie*regels). Bij de constructie van een bewijs in de wiskundige praktijk kun je immers op twee manieren tegen (bijvoorbeeld) een implicatie $P \to Q$ aanlopen:

1. als een *gegeven*, waarvan je dus gebruik mag maken in je bewijs,

2. als een *te bewijzen*, dus als *conclusie* van het te construeren bewijs (of gedeelte daarvan).

Het ligt daarom voor de hand dat er ook twee bewijsregels zijn voor het implicatieteken: (1.) die het *gebruiken* van implicaties beschrijft: de *eliminatie* regel, en (2.) die beschrijft hoe je implicaties moet bewijzen: de *introductie* regel. De nomenclatuur van regels is simpel: de *eliminatie*regel van het teken ♠ wordt aangegeven met ♠E, en ♠I geeft de *introductie*regel van dat teken aan.

Gebruiksaanwijzing. Bij eerste lezing is de overvloed aan regels verwarrend. Blijf er daarom niet te lang mee bezig. Beperk je in eerste instantie bijvoorbeeld tot de discussie van implicatie. Lees wel Sectie 2.3 over taktiek, en ga, al naar gelang de behoefte, terug om wat meer regels te consumeren, naar aanleiding van latere bewijsproblemen en bewijzen.

Implicatie

Het implicatieteken (dat hier eenvoudshalve als $\rightarrow$ wordt geschreven, en niet als $\Rightarrow$) heeft één eliminatie- en één introductie-regel. Beide regels liggen nogal voor de hand als je aan de praktijk denkt; je zou zelfs van mening kunnen zijn dat ze te triviaal zijn om op te schrijven. Maar dat vonden de oude grieken kennelijk niet.

$\rightarrow$E, Eliminatie regel voor $\rightarrow$, modus ponens.

$$(P \rightarrow Q), P \;\models\!\!\Longrightarrow\; Q$$

In woorden: uit $P \rightarrow Q$ en P kun je de conclusie Q trekken.

Het teken $\models\!\!\Longrightarrow$ wordt gebruikt voor de relatie van *direct gevolg*: wat rechts van $\models\!\!\Longrightarrow$ staat kan direct worden geconcludeerd uit wat links staat.

Operationele beschrijving. Als je gebruik wilt maken van een *gegeven* van de vorm $P \rightarrow Q$, probeer dan (eerst) P te bewijzen; $\rightarrow$E stelt je dan in staat om, gebruik makend van $P \rightarrow Q$, de conclusie Q te trekken.

Motivering. Onnodig. De betekenis van een implicatie $P \rightarrow Q$ is immers precies dat als P waar is, Q dat óók is.

$\rightarrow$I, Introductie regel voor $\rightarrow$, deductie regel.

Operationele beschrijving. Als je $P \rightarrow Q$ moet bewijzen, neem dan P als nieuw gegeven aan, en probeer een bewijs te vinden van Q. Lukt dat, dan kan (volgens $\rightarrow$I) $P \rightarrow Q$ als bewezen gelden.

Motivering. Je weet (waarheidstafel $\rightarrow$) dat als P onwaar is, $P \rightarrow Q$ waar is. Dus er valt alleen nog iets te bewijzen, als P waar is; nl.: dat Q dan óók waar is. Daarom is het aannemen van P als extra gegeven gerechtvaardigd.

In de praktijk gebruik je de deductie regel aangekleed op de volgende manier.

> *Gegeven:* ...
> *Te bewijzen:* $P \rightarrow Q$.
> *Bewijs:* Onderstel, dat (naast het eerdere *gegeven*) P geldt. Hier volgt een bewijs, dat Q geldt: (... volgt dat bewijs ...) Dus, Q. $\dashv$
> Concluderend: (= deductie regel!), $P \rightarrow Q$. $\dashv$

Overigens wordt de laatste, concluderende regel (de eigenlijke toepassing van de deductie regel) vaak aan de goede verstaander overgelaten.

Een enigszins andere inkleding van het gebruik van de deductie regel, die het reducerend karakter onthult, (met een nieuw *gegeven*, *te bewijzen* en *bewijs*) zie je in het voorbeeld hierna.

In de praktijk zul je misschien nog andere regels gebruiken voor $\rightarrow$, maar in de regel zullen die uit deze twee volgen, en heten daarom *afgeleid*. Een voorbeeld van een afgeleide regel is de volgende:

$$P \rightarrow Q,\; Q \rightarrow R \;\models\!\!\Longrightarrow\!\!\Longrightarrow\; P \rightarrow R.$$

Hierin is de notatie $\models\!\!\Rightarrow$ gebruikt om een gevolgtrekking aan te geven die misschien niet *direct* is.

Een bewijs hiervan m.b.v. $\rightarrow$E en $\rightarrow$I gaat als volgt:

Gegeven: $P \rightarrow Q, Q \rightarrow R$
Te bewijzen: $P \rightarrow R$
Bewijs: Volgens $\rightarrow$I moet je P als gegeven toevoegen en proberen om R te bewijzen. Dit creëert de volgende nieuwe situatie:

Gegeven: $P \rightarrow Q, Q \rightarrow R$ (oud), P (nieuw)
Te bewijzen: R
Bewijs: $\rightarrow$E toepassend op P en $P \rightarrow Q$ levert Q;
$\rightarrow$E nogmaals toepassend op Q en $Q \rightarrow R$ levert tenslotte R. ⊣
$\rightarrow$I levert nu het gevraagde. ⊣

N.B.: de notatie $\models\!\!\Rightarrow$ kan worden gebruikt voor een compactere formulering van de deductie regel:

$$\text{als } \Gamma, P \models\!\!\Rightarrow Q, \text{ dan } \Gamma \models\!\!\Rightarrow (P \rightarrow Q).$$

Hierin staat Γ voor een willekeurige rij van gegevens.

5 ♣ Opgave. Laat zien dat de regel $P \rightarrow Q,\ P \rightarrow (Q \rightarrow R) \models\!\!\Rightarrow P \rightarrow R$ kan worden afgeleid uit $\rightarrow$E en $\rightarrow$I.

Wat hierboven is verteld m.b.t. $\rightarrow$ geldt ongeveer netzo voor de andere logische operaties — alleen de détails van de regels zijn natuurlijk anders. Hieronder worden ze stuk voor stuk behandeld.

Conjunctie

De regels voor $\wedge$ zijn volledig onproblematisch.

$\wedge$E, Eliminatie regels voor $\wedge$.

$$P \wedge Q \models\!\!\Rightarrow P,$$

$$P \wedge Q \models\!\!\Rightarrow Q$$

(uit een conjunctie volgen beide leden direct).

$\wedge$I, Introductie regel voor $\wedge$.

$$P, Q \models\!\!\Rightarrow P \wedge Q$$

(een conjunctie volgt direct uit zijn beide leden).

Equivalentie

Omdat een equivalentie kan worden opgevat als een conjunctie van twee implicaties, liggen de regels voor $\leftrightarrow$ nu voor de hand.

$\leftrightarrow$E, Eliminatie regels voor $\leftrightarrow$.

$$P \leftrightarrow Q,\ P \ \models\!\!\!\Longrightarrow\ Q,$$

$$P \leftrightarrow Q,\ Q \ \models\!\!\!\Longrightarrow\ P.$$

$\leftrightarrow$I, Introductie regel voor $\leftrightarrow$. Als je $P \leftrightarrow Q$ moet bewijzen, dan worden *twee* dingen verlangd:

($\rightarrow$) neem P als nieuw gegeven aan, en probeer een bewijs te vinden van Q;

($\leftarrow$) neem Q als nieuw gegeven aan, en probeer een bewijs te vinden van P.

Lukt dit, dan kan $P \leftrightarrow Q$ als bewezen gelden.

In de praktijk kleed je dit als volgt in.

Te bewijzen: $P \leftrightarrow Q$.
Bewijs:
$P \rightarrow Q$: onderstel, dat P. (Volgt bewijs, dat Q.)
$Q \rightarrow P$: onderstel, dat Q. (Volgt bewijs, dat P.) $\dashv$

6 ♣ Opgave. Bewijs de regels $P \leftrightarrow Q \ \models\!\!\!\Longrightarrow\ (P \rightarrow R) \leftrightarrow (Q \rightarrow R)$ en $P \leftrightarrow Q \ \models\!\!\!\Longrightarrow\ (R \rightarrow P) \leftrightarrow (R \rightarrow Q)$ m.b.v. de voor $\rightarrow$ en $\leftrightarrow$ gegeven regels.

Negatie

$\neg$E, Eliminatie regel voor $\neg$.

Operationele beschrijving. Als $\neg P$ is gegeven, probeer dan ook nog P te bewijzen. Lukt dit, dan staat $\neg$E je *iedere* gewenste conclusie toe.

$\neg$I, Introductie regel voor $\neg$.

Operationele beschrijving. Als je $\neg P$ moet bewijzen, neem dan P als nieuw gegeven aan en probeer een bewijs te vinden van iets dat *evident onwaar* is. Lukt dat, dan geldt $\neg P$ als bewezen.

Voorbeeld van een evidente onwaarheid in deze context (waarin P als nieuw gegeven wordt aangenomen) is $\neg P$. Maar in een concrete wiskundige context kan dit ook zijn, dat $0 = 1$ e.d.

Merk op: $\neg$I zegt dat je, bij het bewijzen van $\neg P$, altijd gratis over het gegeven P kunt beschikken. Zie het voorbeeld bij Opgave 7.

BO, Bewijs uit het Ongerijmde.

Operationele beschrijving. (Vergelijk dit met ¬I.) Om P te bewijzen neem je $\neg P$ als (extra) gegeven aan, en je probeert daarmee een evidente onwaarheid te bewijzen. Lukt dat, dan geldt P volgens BO als bewezen.

Het idee van dit bewijspatroon is het volgende: als een aperte onwaarheid m.b.v. $\neg P$ kan worden bewezen, dan betekent dat dat $\neg P$ incorrect is. Dan moet (dus) P gelden.

In Sectie 7.1 wordt dit als een eliminatie regel geklassificeerd, maar eigenlijk is dit dubieus.

Advies. De bewijsfiguur Bewijs uit het Ongerijmde is een noodsprong: bedoeld voor gevallen waarin je geen andere mogelijkheid ziet. Grijp hier dus niet te gauw naar, en probeer het eerst rechtstreeks: zo'n bewijs is altijd eleganter en informatiever dan één met BO.

7 ♣ Opgave. Bewijs:

1. $P \to Q \Longmapsto \neg Q \to \neg P$,
2. $\neg Q \to \neg P \Longmapsto P \to Q$,
3. $P \leftrightarrow Q \Longmapsto \neg P \leftrightarrow \neg Q$.

Voorbeeld: 2.
Pas de deductie regel toe en reduceer het probleem tot $\neg Q \to \neg P,\ P \Longmapsto Q$. Toepassen van BO reduceert dit tot het probleem om een evidente onwaarheid te bewijzen op grond van gegevens $\neg Q \to \neg P$, P en $\neg Q$. Dit is makkelijk: met modus ponens volgt uit eerste en laatste gegeven, dat $\neg P$; de evidente onwaarheid hiervan volgt uit de aanwezigheid van P onder de gegevens.

Disjunctie

∨ E, Eliminatie regel voor ∨. Als je het gegeven $P \vee Q$ wilt gebruiken bij het bewijs van een bewering R, geef dan *twee* bewijzen: één van R uit het nieuwe gegeven P, en één van R uit het nieuwe gegeven Q.

In de praktijk kan dit als volgt worden ingekleed.

Gegeven: $P \vee Q$.
Te bewijzen: R.
Bewijs: (Uit het gegeven volgt, dat (i) P of (ii) Q.)
(i) Stel dat P. (Volgt een bewijs dat R.)
(ii) Stel dat Q. (Volgt nog een bewijs dat R.) ⊣

∨ I, Introductie regels voor ∨.

$$P \Longmapsto P \vee Q,$$

$$Q \Longmapsto P \vee Q$$

(een disjunctie volgt direct uit ieder van zijn disjuncten).

8 ♣ Opgave. Bewijs: $P \vee Q, \neg P \Longmapsto Q$.

Universele Kwantor

∀E, Eliminatie regel voor ∀, instantiatie regel.

$$\forall x\, E(x) \;\models\!\Longrightarrow\; E(t)$$

waarbij t een vrij te kiezen ding is (dat, normaal gesproken, al eerder in de argumentatie is opgetreden). ("Als voor ieder ding x geldt, dat $E(x)$, dan geldt het i.h.b. voor $x := t$.")

∀I, Introductie regel voor ∀, generalisatie regel. Als je moet bewijzen, dat $\forall x\, E(x)$, dan zeg je: "Laat c een willekeurig ding zijn (van de relevante soort)", en je probeert vervolgens voor *dit* ding (waarover je geen extra informatie mag aannemen, en dat dus *niet* al eerder in de argumentatie is opgetreden) te bewijzen, dat het eigenschap E heeft.

2.1 Willekeurige dingen. De bij ∀I gegeven uitleg heeft het over *willekeurige dingen*. Maar wat zijn dat? Wat is bijvoorbeeld een willekeurig natuurlijk getal? Een getal dat niet groot is, niet klein, niet priem, maar ook niet samengesteld? Zijn er ook *onwillekeurige* natuurlijke getallen?

De vragen stellen, is ze beantwoorden: de lading van de bepaling 'willekeurig' is niet van wiskundige aard, maar alleen van psychologische. Willekeurige dingen bestaan niet. Zuiverder is het, om de bepaling 'willekeurig' te vermijden. (Dat advies wordt hier overigens niet altijd gevolgd.) De uitleg bij ∀I wordt daar niet onduidelijker van.

9♣ Opgave. Het volgende patroon kun je vaak in de praktijk gebruiken. Onderstel dat voor een willekeurig ding c geldt, dat $\Gamma, E_1(c) \models\!\Longrightarrow E_2(c)$. Toon aan, dat $\Gamma \models\!\Longrightarrow \forall x(E_1(x) \to E_2(x))$.

Existentiële Kwantor

∃E, Eliminatie regel voor ∃. (Dit lijkt enigszins op ∨E.) Als je het gegeven $\exists x\, E(x)$ wilt gebruiken om te bewijzen, dat P geldt, dan zeg je: "Laat c een ding zijn waarvoor $E(c)$ geldt." (maar dat is dan ook alles, wat je over c mag aannemen), en je probeert hiermee P te bewijzen.

∃I, Introductie regel voor ∃.

$$E(t) \;\models\!\Longrightarrow\; \exists x\, E(x)$$

waarbij t ieder ding mag zijn wat je maar wilt.

Tabel

De volgende tabel geeft een visuele samenvatting van de boven besproken regels. Hierin is het teken ⊥ van Hoofdstuk 7.1 gebruikt als symbool voor een (evident) onware bewering. In de praktijk kan dat natuurlijk van alles zijn, zoals: $1 = 0$,

$P \wedge \neg P$ (P e.o.a. bewering), enz. Vergelijk de tabel op blz. 90. In de kwantorregels staat c voor (de naam van) een ("willekeurig") ding waarover verder geen onderstellingen gemaakt mogen zijn; a is (de naam van) e.o.a. specifiek ding waarvan de keuze vrij is.

	introductie	*eliminatie*
$\rightarrow$	$\begin{array}{c} P \\ \vdots \\ Q \\ \hline P \rightarrow Q \end{array}$	$\dfrac{P \quad P \rightarrow Q}{Q}$
$\leftrightarrow$	$\begin{array}{c} P \quad Q \\ \vdots \quad \vdots \\ Q \quad P \\ \hline P \leftrightarrow Q \end{array}$	$\dfrac{P \quad P \leftrightarrow Q}{Q} \qquad \dfrac{Q \quad P \leftrightarrow Q}{P}$
$\neg$	$\begin{array}{c} P \\ \vdots \\ \bot \\ \hline \neg P \end{array}$	$\begin{array}{c} \neg P \\ \vdots \\ \bot \\ \hline P \end{array} \qquad \dfrac{P \quad \neg P}{Q}$
$\wedge$	$\dfrac{P \quad Q}{P \wedge Q}$	$\dfrac{P \wedge Q}{P} \qquad \dfrac{P \wedge Q}{Q}$
$\vee$	$\dfrac{P}{P \vee Q} \qquad \dfrac{Q}{P \vee Q}$	$\begin{array}{c} P \quad Q \\ \vdots \quad \vdots \\ P \vee Q \quad R \quad R \\ \hline R \end{array}$
$\forall$	$\dfrac{E(c)}{\forall x\, E(x)}$	$\dfrac{\forall x\, E(x)}{E(a)}$
$\exists$	$\dfrac{E(a)}{\exists x\, E(x)}$	$\begin{array}{c} E(c) \\ \vdots \\ \exists x\, E(x) \quad P \\ \hline P \end{array}$

2.3 Taktiek

Hier volgen een aantal handreikingen voor het oplossen van bewijsproblemen.

Doe het niet zó:

Probeer de (voor beginners, begrijpelijke) neiging te onderdrukken, met het *gegeven* te beginnen en te proberen dat op de één of andere manier in het *te bewijzen* te transformeren.

... maar doe het zó:

Kijk eerst naar (de vorm van) het *te bewijzen.*

Een aantal bewijsregels stellen je in staat om een vereenvoudiging van het bewijsprobleem te bewerkstelligen. Bijvoorbeeld:

- als je een implicatie $P \to Q$ moet bewijzen, dan kun je P aan de gegevens toevoegen en proberen Q te bewijzen (deductieregel),
- als je een negatie $\neg P$ moet bewijzen, dan kun je P aan de gegevens toevoegen en proberen een evidente onwaarheid te bewijzen ($\neg$-introductie),
- als je een universele kwantificatie $\forall x\ E(x)$ moet bewijzen, dan kun je ook proberen om $E(c)$ te bewijzen voor een "willekeurig" ding c (van de geschikte soort) ($\forall$-introductie).

Pas nadat je het bewijsprobleem op deze manier zoveel mogelijk hebt gereduceerd kijk je naar het *gegeven* om te zien, hoe dat gebruikt kan worden.

Gebruik *bewijs uit het ongerijmde* (bij *te bewijzen* P, toevoegen van $\neg P$ als *gegeven* en vervolgens proberen om een evidente onwaarheid te bewijzen) alleen als laatste redmiddel.

2.4 Voorbeelden uit de Analyse

Onderstel dat $a_0, a_1, a_2, \ldots$ een rij reële getallen is en dat $a \in \mathbb{R}$. Dan is de uitdrukking $\lim_{i\to\infty} a_i = a$ ("de a_i convergeren naar a") per definitie equivalent met:

$$\forall \varepsilon > 0\ \exists n\ \forall i \geqslant n\ (|a - a_i| < \varepsilon).$$

2.2 Lemma. *Een rij reële getallen heeft hoogstens één limiet.*

Bewijs. Het gevraagde kan als volgt worden ingekleed.
Gegeven: $\lim_{i\to\infty} a_i = a$, $\lim_{i\to\infty} a_i = b$.
Te bewijzen: $a = b$.
Bewijs: Ondanks de waarschuwing boven is een *bewijs uit het ongerijmde* hier niet zo'n gek idee, omdat het nieuwe *gegeven* $\neg(a = b)$, dat is: $a \neq b$, hier equivalent is met het positieve: $|a - b| > 0$. Neem dat dus aan.

Om van de oude gegevens gebruik te kunnen maken moet je ($\forall$E !) een waarde voor ε kiezen. Een zoals blijken zal nuttige keuze is $\varepsilon := \frac{1}{2}|a - b|$. (N.B.: $\varepsilon > 0$.)

Nu geldt ($\forall$E toegepast op $\lim_{i\to\infty} a_i = a$), dat $\exists n\, \forall i \geqslant n\, (|a - a_i| < \varepsilon)$. Dus bestaat ($\exists$E !) n_1 zódat $\forall i \geqslant n_1\ (|a - a_i| < \varepsilon)$. Omdat $\lim_{i\to\infty} a_i = b$ bestaat netzo ($\exists$E) n_2 zódat $\forall i \geqslant n_2 (|b - a_i| < \varepsilon)$. Laat $n := max(n_1, n_2)$, dan geldt dus ($n \geqslant n_1, n_2$, $\forall$E) i.h.b. dat $|a - a_n| < \varepsilon$ en $|b - a_n| < \varepsilon$. Maar dit is kennelijk onmogelijk: m.b.v. de zgn. *driehoeksongelijkheid:*

$$|x + y| \leqslant |x| + |y|$$

(een in de analyse veelgebruikt hulpmiddel; de naam wordt duidelijk als je bedenkt dat dit ook geldt als x en y complexe getallen zijn) volgt, dat: $|a - b| = |a - a_n + a_n - b| \leqslant |a - a_n| + |b - a_n| < 2\varepsilon = |a - b|$ — en dit is de gezochte tegenspraak. ⊣

Opgaven

10 ♣ Onderstel, dat $\lim_{i\to\infty} a_i = a$. Bewijs, dat $\lim_{i\to\infty} a_{2i} = a$.
Beter: onderstel, dat $f : \mathbb{N} \to \mathbb{N}$ een functie is zódat $\forall n \exists m \forall i \geqslant m\ f(i) \geqslant n$. Bewijs, dat $\lim_{i\to\infty} a_{f(i)} = a$.

11 ♣ Onderstel, dat de rijen reële getallen $\{a_n\}_{n=0}^{\infty}$ en $\{b_n\}_{n=0}^{\infty}$ limieten a resp. b hebben, terwijl geldt dat $a < b$.
Bewijs dat een getal n bestaat zódat $\forall m \geqslant n\ (a_m < b_m)$.

12 ♣ Onderstel, dat $\lim_{i\to\infty} a_i = a$ en dat $\lim_{i\to\infty} b_i = b$.
Bewijs, dat $\lim_{i\to\infty}(a_i + b_i) = a + b$.

13 ♣ Een rij reële getallen $\{a_n\}_{n=0}^{\infty}$ heet een *Cauchy* rij als $\forall \varepsilon > 0\ \exists n\ \forall i, j \geqslant n\ (|a_i - a_j| < \varepsilon)$. Bewijs: als $\{a_n\}_{n=0}^{\infty}$ een Cauchy rij is, dan bestaat $C > 0$ zódat $\forall i (|a_i| < C)$.
Aanwijzing: Neem $\varepsilon := 1$.

Het resultaat van de volgende opgave speelt een cruciale rol in de analyse bij bewijzen dat functies continu zijn. Omdat niet van je verwacht wordt dat je de oplossing op dit moment zelf kan vinden staat die erbij — het is een uitstekende illustratie van het gebruik van de bewijsregels van de kwantoren. Het enige dat op dit moment van je wordt verwacht, is: nagaan dat de regels hier correct worden toegepast, en vervolgens het bewijs *begrijpen*, dat is: inzien dat de argumentatie het gevraagde ondubbelzinnig vaststelt.

14 ♣♣ Bewijs dat de *compositie* van twee continue functies f en g — dat is: de functie h gedefinieerd door $h(x) := g(f(x))$, zie Definitie 5.7 (blz. 56) — weer continu is.
Oplossing.
Gegeven: f en g continu, d.w.z. (ε-δ-definitie, 1.1 blz. 13)

$$\forall x\ \forall \varepsilon > 0\ \exists \delta > 0\ \forall y\ (|x - y| < \delta \implies |f(x) - f(y)| < \varepsilon), \tag{2.1}$$

$$\forall a\ \forall \varepsilon > 0\ \exists \delta > 0\ \forall b\ (|a - b| < \delta \implies |g(a) - g(b)| < \varepsilon). \tag{2.2}$$

Te bewijzen: $\forall x\ \forall \varepsilon > 0\ \exists \delta > 0\ \forall y\ (|x - y| < \delta \implies |g(f(x)) - g(f(y))| < \varepsilon)$.
Bewijs: Omdat het *te bewijzen* begint met twee universele kwantoren — $\forall x$ en $\forall \varepsilon > 0$ — begint het verhaal — $\forall$I ! — met het fixeren van twee willekeurige waarden $x \in \mathbb{R}$ en $\varepsilon > 0$.
Gegeven (2.2) kan nu worden gebruikt d.m.v. $\forall$E door waarden voor a en ε te specificeren. Er zal blijken, dat $a := f(x)$ en de eerder gekozen ε nuttige keuzen zijn. Vervolgens levert (2.2) je — $\exists$E ! — een $\delta_1 > 0$ zódat

$$\forall b\ (|f(x) - b| < \delta_1 \implies |g(f(x)) - g(b)| < \varepsilon). \tag{2.3}$$

Gegeven (2.1) toepassend met *onze* x en $\varepsilon := \delta_1$ ($\forall$E) krijg je ($\exists$E) een $\delta > 0$ zódat

$$\forall y\ (|x - y| < \delta \implies |f(x) - f(y)| < \delta_1). \tag{2.4}$$

Dit is de δ die je moet hebben; d.w.z.:
Claim: $\forall y\ (|x - y| < \delta \implies |g(f(x)) - g(f(y))| < \varepsilon)$. (Hieruit volgt het gevraagde met $\exists$I.)
Bewijs: Laat ($\forall$I, $\to$I — of zie Opgave 9) $|x - y| < \delta$. Uit (2.4) (met *deze* y — $\forall$E) vind je, dat $|f(x) - f(y)| < \delta_1$.
Uit (2.3) (met $b := f(y)$ — $\forall$E) vind je tenslotte, dat $|g(f(x)) - g(f(y))| < \varepsilon$. ⊣

Samenvatting

Vragen:

- noem zes van de tien geboden voor een "goed bewijs",
- noem de bewijsregels voor introductie en eliminatie van een aantal logische tekens.

Literatuur

Beknopte en praktische informatie over het bewijs in de wiskunde, met goede voorbeelden, geeft Devlin [4]. Veel uitvoeriger, speciaal over bewijzen in de wiskunde, is het uitstekende Velleman [15]. Nederpelt [11] gaat uitvoerig in op de taal van de wiskunde en de vorm van bewijzen, maar is ook moeilijk.

Hoofdstuk 3

Verzamelingen

3.1 Het Verzameling-begrip

Verzamelingen spelen een fundamentele rol in de hedendaagse wiskunde. Bekende en vertrouwde voorbeelden van verzamelingen zijn $\mathbb{N}$ — de verzameling van natuurlijke getallen 0, 1, 2,...; $\mathbb{Z}$ — de verzameling van gehele getallen 0, 1, 2,..., -1, -2,...; $\mathbb{Q}$ — de verzameling van rationale getallen (breuken), en $\mathbb{R}$ — de verzameling van alle reële getallen.

Een bevredigende *definitie* van het begrip verzameling is niet goed mogelijk; de gebruikelijke *axiomatische* benadering is die van Zermelo en Fraenkel (ZF).

Axiomas vs. Stellingen, Primitieve Begrippen vs. Definities. Zoals al gezegd, in de wiskunde wordt de waarheid van een bewering gewoonlijk vastgesteld door een bewijs. De meeste bewijzen maken gebruik van hypothesen die eerder bewezen zijn. Om ergens te kunnen beginnen moeten sommige beweringen worden geaccepteerd zonder bewijs. De keuze, welke dat zijn, is soms nogal willekeurig, maar soms ook niet (criteria: eenvoud, intuïtieve evidentie), of wordt bepaald door natuurlijke afperking van het onderwerp (een bewijs kan, binnen de gegeven context, niet voorhanden zijn). Zonder bewijs geaccepteerde beweringen heten *axiomas*. Voorbeelden hier zijn de soms genoemde verzamelingstheoretische axiomas van ZF zoals Extensionaliteit 3.2. Verder worden als axioma geaccepteerd het principe van Volledige Inductie 6.1 voor de natuurlijke getallen en sommige eigenschappen van de ordening van de verzameling $\mathbb{R}$ van reële getallen (Sectie 10.4 blz. 141). Beroemde axiomas zijn die van Euclides voor de meetkunde.

Bewezen beweringen heten *stellingen* (als ze een belangrijk geacht inzicht vertegenwoordigen), *lemmas* (als ze als hulpje dienen in andere bewijzen), of *proposities*.

Een analoge tweedeling doet zich voor t.a.v. begrippen. Gewoonlijk worden nieuwe begrippen *gedefinieerd* door *definities* die hun betekenis ondubbelzinnig vastleggen in termen van andere begrippen. Maar tenslotte moet natuurlijk van bepaalde, zgn. *primitieve* begrippen worden uitgegaan zonder dat daarvoor

definities (kunnen) worden gegeven. Voorbeelden van begrippen die hier als primitief worden beschouwd zijn: *verzameling* (een reductie tot andere begrippen is problematisch) en *natuurlijk getal* (een verzamelingstheoretische definitie is mogelijk maar wordt niet gegeven). Een gedefinieerd begrip is dat van een *functie*. Maar: in een behandeling waarin het verzamelingsbegrip niet centraal staat zou dat heel goed als primitief kunnen worden beschouwd.

Georg Cantor (1845-1915), de grondlegger van de verzamelingentheorie, gaf de volgende omschrijving.

Het Comprehensie-principe. *Een verzameling is de samenvatting tot één geheel van bepaalde wel-onderscheiden objekten van ons denken.*

De objekten die op deze manier tot één geheel worden samengevat heten de *elementen* van de verzameling.

Gewoonlijk worden voor de elementen van een verzameling objekten gebruikt, die zelf geen verzameling zijn. Omgaan met zulke verzamelingen is meestal onproblematisch. Maar er wordt nergens uitgesloten dat elementen ook verzamelingen zijn, en dat je in de praktijk dus verzamelingen van verzamelingen van ... verzamelingen kunt tegenkomen.

3.1 Notatie.

1. Als het objekt a tot de verzameling A behoort, dan heet a *element van* A. Notatie: $a \in A$.

2. Als a *geen* element van A is, d.w.z. als $\neg(a \in A)$, dan wordt dit geschreven als: $a \notin A$.

Dus, $0 \in \mathbb{N}$, $\frac{1}{2} \notin \mathbb{N}$, $\frac{1}{2} \in \mathbb{Q}$.

Een verzameling wordt volledig door zijn elementen bepaald: dat is de inhoud van het volgende *Extensionaliteitsaxioma.*

3.2 Extensionaliteits Axioma. *Verzamelingen met dezelfde elementen zijn gelijk. M.a.w., voor alle verzamelingen A en B geldt*

- $\forall x[x \in A \Leftrightarrow x \in B] \Longrightarrow A = B.$ ⊣

In deze formulering zijn verschillende variabelen gebruikt voor twee verschillende soorten van objekten: hoofdletters A en B voor verzamelingen en een kleine letter x voor willekeurige dingen. Zie Opmerking 1.12 (blz. 14) over soorten.
N.B.: de omkering van dit axioma, dat gelijke verzamelingen dezelfde elementen hebben, spreekt vanzelf.
Extensionaliteit maakt deel uit van iedere gangbare axiomatiek, i.h.b. van ZF. Sommige andere axiomas worden vermeld op de daartoe geëigende plaats.

3.2 Hoe Noteer Je een Verzameling

Een verzameling met niet teveel (in ieder geval: eindig veel) elementen $a_1, \ldots, a_n$ kan worden aangegeven met de notatie

$$\{a_1, \ldots, a_n\}$$

die de elementen van de verzameling opsomt. Het Extensionaliteitsaxioma zegt, dat deze notatie een welbepaalde verzameling vastlegt. Dus, $\{0, 2, 3\}$ is de verzameling waarvan de elementen zijn: 0, 2 en 3. Er geldt kennelijk $3 \in \{0, 2, 3\}$, maar $4 \notin \{0, 2, 3\}$. Natuurlijk geldt bijvoorbeeld, dat $\{0, 2, 3\} = \{2, 3, 0\} = \{3, 2, 2, 0\}$: al deze verzamelingen hebben immers *dezelfde* elementen.

- Volgorde en herhalingen in de opsomming zijn irrelevant.

Een verzameling met (oneindig) veel elementen kan zo niet worden weergegeven, tenzij er sprake is van een duidelijk *systeem* in de opsomming. Bijvoorbeeld, $\mathbb{N} = \{0, 1, 2, \ldots\}$ is de verzameling van alle natuurlijke getallen, en $\{0, 2, 4, \ldots\}$ de verzameling van alle *even* natuurlijke getallen: waar '...' hier voor staat, is wel duidelijk. Maar vaak is het beter, om '...' te vermijden, en voor een andere omschrijving te kiezen.

Als E een eigenschap is van objecten, dan wordt met de notatie $E(x)$ bedoeld, dat het ding x de eigenschap E heeft. De *abstractie*-notatie

$$\{\, x \mid E(x) \,\} \tag{3.1}$$

(ook wel: $\{x : E(x)\}$) staat voor de verzameling van alle dingen x die de eigenschap E hebben. Dus, voor ieder ding a is de uitdrukking

$$a \in \{\, x \mid E(x) \,\}$$

equivalent met

$$E(a).$$

Wegens het Extensionaliteitsaxioma kan inderdaad worden gesproken van *de* verzameling van dingen x waarvoor $E(x)$ geldt.

Merk ook op, dat het object $\{x \mid E(x)\}$ in geen enkel opzicht van de (waarde van de) variabele x afhangt. Dus: de abstractie-notatie bindt kennelijk de erin optredende variabele: een nieuw voorbeeld van variabelenbinding.

In de regel zal E betrekking hebben op de elementen van een vooraf gegeven verzameling A. Dan is

$$\{\, x \in A \mid E(x) \,\}$$

de verzameling van alle elementen van A die eigenschap E hebben. Zo kan de verzameling van even natuurlijke getallen worden aangegeven door

$$\{\, n \in \mathbb{N} \mid n \text{ is even} \,\}.$$

Een variatie op deze notatie is de volgende. Als f een operatie is die objecten toevoegt aan objecten met de eigenschap E, dan staat de notatie

$$\{\, f(x) \mid E(x) \,\}$$

voor de verzameling van alle dingen van de vorm $f(x)$ waarbij x eigenschap E moet hebben. Bijvoorbeeld

$$\{\, 2n \mid n \in \mathbb{N} \,\}$$

is weer een andere notatie voor de verzameling van even natuurlijke getallen. Als f of E nog andere parameters naast x bevatten, dan kan deze notatie overigens dubbelzinnig worden, omdat niet meer duidelijk hoeft te zijn, welke variabele als gebonden moet worden beschouwd en welke als vrij. En er is altijd een alternatief dat niet dubbelzinnig is:

$$\{\, f(x) \mid E(x) \,\} \;=\; \{\, y \mid \exists x\, [y = f(x) \;\wedge\; E(x)] \,\}.$$

***Russell paradox.** Het is niet zo, dat *iedere* eigenschap E een corresponderende verzameling $\{x \mid E(x)\}$ heeft. Cantor wist dit al (hoewel zijn Comprehensie Principe anders doet vermoeden), en Russell gaf een bizonder eenvoudig voorbeeld van een eigenschap zonder corresponderende verzameling, gedefinieerd door de conditie $x \notin x$. Als $R = \{\, x \mid x \notin x \,\}$ een verzameling was, dan gold kennelijk wegens het voorafgaande, dat

$$R \in R \iff R \notin R;$$

een propositionele contradictie. (Wat kan de waarheidswaarde zijn van de bewering $R \in R$?) Het verrassende inzicht, dat Cantor's Comprehensie Principe contradictoor is, staat bekend als de *Russell-paradox*.

Met het aannemen dat, voor gegeven verzameling A en eigenschap E, $\{\, x \in A \mid E(x)\}$ altijd een verzameling is — dat is Zermelo's *Aussonderung* of *Separatie Axioma* — kunnen we daarentegen niet in de problemen raken.

Als E een willekeurige eigenschap is, i.h.b. als E niet met een verzameling correspondeert, dan heet $\{x \mid E(x)\}$ wel een *collectie* of *klasse*. Zie de volgende opgaven voor meer voorbeelden. Later wordt beargumenteerd, dat de klasse van *ordinaalgetallen* geen verzameling is (zie Sectie 10.5). Overigens zullen de termen *collectie* en *klasse* hier meestal als synoniemen worden beschouwd van *verzameling*.

Opgaven

15 ♣ Bewijs, dat $\{\{1,2\},\{0\},\{2,1\}\} = \{\{0\},\{1,2\}\}$.

16 ♣♣ Bewijs dat er geen verzameling is, corresponderend met de eigenschap $F(x) :\equiv$ er is geen oneindige rij $x_0 = x \ni x_1 \ni x_2 \ni \ldots$.

17 ♣♣ Bewijs: iedere verzameling A heeft een *deelverzameling* $B \subset A$ (zie Definitie 3.3) zódat $B \notin A$. (Dus, er bestaat *geen verzameling van alle verzamelingen.*)
Aanwijzing. Gebruik de Russell-eigenschap of de eigenschap F van Opgave 16.

3.3 Bizondere Verzamelingen

Verzamelingen met maar één element heten *singletons*. De verzameling waarvan a het enige element is, is $\{ a \}$; hij heet de *singleton van* a.

Vaak wordt een singleton $\{a\}$ verward met z'n element a; maar in de meeste gevallen is het toch zo, dat $a \neq \{ a \}$. Bijvoorbeeld, voor $a = \{0, 1\}$: $\{0, 1\} \neq \{\{0, 1\}\}$. Want: $\{0, 1\}$ heeft twee elementen: de getallen 0 en 1, en $\{\{0, 1\}\}$ heeft er maar één: de verzameling $\{0, 1\}$.
Voor ieder ding x geldt

$$x \in \{ a \} \text{ d.e.s.d.a. } x = a.$$

Een verzameling van de vorm $\{a, b\}$ heet een ("ongeordend") *paar*. Natuurlijk, als $a = b$, dan is het paar $\{a, b\}$ feitelijk een singleton.

Tenslotte is er zelfs een verzameling *zonder* elementen: de *lege verzameling*. Dit curieuze objekt is vaak een bron van verdriet voor de beginnende student en (daarom?) van vermaak voor de cognoscenti. De notatie voor de lege verzameling is $\emptyset$. (Dat $\emptyset$ *bestaat*, volgt uit het Aussonderung Axioma. Als A een willekeurige verzameling is, dan geldt dat $\emptyset = \{x \in A \mid x \neq x\}$.) Natuurlijk is er maar één lege verzameling: dit volgt weer uit het Extensionaliteitsaxioma.

Voor ieder ding x geldt kennelijk

$$x \notin \emptyset.$$

Opgaven

18 ♣ Bewijs:

1. $\{ a \} = \{ b \}$ d.e.s.d.a. $a = b$,
2. $\{a_1, a_2\} = \{b_1, b_2\}$ d.e.s.d.a. $a_1 = b_1 \wedge a_2 = b_2$, of: $a_1 = b_2 \wedge a_2 = b_1$.

19 ♣ Beargumenteer, dat $\emptyset \neq \{\emptyset\}$. En dat $\{\emptyset\} \neq \{\{\emptyset\}\}$.

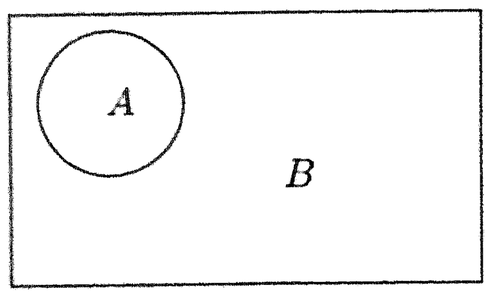
De vraag, of de vergelijking: $a = \{ a \}$ oplossingen heeft (of, algemener, of er verzamelingen a zijn, waarvoor $a \in a$) wordt door de verschillende axiomatieken voor de verzamelingentheorie verschillend beantwoord. De gedaante van een dergelijke verzameling kan als volgt worden beschreven: $a = \{\{\{\cdots \cdots\}\}\}$, maar dit is natuurlijk geen officiele notatie. Voor het "wiskundig gehalte" van de verzamelingentheorie is dit probleem overigens weinig relevant.

3.4 Verzamelingen algebra

3.3 Deelverzamelingen. De verzameling A heet *deelverzameling* van de verzameling B, en B *omvat* A, notaties: $A \subset B$ en $B \supset A$, als ieder element van A ook element van B is:

$$A \subset B :\equiv \forall x \, (x \in A \implies x \in B).$$

Als $A \subset B$ èn $A \neq B$, dan heet A een *echte* deelverzameling van B.



Bijvoorbeeld, $\{0,2\}$ is een echte deelverzameling van $\mathbb{N}$.
Waarschuwing. Vaak zie je $A \subset B$ genoteerd als $A \subseteq B$; de notatie $A \subset B$ zal in zo'n geval worden gebruikt als A een echte deelverzameling van B is.

$\in$ versus $\subset$. Beginners verwarren vaak $\in$ en $\subset$, maar deze relaties zijn toch heel verschillend. Bijvoorbeeld, $A \subset B$ impliceert dat A en B beide verzamelingen zijn, terwijl $a \in B$ alleen impliceert dat B er één is. Aangenomen dat getallen geen verzamelingen zijn geldt dat $1 \in \{0,1,2\}$, maar $1 \not\subset \{0,1,2\}$; terwijl $\{1\} \subset \{0,1,2\}$, en $\{1\} \not\in \{0,1,2\}$. (Zie ook Opgave 17.)

3.4 Stelling. *Voor alle verzamelingen A, B, C geldt:*

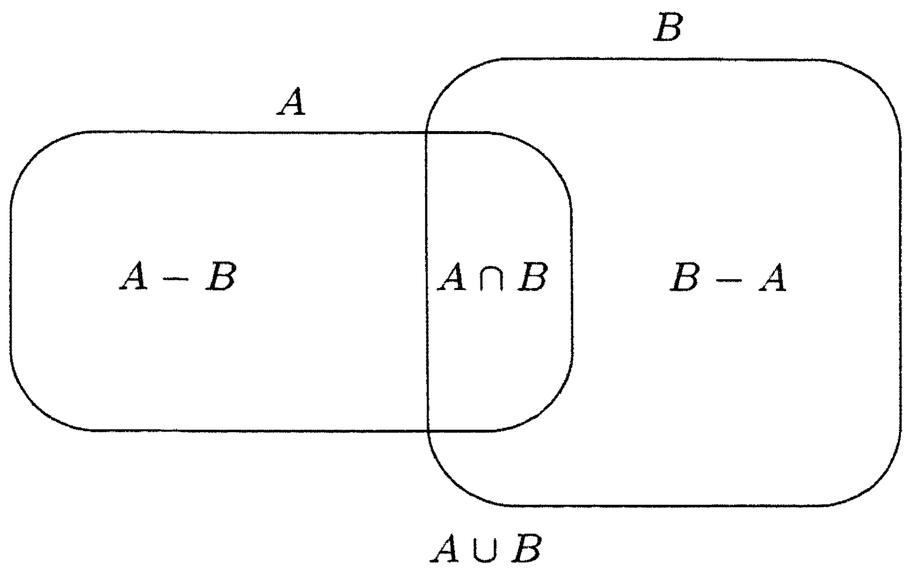
1. $\emptyset \subset A$,
2. $A \subset A$ *(reflexiviteit)*,
3. $A \subset B \ \wedge \ B \subset A \implies A = B$ *(antisymmetrie)*,
4. $A \subset B \ \wedge \ B \subset C \implies A \subset C$ *(transitiviteit)*.

Bewijs. 1. $\emptyset \subset A$ zegt: $\forall x(x \in \emptyset \ \Rightarrow \ x \in A)$. Nu geldt dat, ongeacht de keuze van x, de implicatie $x \in \emptyset \ \Rightarrow \ x \in A$ *waar* is: het linkerlid is immers altijd *onwaar*. Zie de waarheidstafel van de implicatie. Dit is één van die gevallen, waarin een implicatie "triviaal waar" is.
2. Een implicatie $x \in A \ \Rightarrow \ x \in A$ is waar, ongeacht de keuze van x.
3. Dit is precies het Extensionaliteitsaxioma — in een iets andere vorm.
4. Onderstel, dat $A \subset B$ en $B \subset C$. Neem een willekeurig element x van A. Wegens de eerste onderstelling geldt dan ook $x \in B$. De tweede onderstelling levert de conclusie, dat $x \in C$.
Er is nu bewezen ($\forall$I), dat $\forall x(x \in A \ \Rightarrow \ x \in C)$, d.w.z. dat $A \subset C$.
Het laatste uitvoeriger, met vermelding van de regels van Hoofdstuk 2:
Gegeven: $A \subset B$ (i), $B \subset C$ (ii).
Te Bewijzen: $A \subset C$.
Bewijs: M.a.w., $\forall x(x \in A \ \Rightarrow \ x \in C)$. Laat dus (aansturend op $\forall$I) x een "willekeurig" ding zijn.
Claim. $x \in A \ \Rightarrow \ x \in C$.
Onderstel immers (aansturend op $\Rightarrow$I) $x \in A$. Dan geldt volgens (i) ook, dat $x \in B$, en dus volgens (ii), dat $x \in C$.
$\Rightarrow$I: Dit bewijst de claim.
$\forall$I: Dit bewijst $A \subset C$. ⊣

3.5 Doorsnede, Vereniging, Verschil. Onderstel, dat A en B verzamelingen zijn.

1. $A \cap B := \{\, x \mid x \in A \wedge x \in B \,\}$ heet de *doorsnede* van A en B,
2. $A \cup B := \{\, x \mid x \in A \vee x \in B \,\}$ de *vereniging*, en
3. $A - B := \{\, x \mid x \in A \wedge x \notin B \,\}$ het *verschil* van A en B.

In plaats van $A - B$ zie je ook wel de notatie $A \setminus B$.



$\cap$, $\cup$ versus $\wedge$, $\vee$. Vaak worden de tekens $\cap$ en $\cup$ verward met de connectieven $\wedge$ en $\vee$. Aan Definitie 3.5 is te zien, dat er een nauwe relatie tussen deze twee stellen bestaat, maar in hun "grammaticaal gedrag" is er een groot verschil: $\cap$ en $\cup$ produceren, gegeven twee verzamelingen A en B, nieuwe verzamelingen $A \cap B$ resp. $A \cup B$ (dus $\cap$ en $\cup$ kunnen alleen voorkomen tussen verzamelingen), terwijl met $\wedge$ en $\vee$ (die alleen tussen beweringen kunnen voorkomen) twee beweringen Φ en Ψ tot nieuwe beweringen $\Phi \wedge \Psi$ resp. $\Phi \vee \Psi$ kunnen worden samengesteld. Het verband wordt duidelijker als je Definitie 3.5 in de vorm van een aantal equivalenties giet:

1. $x \in A \cap B \iff x \in A \wedge x \in B$,
2. $x \in A \cup B \iff x \in A \vee x \in B$,
3. $x \in A - B \iff x \in A \wedge x \notin B$.

3.6 Disjunct. Verzamelingen A en B heten *disjunct* als $A \cap B = \emptyset$.

Voorbeeld. Voor $A = \{1, 2, 3\}$ en $B = \{3, 4\}$ geldt: $A \cup B = \{1, 2, 3, 4\}$, $A \cap B = \{3\}$ en $A - B = \{1, 2\}$. A en B zijn niet disjunct, want $3 \in A \cap B$.

Sommige onderdelen van de volgende stelling corresponderen met onderdelen van Stelling 1.5, blz. 10.

3.7 Stelling. *Voor alle verzamelingen A, B en C gelden de volgende regels:*

1. $A \cap \emptyset = \emptyset$; $A \cup \emptyset = A$,
2. $A \cap A = A$; $A \cup A = A$ *(idempotentie)*,
3. $A \cap B = B \cap A$; $A \cup B = B \cup A$ *(commutativiteit)*,
4. $A \cap (B \cap C) = (A \cap B) \cap C$; $A \cup (B \cup C) = (A \cup B) \cup C$ *(associativiteit)*,
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributiviteit)*.

Onderdeel 3.7.4 is ervoor verantwoordelijk dat in herhaalde doorsneden en verenigingen haakjes mogen worden weggelaten.

Bewijs. Bijvoorbeeld, de eerste distributiewet: voor een willekeurig element x geldt

$$\begin{aligned} x \in A \cap (B \cup C) &\iff x \in A \wedge x \in B \cup C \\ &\iff x \in A \wedge (x \in B \vee x \in C) \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \quad \text{(1.5.4, blz. 10)} \\ &\iff x \in A \cap B \vee x \in A \cap C \\ &\iff x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Conclusie: voor iedere x geldt: $x \in A \cap (B \cup C) \iff x \in (A \cap B) \cup (A \cap C)$. Het Extensionaliteitsaxioma zorgt nu voor de gewenste gelijkheid. Het bewijs komt kennelijk neer op een serie equivalenties: afbreken van de verzamelingstheoretische uitdrukking m.b.v. de definities van $\cap$ en $\cup$, vervolgens een toepassing van de corresponderende distributiewet uit de propositie-logica (in dit geval 1.5.4); en daarna weer de gezochte verzamelingstheoretische uitdrukking opbouwen via de definities. Extensionaliteit vormt het sluitstuk.
De andere bewijzen verlopen precies zo. ⊣

Complement. Fixeer een verzameling X, waarvan alle in het volgende beschouwde verzamelingen deel zijn. Nu kan de volgende notatie worden gebruikt:

$$A^c := X - A$$

A^c is het *complement* van A *in* X. Kennelijk geldt, voor $A \subset X$ en $x \in X$:

$$x \in A^c \;\Leftrightarrow\; x \notin A.$$

N.B.: nogmaals, de notatie A^c veronderstelt een *vaste* X ten opzichte van welke de complementatie wordt uitgevoerd!

Er gelden de volgende wetten (vergelijk weer 1.5):

3.8 Stelling.

1. $(A^c)^c = A$; $X^c = \emptyset$; $\emptyset^c = X$,
2. $A \cup A^c = X$; $A \cap A^c = \emptyset$,
3. $A \subset B \;\Leftrightarrow\; B^c \subset A^c$,
4. $(A \cup B)^c = A^c \cap B^c$; $(A \cap B)^c = A^c \cup B^c$ *(wetten van DeMorgan)*.

Opgaven

20 ♣ Laat zien, dat: $A \not\subset B \;\Leftrightarrow\; A - B \neq \emptyset$.

21 ♣ Bewijs, dat $A \cap B = A - (A - B)$.

22 ♣ A, B en C zijn verzamelingen. Bewijs: $A - C \subset (A - B) \cup (B - C)$.

23 ♣ Bewijs Stelling 3.8.
Voorbeeld. Dezelfde methode als die van het bewijs van Stelling 3.7 levert, voor $x \in X$:

$$\begin{aligned} x \in (A \cup B)^c &\Leftrightarrow \neg(x \in A \cup B) \\ &\Leftrightarrow \neg(x \in A \vee x \in B) \\ &\Leftrightarrow \neg x \in A \wedge \neg x \in B \\ &\Leftrightarrow x \in A^c \wedge x \in B^c \\ &\Leftrightarrow x \in A^c \cap B^c. \end{aligned}$$

M.b.v. Extensionaliteit volgt hieruit de eerste DeMorgan wet.

3.9 Machtsverzamelingen. De *machtsverzameling* van een verzameling X is de verzameling $\wp(X) := \{\, A \mid A \subset X \,\}$ van alle deelverzamelingen van X.

In de ZF-axiomatiek zegt het **Machtsverzameling Axioma** dat iedere verzameling een machtsverzameling heeft.
Wegens Stelling 3.4.1/2 geldt *altijd*, dat $\emptyset \in \wp(X)$ en dat $X \in \wp(X)$. Dus bijvoorbeeld, $\wp(\{\emptyset, 1\}) = \{\emptyset, \{\emptyset\}, \{1\}, \{\emptyset, 1\}\}$. Denk hieraan bij de volgende opgave.

24 ♣ Bepaal: $\wp(\emptyset)$, $\wp(\wp(\emptyset))$ en $\wp(\wp(\wp(\emptyset)))$.
Hoeveel elementen heeft $\wp^5(\emptyset) := \wp(\wp(\wp(\wp(\wp(\emptyset)))))$?
♣Hoeveel paren accolades gebruikt de geëxpandeerde notatie voor deze verzameling?
Hoeveel elementen heeft $\wp(A)$, als A n elementen heeft?

***Boole algebra.** Strukturen van de vorm $(\wp(X), \cap, \cup, ^c, \emptyset, X)$ zijn voorbeelden van *boole-algebras*. Een boole-algebra is een struktuur met drie operaties (overeenkomend met $\cap$, $\cup$ en ^{c}) en twee elementen (overeenkomend met $\emptyset$ en X) die *onder meer* aan de gelijkheden van Stellingen 3.7 en 3.8 voldoet.

Een simpel voorbeeld vormt de 2-elementige boole-algebra over $\wp(X)$ waarbij $X = \{\, \emptyset \,\}$ een één-elementige verzameling is $(\wp(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\})$. Definiëren we de waarheidswaarden als $W := \{\emptyset\}$ en $O := \emptyset$ dan zie je dat $\cap$, $\cup$ en ^{c} juist overeenkomen met de waarheidstafels van $\wedge$, $\vee$ en $\neg$.

25 ♣♣ Geef verzamelings-algebraïsche definities van de waarheidstafels van $\rightarrow$ en $\leftrightarrow$ in deze context.

26 ♣♣ Geef een boole-algebra met 8 elementen.

27 ♣ Onderstel dat f een operatie is en dat E en F eigenschappen zijn.
Geldt nu dat $\{f(x) \mid E(x) \vee F(x)\} = \{f(x) \mid E(x)\} \cup \{f(x) \mid F(x)\}$?
En hoe zit het met $\{f(x) \mid E(x) \wedge F(x)\} = \{f(x) \mid E(x)\} \cap \{f(x) \mid F(x)\}$?
Aanwijzing. Bedenk, dat $\{f(x) \mid F(x)\} = \{f(y) \mid F(y)\}$.

28 ♣ Geldt voor alle verzamelingen A en B dat (i) $\wp(A \cap B) = \wp(A) \cap \wp(B)$? (ii) $\wp(A \cup B) = \wp(A) \cup \wp(B)$? Geef bewijs of tegenvoorbeeld.

3.10 Vereniging, Doorsnede. Onderstel dat voor ieder element $i \in I$ een verzameling A_i is gegeven.

1. $\bigcup_{i \in I} A_i$, de *vereniging* van de verzamelingen A_i, is de verzameling $\{x \mid \exists i \in I(x \in A_i)\}$.

2. Netzo is $\bigcap_{i \in I} A_i$ de notatie voor de *doorsnede* van de verzamelingen A_i, dat is: de verzameling $\{x \mid \forall i \in I(x \in A_i)\}$.

Als de elementen van I verzamelingen zijn, en $A_i = i$ $(i \in I)$, dan heet $\bigcup_{i \in I} A_i$ de *somverzameling* van I; deze wordt geschreven als $\bigcup I$. Eveneens in dat geval wordt $\bigcap_{i \in I} A_i$ geschreven als $\bigcap I$.
Voor het vaak voorkomende geval van een indexverzameling $I = \mathbb{N}$ kunnen $\bigcup_{i \in I} A_i$ en $\bigcap_{i \in I} A_i$ ook, wat aanschouwelijker, worden geschreven als $A_0 \cup A_1 \cup A_2 \cup \cdots$ en $A_0 \cap A_1 \cap A_2 \cap \cdots$.

N.B. Als $I = \emptyset$, dan geldt $\bigcup_{i \in I} A_i = \emptyset$, en $\bigcap_{i \in I} A_i$ is de collectie van *alle* verzamelingen. Het laatste is weer een geval van een triviaal-ware implicatie: als $I = \emptyset$, dan is iedere bewering $i \in I$ onwaar (ongeacht i), dus implicaties $i \in I \Rightarrow x \in A_i$ zijn waar (ongeacht i en x), en alles is element van $\{x \mid \forall i \in I(x \in A_i)\} = \{x \mid \forall i(i \in I \Rightarrow x \in A_i)\}$. De notatie $\bigcap_{i \in I} A_i$ vooronderstelt daarom meestal, dat $I \neq \emptyset$.

Het **Somverzameling Axioma** van de Zermelo-Fraenkel axiomatiek zegt, dat bij iedere verzameling I van verzamelingen de somverzameling $\bigcup I$ bestaat.

29 ♣ Bewijs:

1. $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I}(B \cap A_i)$; $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I}(B \cup A_i)$,
2. $(\bigcup_{i \in I} A_i)^c = \bigcap_{i \in I} A_i^c$; $(\bigcap_{i \in I} A_i)^c = \bigcup_{i \in I} A_i^c$. (Neem aan, dat $A_i \subset X$.)

30 ♣ Geldt de volgende bewering?: Als twee verzamelingen dezelfde deelverzamelingen hebben, dan zijn ze gelijk. Dwz.: als $\wp(A) = \wp(B)$, dan geldt $A = B$.

31 ♣ ♣ Waarom is er wèl een *Somverzameling* axioma in ZF maar geen *Doorsnede* axioma?

Samenvatting

Belangrijkste begrippen:

- Extensionaliteit,
- notaties voor verzamelingen: $\{a_1, \ldots, a_m\}$ (i.h.b., $\emptyset$, $\{a\}$), $\{a \mid E(a)\}$,
- inclusie: $A \subset B$,

- operaties: $\cap$, $\cup$, $-$, ^{c},
- $\wp(A)$.

Vraag:

- noem een aantal verzamelings-algebraïsche wetten.

Literatuur

Zie voor een beknoptere, praktische weergave van hetzelfde materiaal en dat van de volgende twee hoofdstukken Devlin [4]. Het eerste deel van het boek van van Dalen, Doets en de Swart [3] is een inleiding in de verzamelingentheorie in de Nederlandse taal. Een andere inleiding is Halmos [6].

Hoofdstuk 4

Relaties

In dit hoofdstuk maak je kennis met de verzamelingstheoretische kijk op wiskundige relaties. Een groot gedeelte van dit hoofdstuk, Sectie 4.3, gaat over een veelvuldig voorkomend type relatie: de *equivalentierelatie*. Hoofdstukken 9 en 10 gaan over een andere belangrijke ondersoort: de *ordeningsrelaties*.

4.1 Geordende Paren en Producten

Naast de ongeordende paren $\{a, b\}$ van Sectie 3.3, waarin de volgorde van A en b niet terzake doet ($\{a, b\} = \{b, a\}$), bestaan er ook *geordende paren* waarbij de volgorde wèl relevant is. Het *geordende paar* van de objecten a en b wordt genoteerd als:

$$(a, b)\ .$$

Hierin heet a het *eerste element* of de *eerste coördinaat* van (a, b) en b het *tweede element* of *coördinaat*.

Geordende paren voldoen aan de volgende regel:

$$(a, b) = (x, y) \implies a = x \wedge b = y. \tag{4.1}$$

Het geordende paar van a en b legt, behalve de objecten a en b, kennelijk ook hun *volgorde* vast: *eerst* a, *daarna* b. Een geordend paar (a, b) is dus iets anders dan een ongeordend paar $\{a, b\}$: altijd geldt $\{a, b\} = \{b, a\}$, maar $(a, b) = (b, a)$ geldt — volgens (4.1) — kennelijk alléén in het geval, dat $a = b$.
Waarschuwing. Als a en b reële getallen zijn, dan staat de notatie (a, b) ook voor het (open) interval $\{x \in \mathbb{R} \mid a < x < b\}$. Verwar deze notaties niet met elkaar.

***Definitie van geordend paar.** Er is een *definitie* van de notie *geordend paar* mogelijk in verzamelingstheoretische termen, nl.

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

Met deze definitie kun je (4.1) *bewijzen*, maar dat kost nog wat werk. Zie Opgave 34.

Geordende drie-, vier-, ... tallen zijn nu definieerbaar in termen van geordende paren; bijvoorbeeld: $(a, b, c) := (a, (b, c))$, enz.

4.1 Producten. Het (*Cartesisch*) *product* van de verzamelingen A en B is de verzameling van alle geordende paren (a, b) waarvoor $a \in A$ en $b \in B$:

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

In plaats van $A \times A$ kun je ook A^2 schrijven.

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

Als A en B intervallen van reële getallen zijn op de X- resp. Y-as in het platte vlak, dan kan $A \times B$ worden opgevat als een rechthoek in het platte vlak. De van het VWO bekende, fundamentele relatie tussen $\mathbb{R} \times \mathbb{R}$ en het platte vlak is verbonden met de naam Cartesius (René Descartes).

Opgaven

32 ♣ Toon aan dat voor verzamelingen A, B, C, D het volgende geldt:

1. $(A \times B) \cap (C \times D) = (A \times D) \cap (C \times B)$,
2. $(A \cup B) \times C = (A \times C) \cup (B \times C)$; $(A \cap B) \times C = (A \times C) \cap (B \times C)$,
3. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$,
4. $(A \cup B) \times (C \cup D) = (A \times C) \cup (A \times D) \cup (B \times C) \cup (B \times D)$,
5. $[(A - C) \times B] \cup [A \times (B - D)] \subset (A \times B) - (C \times D)$.

Voorbeeld. Het eerste gedeelte van onderdeel 2, $(A \cup B) \times C = (A \times C) \cup (B \times C)$:
($\subset$) Onderstel, dat $p \in (A \cup B) \times C$. Bijvoorbeeld, $p = (a, c)$, met $a \in A \cup B$ en $c \in C$. Dan geldt $a \in A$ of $a \in B$. In het eerste geval geldt er dat $p \in A \times C$ en dus $p \in (A \times C) \cup (B \times C)$; en in het tweede geval geldt er dat $p \in B \times C$ en dus eveneens $p \in (A \times C) \cup (B \times C)$.
($\supset$) Omgekeerd, onderstel, dat $p \in (A \times C) \cup (B \times C)$. Dan geldt $p \in A \times C$ of $p \in B \times C$. In het eerste geval bestaan $a \in A$ en $c \in C$ zódat $p = (a, c)$; dan geldt $a \in A \cup B$ en dus $p \in (A \cup B) \times C$. In het tweede geval bestaan $b \in B$ en $c \in C$ zódat $p = (b, c)$; dan geldt $b \in A \cup B$ en dus eveneens $p \in (A \cup B) \times C$.
Het gevraagde volgt hieruit m.b.v. het Extensionaliteitsaxioma.

33 ♣ Gegeven zijn niet-lege verzamelingen A en B zódat $A \times B = B \times A$. Bewijs, dat $A = B$.

34 ♣♣

1. Bewijs, dat
   (i) $\{a, b\} = \{a, c\} \Longrightarrow b = c$,
   (ii) $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\} \Longrightarrow a = x \wedge b = y$.
2. Neem eigenschap 4.1 van geordende paren aan. Definieer geordende drietallen door: $(a, b, c) := (a, (b, c))$. Bewijs, dat $(a, b, c) = (x, y, z) \Rightarrow (a = x \wedge b = y \wedge c = z)$.

4.2 Relaties

Deze sectie behandelt de verzamelingstheoretische definitie van het begrip relatie.

Hoewel je waarschijnlijk niet in staat bent om uit te leggen wat je *in het algemeen* onder een relatie verstaat (maar Definitie 4.2 zal daar een eind aan maken), ben je desondanks vertrouwd met een aantal concrete relaties. Bijvoorbeeld, met de gewone ordeningsrelatie $<$ tussen natuurlijke getallen.

Voor iedere twee getallen $n, m \in \mathbb{N}$ ligt vast, of de bewering $n < m$ *waar* is of *onwaar*. (Bijvoorbeeld, dat $3 < 5$ is *waar*, maar $5 < 2$ is *onwaar*.) Algemeen: een relatie is iets dat je twee objecten kunt toeschuiven, en dan vertelt of die objecten met elkaar in die gegeven relatie staan of niet. Een niet-wiskundig voorbeeld is de *grootvader* relatie: twee mensen staan in die relatie tot elkaar als de eerste de grootvader van de tweede is.

In de verzamelingentheorie is er een handige manier om het relatie-begrip te *reduceren* tot dat van verzameling. Neem bijvoorbeeld weer de relatie $<$ op $\mathbb{N}$. Associeer met $<$ de verzameling R van geordende paren (n, m) van natuurlijke getallen waarvoor de bijbehorende bewering $n < m$ *waar* is:

$$R := \{\, (n, m) \mid n, m \in \mathbb{N} \wedge n < m \,\}.$$

Merk op, dat de bewering $n < m$ nu equivalent is met: $(n, m) \in R$. (Dus: $(3, 5) \in R$, $(5, 2) \notin R$.)

In de verzamelingentheorie wordt dit verband gebruikt om het algemene begrip van een relatie te *definiëren*. Dus bijvoorbeeld, de ordeningsrelatie $<$ van de natuurlijke getallen wordt *geïdentificeerd* met de verzameling R.

4.2 Relaties. Een *relatie* is per definitie een verzameling van geordende paren. In plaats van $(x, y) \in R$ — R een relatie — schrijf je in de regel: xRy, of $R(x, y)$. Spreek uit: *x staat in de relatie R tot y*, of: *de relatie R bestaat tussen x en y*. De verzameling $Dom(R) := \{x \mid \exists y\ (\ xRy\ )\}$ heet het *domein* van R, en $Ran(R) := \{y \mid \exists x\ (\ xRy\ )\}$ ('*Ran*' voor het Engelse 'range') het *bereik*.

Een productverzameling $A \times B$ is kennelijk een voorbeeld van een relatie. Een ander voorbeeld van een relatie is de lege verzameling $\emptyset$ (het is "triviaal waar" dat ieder element van $\emptyset$ een geordend paar is).

$Dom(R)$ is de verzameling van eerste coördinaten van geordende paren in R en $Ran(R)$ de verzameling van tweede coördinaten van dergelijke paren.

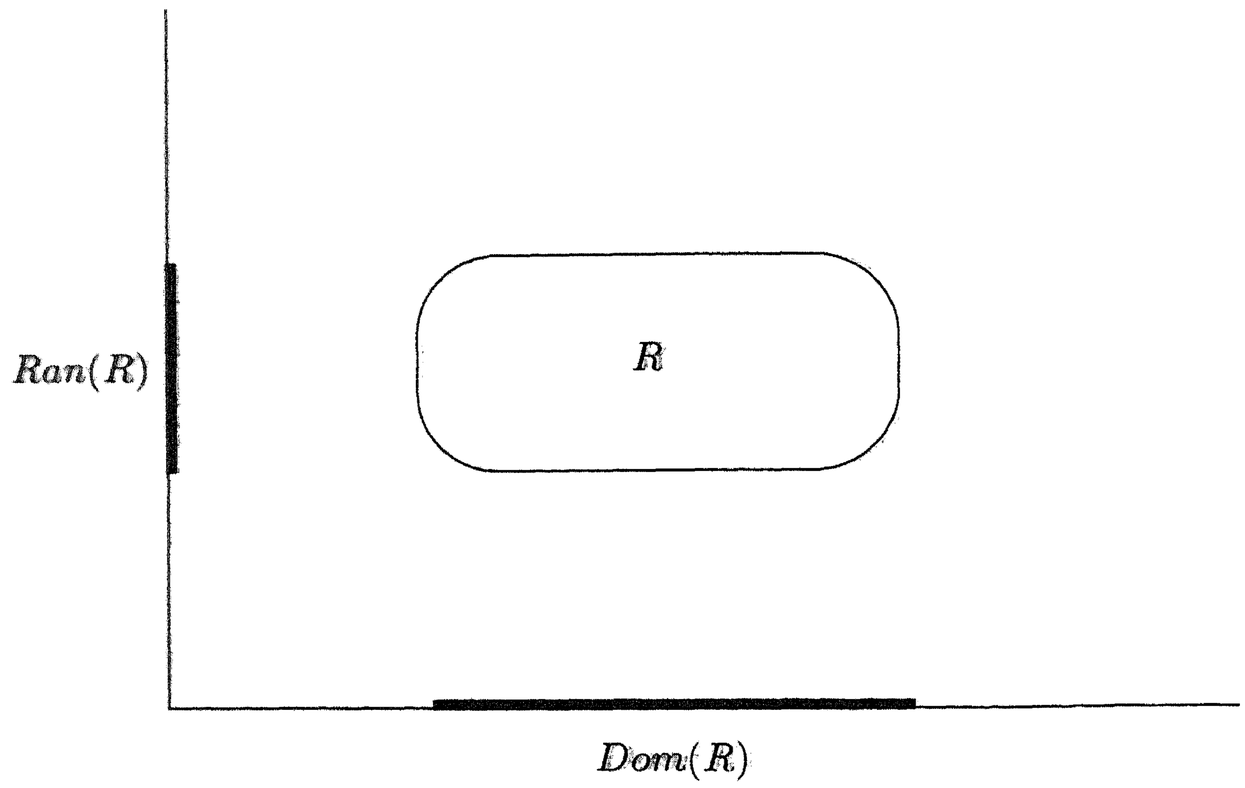
$Dom(\emptyset) = Ran(\emptyset) = \emptyset$, $Dom(A \times B) = A$ (mits B niet-leeg is: $A \times \emptyset = \emptyset$, dus $Dom(A \times \emptyset) = \emptyset$!), en $Ran(A \times B) = B$ (analoog: mits A niet-leeg is).

4.3 Van ... naar, Tussen, Over, Op. De relatie R heet een relatie *van A naar B* of *tussen A* en B als $Dom(R) \subset A$ en $Ran(R) \subset B$.
Een relatie van A naar A heet *op* of *over A*.

Bijvoorbeeld, $R := \{(1, 4), (1, 5), (2, 5)\}$ is een relatie van (onder meer) $\{1, 2, 3$ naar (bijvoorbeeld) $\{4, 5, 6\}$. $Dom(R) = \{1, 2\}$, $Ran(R) = \{4, 5\}$.

Als R een relatie is op de verzameling A, dan kan het complex (A, R) heel goed worden opgevat als een struktuur in de zin van Definitie 1.2 (blz. 4). De verzameling A —het universum van de struktuur— heet dan wel de (bij R) *onderliggende* verzameling.

Als A de X-as in het platte vlak is en B de Y-as, dan is een relatie van A naar B niets anders dan een verzameling in het platte vlak.



De relaties van Definitie 4.2 heten wel *binaire* of *twee-argumentige* relaties om ze te onderscheiden van *ternaire* (drie-argumentige), *quaternaire* (vier-argumentige) ... relaties: verzamelingen van geordende drie-, vier- ... tallen. En er zijn ook *unaire* (één-argumentige) relaties: een één-argumentige relatie over een verzameling A is gewoon een deelverzameling van A, ofwel een eigenschap van elementen van A.

4.4 Identiteit, Inverse.

1. $\Delta_A := \{ (a, a) \mid a \in A \} = \{ (a, b) \in A^2 \mid a = b \}$ is een relatie op A, de *identiteit* op A.

2. Als R een relatie is tussen A en B, dan is $R^* := \{ (a, b) \mid bRa \}$, de *inverse* van R, een relatie tussen B en A.

Voorbeelden.

1. $A \times B$ is de grootste relatie van A naar B.

2. $\emptyset$ is de kleinste relatie van A naar B.

3. Laat $<$ de gewone ordening van, zeg, $\mathbb{R}$ zijn. Dan geldt kennelijk, dat $<^* = >$.

4. $(R^*)^* = R$; $\Delta_A^* = \Delta_A$; $\emptyset^* = \emptyset$ en $(A \times B)^* = B \times A$.

Hoe definieer je een relatie? In de praktijk worden relaties gewoonlijk d.m.v. een *conditie* op paren objecten gedefinieerd (netzo als verzamelingen worden gedefinieerd door een conditie op één object). Bijvoorbeeld, als R de verzameling van alle paren (n, m) van gehele getallen $n, m \in \mathbb{Z}$ is, zódat (*conditie*) n^2 een deler is van m, dan kan een definitie van R, gebruikmakend van het definieerbaar-equivalent-teken $:\equiv$ (Definitie 1.1 blz. 2), er als volgt uitzien:

definieer, voor $n, m \in \mathbb{Z}$: $nRm :\equiv$ n^2 is een deler van m.

'Tussen a en b bestaat een relatie.' In het dagelijks leven mag een bewering van de vorm 'tussen a en b bestaat een relatie' (of 'a en b hebben een relatie') niet ongewoon klinken, in de hier gegeven context is dat wél zo. Niet omdat zo'n bewering fout zou zijn, maar omdat hij kennelijk *altijd* waar is, en dientengevolge bizonder weinig informatief. Zie de volgende opgave. (Natuurlijk zijn beweringen van de vorm 'a staat in relatie R tot b' of 'de relatie R bestaat tussen a en b' gewoonlijk wél informatief!)

35 ♣ Opgave. Bewijs: $\forall x\, \forall y\, \exists R\, (xRy)$. ("Tussen iedere twee dingen bestaat (wel) een relatie.")

4.3 Equivalenties

Een belangrijk type relatie is de *equivalentierelatie.*

4.5 Equivalentierelaties. Een relatie R op de verzameling A heet een *equivalentierelatie*, of kortweg: *equivalentie*, als R de volgende drie eigenschappen heeft:

1. R is *reflexief op* A, d.w.z.: $\forall x \in A : xRx$,
2. R is *symmetrisch*: $\forall x \forall y\, (xRy \;\Rightarrow\; yRx)$,
3. R is *transitief*: $\forall x \forall y \forall z\, (xRy \wedge yRz \;\Rightarrow\; xRz)$.

Zie de tabel op blz. 118 voor de vraag of een aantal veel voorkomende relaties reflexief, symmetrisch of transitief zijn.

Merk op: R is reflexief op A d.e.s.d.a. $\Delta_A \subset R$; R is symmetrisch d.e.s.d.a. $R^* = R$.

Voorbeelden.

0. De relatie $\emptyset$ is (trivialiter) symmetrisch en transitief.

   De relatie $\emptyset$ is reflexief op de verzameling $\emptyset$, maar hij is niet reflexief op een niet-lege verzameling.

   Dus: de relatie $\emptyset$ is een equivalentie op de verzameling $\emptyset$, maar op geen enkele andere verzameling.

1. Laat A een verzameling zijn.

   Δ_A is de kleinste equivalentie op A. A^2 is de grootste equivalentie op A.

2. De relatie $mod(4) := \{(n,m) \mid n-m \text{ is een 4-voud}\}$ is een equivalentie op $\mathbb{Z}$.

3. De relatie $\sim$ tussen vectoren in de 3-dimensionale Euclidische ruimte $\mathbb{R}^3$ gedefinieerd door $\vec{a} \sim \vec{b} :\equiv \exists r \in \mathbb{R}^+ \, (\vec{a} = r\vec{b})$ is een equivalentie.

4. De relatie die tussen twee eindige verzamelingen bestaat als ze evenveel elementen hebben is een equivalentierelatie op de klasse van alle eindige verzamelingen.

36 ♣ Opgave. Zeg van de volgende relaties op $\mathbb{N}$ of ze a. reflexief (op $\mathbb{N}$), b. symmetrisch, c. transitief zijn. (Geef je antwoord in de vorm van een 3×5-tabelletje.)
1. $\emptyset$; 2. $\Delta_{\mathbb{N}}$; 3. $\leqslant$; 4. $\{(2,3),(3,5),(5,2)\}$; 5. $\{(n,m) \mid |n-m| \geqslant 3\}$.

Abstracte equivalentierelaties worden vaak aangegeven met $\sim$ of met $\approx$.

4.6 Equivalentieklassen. Laat R een equivalentie zijn op A, en $a \in A$.
De verzameling $|\, a \,| = |\, a \,|_R := \{\, b \in A \mid bRa \,\}$ heet de *R-equivalentieklasse* van a, of de *equivalentieklasse* van a *modulo* R.
De elementen van een equivalentieklasse heten *representanten* van die klasse. I.h.b., a is een representant van $|\, a \,|$ (want een euivalentierelatie is reflexief), en als bRa geldt dan is b ook een representant van $|\, a \,|$.
Een equivalentieklasse $|\, a \,|_R$ bestaat dus uit alle *eerste* elementen $b \in A$ van geordende paren in R waarvan a het *tweede* element is. Maar omdat R symmetrisch is, is dat hetzelfde als: alle elementen b in geordende paren in R waarin a eveneens voorkomt.

Voorbeelden, voortgezet.

1. De equivalentieklasse van $a \in A$ modulo Δ_A is $\{a\}$.

   De enige equivalentieklasse modulo A^2 is A zelf.

2. De equivalentieklasse van $2 \in \mathbb{Z}$ modulo $mod(4)$ is de verzameling $\{\ldots,-6,-2,2,6,10,14,\ldots\} = \{2+4n \mid n \in \mathbb{Z}\}$.

3. De equivalentieklasse van $(1,1,1) \in \mathbb{R}^3$ modulo $\sim$ is de verzameling $\{(r,r,r) \mid r > 0\}$: een halflijn vanuit de oorsprong, m.u.v. die oorsprong. Je zou kunnen zeggen dat een equivalentieklasse hier een *richting* is.

4. De equivalentieklasse van $\{0,1,2\}$ modulo de hierboven gegeven equivalentierelatie evenveel elementen te hebben is de collectie van alle drieelementige verzamelingen.

   (Volgens Russell's definitie van natuurlijk getal *is* dit het getal drie. Zie Definitie 8.17 blz. 110.)

4.7 Lemma. *Laat R een equivalentie zijn op A. Voor $a,b \in A$ geldt:*

$$|\, a \,|_R = |\, b \,|_R \;\Leftrightarrow\; aRb.$$

Bewijs. $\Rightarrow$: Merk op, dat $a \in |\,a\,|_R$ (want R is reflexief). Als dus $|\,a\,|_R = |\,b\,|_R$, dan geldt ook $a \in |\,b\,|_R$, d.w.z.: aRb.
$\Leftarrow$: Neem aan, dat aRb. Dan geldt ook dat bRa (R is symmetrisch.)
$|\,a\,|_R \subset |\,b\,|_R$: $x \in |\,a\,|_R$ betekent xRa, en dus volgt xRb (R transitief) en $x \in |\,b\,|_R$.
$|\,b\,|_R \subset |\,a\,|_R$: net zo.
Gelijkheid van de equivalentieklassen volgt uit het Extensionaliteitsaxioma. $\dashv$

4.8 Lemma. *Laat R een equivalentie zijn op A.*

1. *Iedere equivalentieklasse is niet-leeg,*
2. *ieder element van A is element van een equivalentieklasse,*
3. *twee verschillende equivalentieklassen zijn disjunct.*

Bewijs. 1/2. Omdat R reflexief is op A geldt voor ieder element $a \in A$: $a \in |a|$.
3. Onderstel, dat $|\,a\,|$ en $|\,b\,|$ niet disjunct zijn. Bijvoorbeeld, $c \in |\,a\,| \cap |\,b\,|$. Dan geldt zowel cRa als cRb. Omdat R symmetrisch is, volgt ook aRc. Dus, aRb (R transitief). Nu volgt dat $|\,a\,| = |\,b\,|$ met Lemma 4.7. $\dashv$

4.9 Verdelingen. Een collectie V van deelverzamelingen van A heet een *verdeling* van A als aan de volgende drie voorwaarden is voldaan:

1. $\emptyset \notin V$
2. $\forall a \in A\, \exists K \in V\, (a \in K)$, d.w.z.: ieder element van A is element van een verzameling in V
3. voor alle $K, L \in V$ geldt: $K \neq L \;\Rightarrow\; K \cap L = \emptyset$.

De elementen van een verdeling heten zijn *componenten.*

4.10 Quotienten. Laat R een equivalentie zijn op de verzameling A. De collectie van equivalentieklassen van R, $A/R := \{|\,a\,| \mid a \in A\}$, heet het *quotient* van A *modulo* R.

4.11 Stelling. *Ieder quotient (van een verzameling, modulo een equivalentie) is een verdeling (van die verzameling).*

Bewijs. Dit is kennelijk niets anders dan een herformulering van Lemma 4.8. $\dashv$

Voorbeelden, voortgezet.

1. $A/\Delta_A = \{\,\{a\} \mid a \in A\,\}$.
2. $A/A^2 = \{A\}$.

De verdeling $\mathbb{Z}/mod(4)$ van $\mathbb{Z}$ geïnduceerd door de equivalentie $mod(4)$ heeft vier componenten: de equivalentieklasse $\{4n \mid n \in \mathbb{Z}\}$ van 0 (die ook de equivalentieklasse van 4, 8, 12,...,-4... is), de equivalentieklasse $\{4n+1 \mid n \in \mathbb{Z}\}$ van 1, de equivalentieklasse $\{4n+2 \mid n \in \mathbb{Z}\}$ van 2, en $\{4n+3 \mid n \in \mathbb{Z}\}$, de equivalentieklasse van 3.

3. De verdeling $\mathbb{R}^3/\sim$ van $\mathbb{R}^3$ heeft als componenten $\{0\}$ en alle halflijnen vanuit de oorsprong.

4. *Het quotient van de collectie van eindige verzamelingen modulo de relatie "evenveel elementen" is —volgens Russell— de verzameling van natuurlijke getallen.

Dus: iedere equivalentie geeft aanleiding tot een verdeling van de onderliggende verzameling in equivalentieklassen.

Het omgekeerde is ook waar: dat is de inhoud van de volgende stelling. Bijvoorbeeld, bij de verdeling van $\mathbb{N}$ in *even* en *oneven* getallen hoort de equivalentie R die kan worden gedefinieerd door $nRm :\equiv n + m$ is even.

4.12 Stelling. *Iedere verdeling (van een verzameling) is een quotient (van die verzameling, modulo een zekere equivalentie).*

Meer specifiek: Laat V een verdeling van de verzameling A zijn. Dan is de relatie R op A, gedefinieerd door

$$xRy :\equiv \exists K \in V\ (x, y \in K)$$

(x en y element van eenzelfde component K van V) een equivalentie op A, en V is de collectie van equivalentieklassen van R.

Bewijs. Opgave 50. ⊣

Volgens Stellingen 4.11 en 4.12 zijn equivalenties en verdelingen twee verschijningsvormen van hetzelfde.

Opgaven

37♣ Zijn de volgende relaties equivalentierelaties op $\{0, 1, 2, 3, 4\}$? Zoja, geef de bijbehorende verdeling(en).

1. $\{(0,0),(0,1),(1,0),(1,1),(2,2),(2,4),(3,3),(4,2),(4,4)\}$,
2. $\{(0,0),(0,3),(0,4),(1,1),(1,2),(2,1),(2,2),(3,0),(3,3),(3,4),(4,0),(4,3),(4,4)\}$.

Antwoord bij 1. Dit is inderdaad een equivalentierelatie. De bijbehorende verdeling is $\{\{0,1\},\{2,4\},\{3\}\}$.

38♣ Geef de equivalentierelaties die horen bij

1. de verdeling $\{\{0\},\{1,2,3\},\{4\}\}$ van $\{0,1,2,3,4\}$,
2. de verdeling $\{\{0,3\},\{1,2,4\}\}$ van $\{0,1,2,3,4\}$,
3. de verdeling van $\mathbb{Z}$ in $\{n \in \mathbb{Z} \mid n < 0\}$ en $\{n \in \mathbb{Z} \mid 0 \leqslant n\}$.

Antwoord bij 1: $\{(0,0),(1,1),(1,2),(1,3),(2,2),(2,3),(3,1),(3,2),(3,3),(4,4)\}$.

39♣ $A = \{1,2,3,4,5\}$,
$R = \{(1,1),(1,2),(1,4),(2,1),(2,2),(2,4),(3,3),(3,5),(4,1),(4,2),(4,4),(5,3),(5,5)\}$.

1. Is R een equivalentie op A? Zoja, beantwoord ook 2 en 3:

2. bepaal $|2|_R$,
3. bepaal A/R.

40 ♣ Definieer de relatie $\sim$ op $\wp(\mathbb{N})$ door: $A \sim B :\equiv (A - B) \cup (B - A)$ is eindig. (Dus bijvoorbeeld, $\mathbb{N} \not\sim \emptyset$, want $(\mathbb{N} - \emptyset) \cup (\emptyset - \mathbb{N}) = \mathbb{N} \cup \emptyset = \mathbb{N}$ is oneindig.) Bewijs dat $\sim$ een equivalentie is.
Voorbeeld. $\sim$ is reflexief. Voor een willekeurige verzameling $A \subset \mathbb{N}$ geldt immers, dat $(A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$, en $\emptyset$ is eindig.

41 ♣ Definieer de relatie R op de wereldpopulatie door: $aRb :\equiv a$ en b hebben een gemeenschappelijke voorouder. Is R transitief?
Zelfde vraag voor de relatie S gedefinieerd door: $aSb :\equiv a$ en b hebben een gemeenschappelijke voorvader langs de mannelijke lijn (i.e.: ze hebben — uitzonderingen daargelaten — dezelfde achternaam).

42 ♣ Voor eindige verzamelingen A (0, 1, 2, 3, 4 en 5 elementen en, i.h.a., n elementen) tellen we in de volgende tabel: het aantal elementen van A^2, het aantal elementen van $\wp(A^2)$, dat is: het aantal relaties op A, het aantal relaties op A die (i) reflexief, (ii) symmetrisch en (iii) transitief zijn, en het aantal equivalenties op A.

A	A^2	$\wp(A^2)$	reflexief	symmetrisch	transitief	equivalentie
0	0	1	1	1	1	1
1	1	2	1	2	2	1
2	?	?	?	?	13	?
3	?	?	?	?	—	?
4	?	?	?	?	—	?
5	?	?	?	?	—	?
n	?	?	?	?	—	—

Geef alle reflexieve, symmetrische, transitieve en equivalentierelaties voor de gevallen, dat $A = \emptyset$ (0 elementen) en $A = \{0\}$ (1 element). Bewijs dat er precies 13 transitieve relaties zijn op $\{0, 1\}$, en geef de 3 niet-transitieve. Vul getallen in voor de vraagtekens. (Antwoorden voor — worden niet gevraagd.)
Aanwijzing. Het is makkelijker om verdelingen te tellen, dan equivalenties.

43 ♣ Bewijs: condities 2 en 3 van Definitie 4.9 zijn met elkaar equivalent met: voor iedere $a \in A$ bestaat er precies één $K \in V$ zódat $a \in K$.

44 ♣ A is een verzameling.
Is de *doorsnede* $R \cap S$ van twee equivalenties R en S op A altijd weer een equivalentie?
En de *vereniging* $R \cup S$?
Bewijs, of geef een (eenvoudig) tegenvoorbeeld.

45 ♣ ♣ Onderstel, dat R en S equivalenties op A zijn zódat $R \subset S$. Bewijs, dat iedere S-equivalentieklasse *vereniging* is (zie Definitie 3.10, blz. 38) van (één of meer) R-equivalentieklassen.

46 ♣ Gegegeven is de relatie $R := \{(2, 0), (1, 5), (0, 3)\}$ op de verzameling $A{:=}\{0, 1, 2, 3, 4, 5\}$. Wat is de *kleinste* (in de zin van: aantal elementen) equivalentie $S \supset R$ op A? Wat is A/S? Hoeveel equivalenties zijn er op A die R omvatten? Geef de bijbehorende verdelingen van A.
Aanwijzing. Vraag je af, welke geordende paren aan R moeten worden toegevoegd om er een equivalentie van te maken. (Voor de laatste vraag kun je Opgave 45 gebruiken.)

47 ♣♣ Gegeven is een relatie R op de verzameling A. Definieer $aSb :\equiv a = b$, óf er is een eindige rij $a_0, \ldots, a_n \in A$ met: $a_0 = a$, $a_n = b$, en voor alle $i < n$: $a_i R a_{i+1}$ of $a_{i+1} R a_i$. Toon aan: (i) $R \subset S$; (ii) S is een equivalentie; en (iii) S is deel van iedere R-omvattende equivalentie.

48 ♣ Definieer de relaties $\sim$ en $\approx$ op $\mathbb{R}$ door $p \sim q :\equiv p \times q \in \mathbb{Z}$, $p \approx q :\equiv p - q \in \mathbb{Z}$. Zijn dit equivalenties? Zoja, beschrijf de bijbehorende verdeling(en).

49 ♣ $Q := \{(0,0), (0,1), (0,5), (5,0), (2,4)\}$.
Van de equivalentierelatie R op $\{0,1,2,3,4,5\}$ wordt gegeven, dat $Q \subset R$ en $(0,2) \notin R$.

1. Beargumenteer, dat $(1,5) \in R$ en $(4,5) \notin R$.
2. Geef de verdeling die hoort bij de kleinste (in de zin van: aantal elementen) equivalentierelatie $\supset Q$.
3. Voor hoeveel equivalentierelaties S op $\{0,1,2,3,4,5\}$ geldt dat $Q \subset S$ en $(0,2) \notin S$? Geef de bijbehorende verdelingen.

50 ♣ Bewijs Stelling 4.12.

Samenvatting

Belangrijkste begrippen:

- geordend paar (a,b), product $A \times B$,
- relatie (Dom, Ran), relatie op, equivalentierelatie,
- equivalentieklasse, quotient,
- verdeling.

Vragen:

- geef voorbeelden van relaties en equivalentierelaties op (zeg) $\mathbb{N}$,
- hoe geeft een equivalentie aanleiding tot een verdeling van de onderliggende verzameling?
- wat is de bij een gegeven verdeling horende equivalentie?

Hoofdstuk 5

Functies

5.1 Basisbegrippen

Het functie-begrip is vermoedelijk *het* wiskundige begrip bij uitstek — misschien belangrijker nog dan dat van een verzameling.

Een functie kun je een *argument* toeschuiven, en levert dan een *functiewaarde* retour. (Op deze manier kun je een koffie-automaat dus opvatten als een functie: argumenten zijn kwartjes of guldens, functiewaarden zijn bekertjes koffie.) De verzamelingentheorie heeft de volgende simpele definitie voor de notie van een functie, namelijk, als een speciaal soort relatie.

5.1 Functies. Een relatie f heet een *functie* of *afbeelding* als geldt

$$(x, y) \in f \ \wedge \ (x, z) \in f \implies y = z$$

— d.w.z.: bij iedere $x \in Dom(f)$ bestaat precies één $y \in Ran(f)$ zódat $(x, y) \in f$.
Het *definitiegebied* of *domein* $Dom(f)$ van de functie f is $\{x \mid \exists y\,((x, y) \in f)\}$ — weer dezelfde verzameling (zie Definitie 4.2 blz. 43) als die bij relaties; en netzo is $Ran(f) := \{y \mid \exists x\,((x, y) \in f)\}$ weer het *bereik* van f.
Elementen van $Dom(f)$ heten *argumenten* van f, elementen van $Ran(f)$ *functiewaarden.*
Onderstel, dat $x \in Dom(f)$. Het unieke ding $y \in Ran(f)$ waarvoor geldt dat $(x, y) \in f$ wordt genoteerd als $y = f(x)$. De functiewaarde y heet het *beeld van* x of de (functie) *waarde* van f *in* x en x heet een *origineel* van y of *origineel onder* f van y.
Je kunt $y := f(x)$ ook opvatten als het resultaat van de toepassing (*applicatie*) van f op het element x.
Dat $f(x) = y$ geldt wordt soms aangegeven met de notatie: $f : x \longmapsto y$.

Vergelijk de volgende terminologie met die van 4.3 (blz. 43) voor relaties.

5.2 Van ...naar, Op, Codomein. Vaak worden functies niet geïsoleerd beschouwd, maar in de context van twee verzamelingen: f heet een functie *van*

de verzameling X *naar* de verzameling Y, notatie:

$$f : X \longrightarrow Y,$$

als $Dom(f) = X$ en $Ran(f) \subset Y$. (Let op: hier verschilt de terminologie met die van 4.3!) In dit geval heet Y het *codomein* van f.
Een functie f heet (gedefinieerd) *op* de verzameling X als $X = Dom(f)$.

Voorbeelden. $f := \{(1,4),(2,4),(3,6)\}$ is een functie. $Dom(f) = \{1,2,3\}$, $Ran(f) = \{4,6\}$. Er geldt (bijvoorbeeld), dat $f : \{1,2,3\} \to \{4,5,6\}$.
Verzamelingstheoretisch wordt de functie $f : \mathbb{N} \to \mathbb{N}$ die gedefinieerd is door: $f(n) := n^2 + 1$, *geïdentificeerd* met de *relatie* $\{(n, n^2+1) \mid n \in \mathbb{N}\}$. $Ran(f) = \{1,2,5,10,\ldots\}$.
Δ_X, de identiteitsrelatie op X, (Definitie 4.4, blz. 44) is ook een functie van X naar X. Als functie opgevat wordt Δ_X meestal genoteerd als 1_X.
Als $X \subset Y$, dan geldt natuurlijk ook dat $1_X : X \longrightarrow Y$.
In het bizonder: voor iedere verzameling Y is $\emptyset = 1_\emptyset$ een functie van $\emptyset$ naar Y.
Als f een functie is, dan geldt kennelijk dat $f = \{(a, f(b)) \mid a \in Dom(f)\}$, en $Ran(f) = \{f(a) \mid a \in Dom(f)\}$.

***Méér argumenten.** Functies als boven geïntroduceerd hebben maar één argument. In de praktijk komen ook meer-argumentige (binaire, ternaire, ...) functies voor, zoals de optelling en de vermenigvuldiging op $\mathbb{N}$. Een *binaire* functievan A naar B kan worden gedefinieerd als een één-argumentige functie van A^2 naar B, d.w.z., als een functie waarvan de argumenten geordende paren zijn. Als $f : A^2 \to B$ zo'n functie is, en $a_1, a_2 \in A$, dan is $f((a_1, a_2))$ de functiewaarde in het paar (a_1, a_2); maar die schrijf je natuurlijk met maar één stel haakjes: $f(a_1, a_2)$.

5.3 Hoe bewijs je dat twee functies gelijk zijn? Als f en g functies zijn die hetzelfde domein hebben ($Dom(f) = Dom(g)$) en daarop dezelfde "actie" vertonen (d.w.z., dat $\forall x \in Dom(f)(f(x) = g(x))$), dan geldt — volgens het Extensionaliteitsaxioma 3.2, blz. 30 — dat $f = g$ (ga na).
Het codomein van een functie speelt een rol bij de begrippen compositie en surjectiviteit, verderop. Merk op: als $f : X \longrightarrow Y$ en $Y \subset Y'$, dan geldt natuurlijk ook, dat $f : X \longrightarrow Y'$. Soms wordt de functie f in de tweede situatie (naar Y') *onderscheiden* van de functie f in de eerste situatie (naar Y) — ook al zijn ze dus volgens onze (verzamelingstheoretische) definities één en hetzelfde ding. Dus, functies met verschillend codomein kunnen in deze context als verschillend worden gerekend, ook al hebben ze hetzelfde domein en vertonen ze daarop dezelfde "actie".

Hoe definieer je functies? Onderstel dat de uitdrukking $t(x)$ een element van Y beschrijft, iedere keer dat $x \in X$. Gebruikmakend van $:=$ voor *per definitie gelijk aan* (Definitie 1.1 blz. 2) wordt dan een functie $f : X \longrightarrow Y$ gedefinieerd door de stipulering dat voor alle $x \in X$: $f(x) := t(x)$.
Voorbeelden:

1. $t(x)$ is hier de uitdrukking $2x^2 + 3$:
   Definieer de functie $g : \mathbb{R} \longrightarrow \mathbb{R}$ door $g(x) := 2x^2 + 3$.
2. $t(x)$ is hier de uitdrukking $\int_0^x y \sin y dy$:
   Definieer $h : \mathbb{R} \longrightarrow \mathbb{R}$ door: $h(x) := \int_0^x y \sin y dy$.

*De zgn. *lambda*-notatie met het λ-symbool voor een zo gedefinieerde functie is: $\lambda x.t(x)$ (of, met vermelding van het domein: $\lambda x \in X.t(x)$). Dus, $\lambda x.2x^2 + 3$ is (een notatie voor) de functie g onder 1, en $\lambda x. \int_0^x y \sin y dy$ is de functie h onder 2.
In de uitdrukking $\lambda x.t(x)$ wordt de variabele x gebonden door λ.

Een voorbeeld van zo'n functie-definitie is de de volgende.

5.4 Restricties. Onderstel, dat $f : X \longrightarrow Y$ en $A \subset X$. De *restrictie* of *beperking van f tot A* is de functie $h : A \to Y$ gedefinieerd door $h(a) := f(a)$. De notatie voor deze functie is $f|A$.

5.5 Beeld, Origineel. Onderstel, dat $f : X \longrightarrow Y$, $A \subset X$ en $B \subset Y$.

1. $f[A] := \{f(x) \mid x \in A\}$ heet het *beeld* of de *beeldverzameling* van A onder f;
2. $f^{-1}[B] := \{x \in X \mid f(x) \in B\}$ heet het (volledig) *origineel* van B onder f.

Dus:

1. $y \in f[A] \Leftrightarrow \exists x \in A(y = f(x))$,
2. $x \in f^{-1}[B] \Leftrightarrow f(x) \in B$.

Uit 1 volgt, dat $x \in A \Rightarrow f(x) \in f[A]$. Maar: *er hoeft niet te gelden, dat* $f(x) \in f[A] \Rightarrow x \in A$. (Voorbeeld: $f = \{(0,2),(1,2)\}$, $x = 0$, $A = \{1\}$.)

Ronde vs. rechte haken. Onderscheid de notaties $f(a)$ (ronde haken) en $f[A]$ (vierkante haken): bij de notatie $f(a)$ wordt altijd vooronderstelt, dat $a \in Dom(f)$, en $f(a)$ is de functiewaarde van a onder f. Bij $f[A]$ is de vooronderstelling, dat $A \subset Dom(f)$, en $f[A]$ is de *verzameling* van functiewaarden $f(x)$ voor $x \in A$.
In de gemiddelde wiskundige tekst wordt dit onderscheid overigens niet altijd gerespecteerd. Er worden dan domweg altijd ronde haken gebruikt en wat bedoeld wordt moet uit de context blijken. Meestal is wel duidelijk of je te maken hebt met een *element* of een *deelverzameling* van $Dom(f)$, (maar als de elementen van $Dom(f)$ zelf verzamelingen zijn dan kun je een probleem hebben).

Waarschuwing. In de uitdrukking $f^{-1}[B]$ heeft f^{-1} *geen* zelfstandige betekenis. De notatie f^{-1} wordt ongelukkigerwijs ook nog gebruikt voor de *inverse* van een bijectieve functie (zie Notatie 5.12, blz. 58). De relatie die de functie f óók is heeft altijd een inverse, maar die wordt aangegeven door f^* (zie Definitie 4.4.2, blz. 44), en deze inverse is niet altijd een functie. Een functie heeft niet altijd een inverse *functie*; maar de uitdrukking: $f^{-1}[B]$ is altijd gedefinieerd.

Opgaven

51 ♣ Bekijk de relatie $R := \{(0,4),(1,2),(1,3)\}$.

1. Is R een functie?
   Zoja, bepaal $Dom(R)$ en $Ran(R)$.
2. Herinner: $R^* = \{(b,a) \mid (a,b) \in R\}$ is de inverse van de relatie R. (Definitie 4.4, blz. 44).
   Is R^* een functie?
   Zoja, bepaal $Dom(R^*)$ en $Ran(R^*)$.

52 ♣ Ga na, dat $f[A] = Ran(f|A)$ en $f[Dom(f)] = Ran(f)$; $f^{-1}[B] = Dom(f \cap (X \times B))$ en $f^{-1}[Ran(f)] = Dom(f)$.

53 ♣ $X = \{0,1,2,3\}, Y = \{2,3,4,5\}, f = \{(0,3),(1,2),(2,4),(3,2)\}$. Bepaal $f|\{0,3\}$, $f[\{1,2,3\}]$ en $f^{-1}[\{2,4,5\}]$.

54 ♣ Onderstel, dat $f : X \longrightarrow Y$ en $A \subset X$. Ga na, dat $f|A = f \cap (A \times Y)$.

55 ♣ Gegeven is, dat $f : A \to Y$, $g : B \to Y$, en $A \cap B = \emptyset$. Bewijs, dat $f \cup g : A \cup B \to Y$.
Wat kan er fout gaan als $A \cap B \neq \emptyset$?

56 ♣♣ Gegeven is een verdeling V van X, en voor iedere component $A \in V$ een functie $f_A : A \to Y$. bewijs, dat $\bigcup_{A \in V} f_A : X \to Y$.

57 ♣ Gegeven zijn $f : X \to Y$, $A, B \subset X$ en $C, D \subset Y$. Bewijs:

1. $A \subset B \;\Rightarrow\; f[A] \subset f[B]$;
   $C \subset D \;\Rightarrow\; f^{-1}[C] \subset f^{-1}[D]$,
2. $f[A \cup B] = f[A] \cup f[B]$;
   $f[A \cap B] \subset f[A] \cap f[B]$;
   $f[A - B] \supset f[A] - f[B]$,
3. $f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D]$;
   $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$;
   $f^{-1}[C - D] = f^{-1}[C] - f^{-1}[D]$,
4. $f[f^{-1}[C]] \subset C$;
   $f^{-1}[f[A]] \supset A$.

($f^{-1}[\ ]$ heeft dus mooiere eigenschappen t.a.v. de verzamelingsalgebraïsche operaties dan $f[\ ]$.)
Geef eenvoudige voorbeelden waaruit blijkt dat de inclusies in 2 en 4 in het bovenstaande niet door gelijkheden kunnen worden vervangen.
Voorbeelden.
Het laatste onderdeel van 2, $f[A - B] \supset f[A] - f[B]$:
Onderstel, dat $y \in f[A] - f[B]$. Dan geldt $y \in f[A]$ en $y \notin f[B]$. Vanwege het eerste bestaat $x \in A$ zódat $y = f(x)$. Vanwege het tweede geldt $x \notin B$ (anders had je $y = f(x) \in f[B]$). Dus, $x \in A - B$, en $y = f(x) \in f[A - B]$.

Het laatste onderdeel van 3, $f^{-1}[C-D] = f^{-1}[C] - f^{-1}[D]$:

$$\begin{aligned} x \in f^{-1}[C-D] &\iff f(x) \in C - D \\ &\iff (f(x) \in C) \wedge (f(x) \notin D) \\ &\iff x \in f^{-1}[C] \wedge x \notin f^{-1}[D] \\ &\iff x \in f^{-1}[C] - f^{-1}[D]. \end{aligned}$$

De gezochte gelijkheid volgt m.b.v. Extensionaliteit.
T.b.v. onderdeel 2, vgl. Opgave 27 (blz. 37).

5.2 Surjectie, Injectie, Bijectie; Compositie

5.6 Surjectie, Injectie, Bijectie. Onderstel dat $f : X \longrightarrow Y$. f heet

1. *surjectief*, een *surjectie*, of *op* Y, notatie: $f : X \xrightarrow{\text{op}} Y$, als ieder element $b \in Y$ *minstens* één origineel heeft onder f, d.w.z., als $f[X] = Y$;

2. *injectief*, een *injectie*, of *één-éénduidig* (1–1), notatie: $f : X \xrightarrow{1-1} Y$, als iedere $b \in Y$ *hoogstens* één origineel heeft onder f;

3. *bijectief* of een *bijectie* als f zowel surjectief als injectief is.

Een bijectie $f : X \to X$ van een verzameling X naar zichzelf heet ook een *permutatie* van X.

Voorbeelden. Surjectiviteit, injectiviteit en bijectiviteit zijn bizondere eigenschappen van functies: de "meeste" functies zijn noch surjectief, noch injectief. Bijvoorbeeld, $\sin : \mathbb{R} \to \mathbb{R}$ is niet surjectief (bijv. de waarde $2 \in \mathbb{R}$ wordt door sin niet aangenomen) en niet injectief (bijv. $\sin 0 = \sin \pi$).
$1_X : X \to X$ is een bijectie, ongeacht de verzameling X.
Moeilijk voorbeeld: Laat A een verzameling zijn. Volgens Stellingen 4.11 en 4.12 is de afbeelding die een equivalentierelatie R op A transformeert in het bijbehorende quotient A/R van A modulo R een bijectie tussen de verzameling van equivalenties op A en de verzameling van verdelingen van A.
Bekijk $f := \{(0,1),(1,0),(2,1)\}$. Dus, $Dom(f) = \{0,1,2\}$. De functie $f : \{0,1,2\} \longrightarrow \{0,1\}$ is surjectief, maar $f : \{0,1,2\} \longrightarrow \{0,1,2\}$ is *niet* surjectief. Het surjectiviteits-begrip veronderstelt dus, dat met de functie ook zijn codomein is gegeven; zie 5.3 (blz. 52). Maar, ongeacht dit codomein: f is kennelijk niet injectief, omdat 0 en 2 hetzelfde beeld 1 hebben. Deze functie is dus ook niet bijectief (ongeacht het beschouwde codomein).

Hoe bewijs je dat een gegeven functie injectief/surjectief is? De volgende implicatie is een nuttige en veel gebruikte manier om uit te drukken dat een functie f injectief is:

$$f(x) = f(y) \implies x = y.$$

De contrapositie hiervan: $x \neq y \implies f(x) \neq f(y)$, is hiermee equivalent en zegt dat verschillende originelen verschillende beelden hebben.
Dat $f : X \to Y$ surjectief is wordt door de volgende bewering uitgedrukt:

$$\forall b \in Y \; \exists a \in X \; f(a) = b.$$

58 ♣ Opgave. Zijn de volgende functies injectief/surjectief? (N.B.: $\mathbb{R}^+ = \{x \in \mathbb{R} \mid 0 < x\}$.)
(i) $\sin : \mathbb{R}^+ \to \mathbb{R}$, (ii) $\sin : \mathbb{R} \to [-1, +1]$, (iii) $\sin : [-1, +1] \longrightarrow [-1, +1]$, (iv) $e^x : \mathbb{R} \to \mathbb{R}$, (v) $\tan : \mathbb{R} \to \mathbb{R}$, (vi) $\log : \mathbb{R}^+ \to \mathbb{R}$, (vii) $\surd : \mathbb{R}^+ \to \mathbb{R}^+$.

5.7 Composities. Neem aan, dat $f : X \longrightarrow Y$ en $g : Y \longrightarrow Z$. Dus: het *codomein* van f is gelijk aan het *domein* van g. De *compositie* van f en g is de functie $g \circ f : X \longrightarrow Z$ (g *na* f, ook kortweg genoteerd als gf) die gedefinieerd is door

$$(g \circ f)(x) := g(f(x)).$$

("Pas eerst f toe en vervolgens g" — dankzij de gebruikelijke "prefix"-notatie voor functie-applicatie staan f en g jammer genoeg in de, vgl. met de hier te lande gebruikelijke leesrichting, *tegenovergestelde* volgorde in de notaties $g \circ f$ en gf voor de compositie.)

N.B.: De notatie $g \circ f$ veronderstelt dus altijd, dat het *codomein* van f hetzelfde is als het *domein* van g; verder hebben $g \circ f$ en f dezelfde domeinen en $g \circ f$ en g dezelfde codomeinen.

Voorbeelden.
In de analyse kom je veel composities tegen. Bijvoorbeeld: als $f : \mathbb{R} \to \mathbb{R}^+$ de functie $x \mapsto x^2 + 1$ is, en $g : \mathbb{R}^+ \to \mathbb{R}$ de functie $x \mapsto \sqrt{x}$, dan is $g \circ f : \mathbb{R} \to \mathbb{R}$ de functie $x \mapsto \sqrt{x^2 + 1}$: $(g \circ f)(x) = g(f(x)) = g(x^2 + 1) = \sqrt{x^2 + 1}$.
Zie Opgave 71, blz. 60. De compositie $f \circ f$ van de daar gegeven functie f met zichzelf is $\{(0,2),(1,0),(2,1),(3,1),(4,0)\}$.

5.8 Opmerking. Als $f : X \to Y$, dan geldt dat $f \circ 1_X = 1_Y \circ f = f$. ⊣

Onderstel, dat $f : X \to Y$, $g : Y \to Z$ en $h : Z \to U$. Er zijn nu *drie* manieren om een functie van X naar U te definiëren: (i) $(h \circ g) \circ f$, (ii) $= h \circ (g \circ f)$, en (iii) $h \circ g \circ f$: achterelkaar uitvoeren van f, g en h. Het volgende lemma zegt, dat al deze functies hetzelfde zijn; i.h.b. is de compositie-operatie op functies dus *associatief*.

In het vervolg wordt zo'n compositie genoteerd als $h \circ g \circ f$ of kortweg als hgf.

5.9 Lemma. *Als* $f : X \to Y$, $g : Y \to Z$ *en* $h : Z \to U$, *dan geldt* $(h \circ g) \circ f = h \circ g \circ f = h \circ (g \circ f)$.

Bewijs. Onderstel, dat $x \in X$. Dan geldt:
$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))(= (h \circ g \circ f)(x)) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$.

De functies $(h \circ g) \circ f$ en $h \circ (g \circ f)$ hebben hetzelfde domein (X) en codomein (U) en vertonen op het domein dezelfde actie. Dus zijn ze (5.3, blz. 52) gelijk. ⊣

5.10 Lemma. *Onderstel, dat $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$. Er geldt:*

1. *$g \circ f$ injectief $\Longrightarrow$ f injectief,*
2. *$g \circ f$ surjectief $\Longrightarrow$ g surjectief,*
3. *f en g injectief $\Longrightarrow$ $g \circ f$ injectief,*
4. *f en g surjectief $\Longrightarrow$ $g \circ f$ surjectief.*

Bewijs. Voorbeelden.
1. *Gegeven:* $g \circ f$ injectief, d.w.z.: $(gf)(a_1) = (gf)(a_2) \Rightarrow a_1 = a_2$.
Te bewijzen: f injectief, d.w.z.: $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.
Bewijs: Neem aan, dat $f(a_1) = f(a_2)$. Dan geldt vanzelfsprekend, dat $g(f(a_1)) = g(f(a_2))$. (Als je g tweemaal hetzelfde argument $f(a_1)$ $(= f(a_2))$ toeschuift, dan levert die tweemaal dezelfde waarde af.) Maar nu geldt $(gf)(a_1) = g(f(a_1)) = g(f(a_2)) = (gf)(a_2)$. Uit het gegeven volgt dan dat $a_1 = a_2$.
2. *Gegeven:* $g \circ f$ surjectief.
Te bewijzen: g surjectief.
Bewijs: Onderstel, dat $c \in Z$. Gezocht wordt een g-origineel van c in Y. Omdat $g \circ f$ surjectief is heeft c een $g \circ f$-origineel $a \in X$. Dus, $g(f(a)) = (g \circ f)(a) = c$. M.a.w.: $f(a)$ is het gezochte g-origineel van c.
4. *Gegeven:* f en g zijn surjectief.
Te bewijzen: $g \circ f$ is surjectief. D.w.z.: ieder element $c \in Z$ heeft een origineel onder $g \circ f$.
Bewijs: Laat dus $c \in Z$. Omdat (gegeven) g surjectief is bestaat een element $b \in Y$ zódat $g(b) = c$. Omdat (gegeven) f surjectief is bestaat een element $a \in X$ zódat $f(a) = b$. Nu volgt $(g \circ f)(a) = g(f(a)) = g(b) = c$. Dus, a is het gezochte origineel. ⊣

Opgaven

59 ♣ Vgl. Lemma 5.10.1. Geef een voorbeeld waarin $g \circ f$ bijectief is, maar g niet injectief en f niet surjectief.
Goed. — Maar heb je niet een eenvoudiger voorbeeld?

60 ♣ Bewijs Lemma 5.10.3.

61 ♣ Gegeven zijn functies $f : X \to Y$ en $g : Y \to Z$ zódat hun compositie $g \circ f$ een bijectie is. Bewijs dat f surjectief is d.e.s.d.a. g injectief is.

62 ♣ (Vgl. Opgave 10, blz. 26.) Onderstel, dat $\lim_{i \to \infty} a_i = a$, en dat $f : \mathbb{N} \to \mathbb{N}$ een willekeurige injectie is. Bewijs, dat $\lim_{i \to \infty} a_{f(i)} = a$.

5.3 Inversen

De notie van een inverse van een *bijectie* is niet erg problematisch.
Herinner: $f^* = \{(b,a) \mid (a,b) \in f\} = \{(f(a),a) \mid a \in X\}$ is de inverse van de functie f opgevat als relatie (Definitie 4.4, blz. 44).

5.11 Lemma. *Als $f : X \to Y$ een bijectie is, dan is f^* een functie van Y naar X die óók een bijectie is.*

Bewijs. f^* is een functie: direct gevolg van het feit dat f injectief is.
f^* is een functie op Y, $Dom(f^*) = Y$: direct gevolg van het feit dat f surjectief is.
f^* is een functie naar X, $Ran(f^*) \subset X$: duidelijk is zelfs, dat $Ran(f^*) = X$.
Conclusie: f^* is een — surjectieve — functie van Y naar X.
f^* is injectief: Onderstel, dat $(b_1, a), (b_2, a) \in f^*$. Dan geldt $b_1 = f(a) = b_2$. ⊣

5.12 Inversen. De "relatie"-inverse f^* van een bijectie f wordt in het vervolg genoteerd als f^{-1}. f^{-1} heet *de inverse* van de bijectie f.
Waarschuwing: de notatie $f^{-1}(x)$ vooronderstelt dat f een *bijectie* is. Zie ook de eerder gegeven waarschuwing op blz. 53 m.b.t. het gebruik van f^{-1}.

Behalve inversen-zonder-meer zijn er ook nog *links-* en *rechts*-inversen.

5.13 Links- en rechts-inversen. Onderstel, dat $f : X \longrightarrow Y$, $g : Y \longrightarrow X$ en $g \circ f = 1_X$. Dan heet g een *links-inverse* van f en f een *rechts-inverse* van g.

De conditie $g \circ f = 1_X$ wil zeggen: als je een willekeurig element $a \in X$ neemt, daarop f toepast, en vervolgens g op het resultaat $f(a)$, dan ben je weer terug bij a: $g(f(a)) = a$.

Voorbeeld. Als $f : X \to Y$ een bijectie is, dan is $f^{-1} : Y \to X$ zowel links- als rechts-inverse van f.

Hierna worden o.m. de volgende vragen beantwoord:

- Wat zijn de eigenschappen van links/rechts inversen?
- Welke functies hebben een links/rechts inverse?
- Hoe maak je links/rechts inversen?

5.14 Eigenschappen.

1. *Rechts-inversen zijn injectief,*
2. *links-inversen zijn surjectief.*

Bewijs. Direct uit Lemma 5.10, aangezien $1_X : X \to X$ een bijectie is. ⊣

Het volgende lemma zegt dat als een functie f zowel een links- als een rechts-inverse heeft — dan is f dus een bijectie — die beide inversen gelijk zijn aan de inverse $f^{-1} = f^*$ van f.

5.15 Lemma. *Als $g : Y \to X$ en $h : Y \to X$ links- resp. rechts-inverse zijn van $f : X \to Y$, dan geldt $g = h = f^* = f^{-1}$.*

Bewijs. Er geldt (zie 5.8, blz. 56) $g = g \circ 1_Y = g \circ (f \circ h) = (g \circ f) \circ h = 1_X \circ h = h$. Omdat (5.14) f een bijectie is, geldt $f^* = f^{-1}$, en dit is een (zowel links- als) rechts-inverse van f. Dezelfde calculatie, met h vervangen door f^{-1}, levert dus, dat $g = f^{-1}$. ⊣

Links-inversen

Als een functie een links-inverse heeft, dan is hij daarvan een rechts-inverse, en *dus* (5.14) is hij injectief. Omgekeerd hebben injecties (op één uitzondering na) links-inversen.

Laat $f : X \to Y$ een injectie zijn. De inverse *relatie* $f^* := \{(f(a), a) \mid a \in X\}$ van f is — omdat f een injectie is — ook een functie. f^* is zelfs een injectie. Er geldt, dat $f^* : Ran(f) \to X$. Als f niet surjectief is, dan is f^* geen functie van Y naar X. Maar natuurlijk kun je f^* altijd (tenminste: als $X \neq \emptyset$) aanvullen tot zo'n functie. Opgave 63 vertelt je onder meer, dat zulke aanvullingen altijd links-inverse zijn van f. Er geldt dus:

5.16 Lemma. *Iedere injectie met een niet-leeg domein heeft een links-inverse.*

Opgaven

63 ♣ Gegeven zijn een injectie $f : X \to Y$ en een functie $g : Y \to X$. Bewijs dat de volgende twee condities equivalent zijn.

1. g is links-inverse van f,
2. $f^* \subset g$.

64 ♣ $X = \{0, 1\}$, $Y = \{2, 3, 4, 5\}$, $f = \{(0, 3), (1, 4)\}$. Nu geldt dat $f : X \to Y$. Hoeveel links-inversen heeft f?

65 ♣ Geef een voorbeeld van een injectie die *geen* links-inverse heeft.

Rechts-inversen

Als een functie een rechts-inverse heeft, dan is hij daarvan een links-inverse, en *dus* (5.14) is hij surjectief.

Laat $f : X \to Y$ een surjectie zijn. Dat $h : Y \to X$ rechts-inverse is van f betekent: $f \circ h = 1_Y$. D.w.z.: h moet een element $b \in Y$ afbeelden op een f-origineel van b. Omdat f een surjectie is, *heeft* iedere $b \in Y$ een f-origineel (misschien zelfs meer dan één). Een rechts-inverse h van de surjectie $f : X \to Y$ wordt dus verkregen door het kiezen, voor iedere $b \in Y$, van één f-origineel als h-waarde $h(b)$ van b. Dit bewijst het volgende

5.17 Lemma. *Iedere surjectie heeft een rechts-inverse.* ⊣

Opgaven

66 ♣ Hoeveel rechts-inversen heeft de functie $\{(0,5),(1,5),(2,5),(3,6),(4,6)\}$ (beschouwd als functie van $\{0,1,2,3,4\}$ naar $\{5,6\}$)?

67 ♣ In de analyse komen veel rechts-inversen voor. De volgende opgaven illustreren dat daar meestal één de voorkeur verdient.

1. De surjectie $f : \mathbb{R} \to \mathbb{R}^+$ wordt gedefinieerd door $f(x) := x^2$. Geef drie verschillende rechts-inversen van deze functie.
2. Zelfde vraag voor de surjectie $g : [0,\pi] \to [0,1]$ gedefinieerd door $g(x) := \sin x$.

De volgende opgave laat zien, dat alle rechts-inversen van een surjectie f verkregen worden door de inverse relatie f^* van f (die misschien geen functie is) te verkleinen tot een functie.

68 ♣ Gegeven zijn een surjectie $f : X \to Y$ en een functie $h : Y \to X$. Bewijs dat de volgende twee condities equivalent zijn.

1. h is rechts-inverse van f,
2. $h \subset f^*$.

***Functies als verdelingen.** In de praktijk worden equivalentierelaties of verdelingen vaak ingevoerd via een functie. *Par abus de language* worden functies daarom soms verdelingen genoemd. Voorbeelden van zulke functies op de verzameling van alle mensen: "de sexe van x" (verdeelt de bevolking in mannen en vrouwen), "de kleur van x" (raciale verdeling), "de leeftijd van x" (plm. honderd equivalentieklassen). De volgende opgave legt uit hoe dit in zijn werk gaat en vraagt aan te tonen dat iedere equivalentierelatie zó kan worden verkregen.

69 ♣ Laat $f : A \to I$ een surjectie zijn. Definieer de relatie R op A door: $aRb :\equiv f(a) = f(b)$. Dus, $R = \{(a,b) \in A^2 \mid f(a) = f(b)\}$. Bewijs:

1. R is een equivalentie op A,
2. $A/R = \{f^{-1}[\{i\}] \mid i \in I\}$,
3. bij iedere equivalentie S op A bestaat een functie g op A zódat $aSb \Leftrightarrow g(a) = g(b)$.

70 ♣ Gegeven is $f : A \to B$; $A \neq \emptyset$.

1. Bewijs: als f een injectie is dan bestaat bij iedere $g : A \to C$ een functie $h : B \to C$ zódat $g = hf$.
2. Bewijs: als bij iedere $g : A \to C$ een functie $h : B \to C$ bestaat zódat $g = hf$, dan is f een injectie.

71 ♣ De functie $f : \{0,1,2,3,4\} \to \{0,1,2,3,4\}$ is gedefinieerd door de volgende tabel:

x	0	1	2	3	4
$f(x)$	1	2	0	0	3
$(ff)(x)$					
$(fff)(x)$					

1. Bepaal de composities ff, fff en $ffff$ door verder invullen van de tabel.
2. Hoeveel elementen heeft de verzameling $\{f, ff, fff, \ldots\}$? (N.B.: de elementen van deze verzameling zijn dus functies!)
3. Geef een voorbeeld van een functie $g : \{0,1,2,3,4\} \to \{0,1,2,3,4\}$ zódat $\{g, gg, ggg, \ldots\}$ 6 elementen heeft.

72 ♣ Gegeven is een eindige verzameling A en een bijectie $f : A \to A$. $f^1 = f$, $f^2 = ff$, $f^3 = fff$,... zijn dan allemaal bijecties : $A \to A$.

1. Bewijs dat ergens in deze rij de bijectie 1_A voorkomt. D.w.z.: er is een getal n zódat $f^n = 1_A$.
2. Onderstel, dat A k elementen heeft. Kun je een bovengrens geven voor n?

73 ♣ Gegeven is een functie $h : X \to X$ met de eigenschap, dat $hhh = 1_X$.
Bewijs, dat h een bijectie is.
Geef een eenvoudig voorbeeld van een verzameling X en een functie $h : X \to X$ zódat $hhh = 1_X$ en $h \neq 1_X$.

74 ♣ Gegeven is een equivalentie relatie R op een verzameling A. Bewijs: bij iedere equivalentie $S \supset R$ op A bestaat een functie $g : A/R \to A/S$ met, voor $a \in A$: $|\, a \,|_S = g(|\, a \,|_R)$.

75 ♣ Bewijs: iedere functie die een surjectieve rechts-inverse heeft is een bijectie.
Idem: iedere functie die een injectieve links-inverse heeft is een bijectie.

5.4 *Definiëren van Functies en Relaties op Quotienten

Opgave 76 beschrijft een probleem dat je geregeld zal tegenkomen in situaties waarin een equivalentierelatie een rol speelt. (Hier vind je als voorbeelden alleen de definities van de arithmetische operaties op kardinaalgetallen en hun ordening in Sectie 8.5 en die voor ordetypen in Definities 10.5, 10.7, 10.8 en 10.10.)

Hierbij is een functie (of relatie) f gegeven op een verzameling A waarop een equivalentierelatie $\sim$ is gedefinieerd. Het probleem bestaat eruit te laten zien dat een "soortgelijke" functie (of relatie) $f^\sim$ bestaat op het quotient $A/\sim$ van equivalentieklassen modulo $\sim$ (Definitie 4.10 blz. 47). De opgave geeft een conditie waaronder dit mogelijk is.

Voorbeeld. $A = \mathbb{Z}$, $\sim = mod(4)$, $f = +$ is de optellings-operatie. Ga na, dat aan (5.1) uit Opgave 76 is voldaan. Uit dezelfde Opgave volgt nu, dat een operatie $+' := +^{mod(4)}$ op $\mathbb{Z}/mod(4)$ bestaat zódat $|n| +' |m| = |n+m|$: de optelling van $\mathbb{Z}$ induceert een "optelling" op het quotient $\mathbb{Z}/mod(4)$. Voor deze nieuwe optelling geldt bijvoorbeeld, dat $|3| +' |2| = |5| = |1|$.
Hetzelfde verschijnsel doet zich voor t.a.v. vermenigvuldiging $\times$. Merk op, dat voor $\times' := \times^{mod(4)}$ geldt, dat $|2| \times' |2| = |4| = |0|$: in $\mathbb{Z}/mod(4)$ is het nul-element te schrijven als product van elementen (zgn. *nul-delers*) die van het nul-element verschillen.

Zie verder onder 5.18.

76 ♣ Opgave. Onderstel, dat $\sim$ een equivalentierelatie is op A en dat $f : A^2 \to A$ een (bijv.) binaire functie is van A naar A zódat aan de volgende conditie is voldaan voor alle $a, b, x, y \in A$:

$$a \sim x \wedge b \sim y \implies f(a,b) \sim f(x,y). \tag{5.1}$$

Bewijs dat precies één functie $f^\sim : (A/\sim)^2 \to B$ bestaat zódat voor $a, b \in A$: $f^\sim(|a|,|b|) = |f(a,b)|$.

5.18 Representant-onafhankelijke definitie. De voorafgaande opgave zegt a.h.w. dat, onder conditie (5.1), een functie $f^\sim$ kan worden gedefinieerd op het quotient $A/\sim$ door de vergelijking $f^\sim(|a|,|b|) = |f(a,b)|$.

Behalve dat conditie (5.1) *voldoende* is opdat de vergelijking $f^\sim(|a|,|b|) = |f(a,b)|$ opgevat kan worden als definitie van een functie $f^\sim$ is ze ook *noodzakelijk*. Immers, als $x \sim a$ en $y \sim b$ gelden, dan hebben we dat $|a| = |x|$ en $|b| = |y|$. En dan volgt $|f(a,b)| = f^\sim(|a|,|b|) = f^\sim(|x|,|y|) = |f(x,y)|$, dus $f(a,b) \sim f(x,y)$.

Met de kreet, dat de "definitie" $f^\sim(|a|,|b|) = |f(a,b)|$ van $f^\sim$ *representant-onafhankelijk* is, d.w.z.: dat de "uitkomst" $|f(a,b)|$ van $f^\sim(|a|,|b|)$ niet van de gekozen representanten a en b van de klassen $|a|$ en $|b|$ afhangt, wordt bedoeld dat aan conditie (5.1) wordt voldaan.

Een analoog verhaal gaat op voor het definiëren van één-argumentige functies, of relaties, op $A/\sim$. Zie Opgave 77.

Opgaven.

77 ♣ Onderstel, dat $\sim$ een equivalentierelatie is op A en dat $R \subset A^2$ een relatie is op A zódat aan de volgende conditie is voldaan voor alle $a, b, x, y \in A$:

$$a \sim x \wedge b \sim y \wedge aRb \;\Rightarrow\; xRy. \tag{5.2}$$

Bewijs dat precies één relatie $R^\sim \subset (A/\sim)^2$ bestaat zódat voor $a, b \in A$: $|a| R^\sim |b| \;\Leftrightarrow\; aRb$.

78 ♣ A en B zijn verzamelingen. Definieer de relatie $\sim$ op $A \times B$ door: $(a,b) \sim (x,y) \;\equiv\; a = x$. Ga na, dat $\sim$ een equivalentie is op $A \times B$. Geef een bijectie $: (A \times B)/\!\!/\sim \longrightarrow A$ tussen het quotient van $A \times B$ modulo $\sim$ en A. Geef, voor iedere equivalentieklasse, een bijectie tussen de klasse en B.

5.5 *Producten en Machten

5.19 Producten, Machten. Onderstel dat voor ieder element $i \in I$ een niet-lege verzameling X_i is gegeven. Het *product* $\prod_{i \in I} X_i$ is de verzameling van alle functies f zódat $Dom(f) = I$ terwijl voor alle $i \in I$: $f(i) \in X_i$.
Voor $I = \{0, \ldots, n-1\}$ wordt dit product ook genoteerd als $X_0 \times \cdots \times X_{n-1}$.
Als alle X_i $(i \in I)$ hetzelfde zijn, $X_i = X$, dan wordt dit product genoteerd als X^I. Dit heet een *macht*.

Notatie. X^I is dus de verzameling van alle functies $f : I \to X$.

Opgaven

79 ♣♣ Onderstel, dat X en I n resp. m elementen hebben. Ga na, dat X^I er n^m heeft.
Aanwijzing. Inductie naar m — zie evt. Hoofdstuk 6, blz. 65, voor Volledige Inductie.

Er zijn nu *twee* verschillende interpretaties van de uitdrukking $X \times Y$: (i) als $\prod_{i \in \{0,1\}} X_i$ met $X_0 = X$ en $X_1 = Y$, en (ii) als $\{(x, y) \mid x \in X \wedge y \in Y\}$.

80 ♣♣ Waarom "kan dit geen kwaad"?

81 ♣♣ Gegeven zijn de verzamelingen X en Y.
Op de functieverzameling $Y^X := \{f \mid f : X \to Y\}$ wordt de relatie $\approx$ gedefinieerd door:
$f \approx g :\equiv$ er zijn permutaties i van X en j van Y (bijecties $i : X \to X$ en $j : Y \to Y$) zódat $if = gj$.

1. Bewijs dat $\approx$ een equivalentierelatie is op Y^X.
2. Gegeven is dat $Y = \{0, 1, 2\}$ en $X = \{0, 1, 2, 3\}$.
   (a) Bewijs: als $f, g : Y \to X$ injecties zijn, dan geldt $f \approx g$.
   (b) Bewijs dat $\{(0, 0), (1, 0), (2, 1)\} \approx \{(0, 1), (1, 3), (2, 3)\}$.
   (c) Hoeveel equivalentieklassen heeft $\approx$? Geef van iedere equivalentieklasse één representant.

82 ♣

1. Gegeven zijn verzamelingen X, Y en Z en een functie $h : Y \to Z$. Definieer de afbeelding $F : Y^X \to Z^X$ door $F(g) := hg$. Bewijs:
   (a) als h een injectie is, dan is F een óók injectie,
   (b) als h een surjectie is, dan is F óók een surjectie.
2. Gegeven zijn verzamelingen $X \neq \emptyset$, Y en Z en een functie $h : X \to Y$. Definieer de afbeelding $F : Z^Y \to Z^X$ door $F(g) := gh$. Bewijs:
   (a) als h een injectie is, dan is F een surjectie,
   (b) als h een surjectie is, dan is F een injectie.

Samenvatting

Belangrijkste begrippen:

- functie, functie op, functie van...naar, domein, codomein,
- $f(a)$, $Dom(f)$, $Ran(f)$, $f : X \to Y$, $f : a \mapsto b$,
- $f|A$, $f[A]$, $f^{-1}[B]$,
- surjectief, injectief, bijectief,
- compositie $g \circ f$,

- (links-, rechts-) inversen.

Vragen:

- wat zijn de verbanden tussen injectiviteit en surjectiviteit van functies en hun composities?
- welke functies hebben (links/rechts-) inversen, en hoe maak je die inversen?

Hoofdstuk 6

Eindig vs. Oneindig

Verzamelingen kunnen worden ingedeeld naar grootte. Een eerste onderscheiding is die in eindige- en oneindige verzamelingen: het onderwerp van dit hoofdstuk. De grootte van een eindige verzameling kan worden vastgesteld door zijn elementen te tellen. Hier zie je dat het ook mogelijk is om op een precieze manier over de grootte van *oneindige* verzamelingen te spreken. Het is één van de grote ontdekkingen van Cantor dat er oneindige verzamelingen van verschillende grootte zijn. Bijvoorbeeld: $\mathbb{Q}$ heeft (weliswaar méér, maar) — in de precieze betekenis van Definitie 6.6 — *evenveel* elementen als $\mathbb{N}$, terwijl het aantal elementen van $\mathbb{R}$ *groter* is dan dat van $\mathbb{N}$. Deze ontdekking is het onderwerp van Hoofdstuk 8.

6.1 Volledige Inductie

$\mathbb{N} = \{0, 1, 2, \ldots\}$ is de verzameling van natuurlijke getallen. Misschien de belangrijkste eigenschap van de natuurlijke getallen wordt gegeven door het Principe van Volledige Inductie, dat je in staat stelt *universele* beweringen van de vorm $\forall n \in \mathbb{N}\, E(n)$ te bewijzen.

6.1 Volledige Inductie. *Voor iedere verzameling $X \subset \mathbb{N}$ geldt:*
als $0 \in X$ en $\forall n \in \mathbb{N}(n \in X \Rightarrow n+1 \in X)$, dan $X = \mathbb{N}$. ⊣

Het principe van volledige inductie lijkt op het eerste gezicht tamelijk flauw: het is immers zo overduidelijk *geldig*. Namelijk, onderstel eens, dat voor $X \subset \mathbb{N}$ geldt dat $0 \in X$ en $\forall n \in \mathbb{N}(n \in X \Rightarrow n+1 \in X)$. Dan is het duidelijk, dat ook $\mathbb{N} \subset X$ (en dus $X = \mathbb{N}$): $0 \in X$ geldt per hypothese. Verder geldt i.h.b. ($\forall$E, $n := 0$) dat $0 \in X \Rightarrow 1 \in X$. Dus (MP), $1 \in X$. Maar ook geldt ($\forall$E, $n := 1$) dat $1 \in X \Rightarrow 2 \in X$. Dus, $2 \in X$. Enzovoorts, de hele rij van natuurlijke getallen af.

Maar, ondanks deze overduidelijke geldigheid: het belang van inductie kan moeilijk worden onderschat. Het is het belangrijkste, en in essentie het enige, instrument waarmee informatie kan worden verkregen over de (elementen van

de) oneindige verzameling $\mathbb{N}$, en, meer algemeen, over eindige verzamelingen (zie Opgave 98, blz. 73).

Verzamelingen vs. Eigenschappen. Met iedere *eigenschap* E van natuurlijke getallen correspondeert een *verzameling* van natuurlijke getallen: $\{n \in \mathbb{N} \mid E(n)\}$ (zie blz. 31). Volledige inductie kan daarom ook met eigenschappen i.p.v. met verzamelingen worden geformuleerd, als volgt:

> Als E een eigenschap van natuurlijke getallen is, waarvoor geldt dat
>
> (i) $E(0)$,
> (ii) $\forall n \in \mathbb{N}\,[E(n) \;\Rightarrow\; E(n+1)]$,
>
> dan geldt dat $\forall n \in \mathbb{N}\, E(n)$.

Inductie: -Basis, -Stap, -Hypothese. Opdat $E(n)$ geldt voor alle $n \in \mathbb{N}$ is het volgens het inductie principe voldoende om te laten zien
(i) dat dit i.h.b. geldt voor $n = 0$, i.e., dat $E(0)$, en
(ii) dat dit geldt voor $n+1$, onder de veronderstelling dat het geldt voor n; i.e., dat $\forall n \in \mathbb{N}\,[E(n) \;\Rightarrow\; E(n+1)]$.

Een bewijs van (i) heet de *basis* van het bewijs met inductie, en een bewijs van (ii) de *inductiestap*. Voor die inductiestap moet kennelijk (volgens de bewijsregels $\forall$I en $\rightarrow$I) voor een *willekeurig* natuurlijk getal n worden aangetoond, dat $E(n+1)$ geldt, terwijl geldigheid van $E(n)$ als *gegeven* mag worden aangenomen. Dit nieuwe gegeven heet de *inductiehypothese*. De aardige bonus van een bewijs met inductie is, dat deze inductiehypothese helemaal gratis is.

Voetangels? Klemmen? De eerste keren dat je inductie tegenkomt of inductie zelf probeert te gebruiken, kan het je mogelijk verontrusten dat je zomaar per inductiehypothese aannemen kunt, dat een *willekeurig* getal n de betreffende eigenschap E heeft. Dat is toch immers precies wat er te bewijzen valt? Maar door het zó, met de bepaling 'willekeurig' te formuleren, wordt je op het verkeerde been gezet: zie de discussie 2.1 (blz. 23) over *willekeurige* dingen. De inductiestap bestaat uit het bewijs van $\forall n \in \mathbb{N}\,[E(n) \;\Rightarrow\; E(n+1)]$. Hoe je een bewering van deze vorm geacht wordt te bewijzen lees je bij de behandeling van de regels $\forall$I (generalisatieregel) en $\rightarrow$I (deductieregel) in Hoofdstuk 2, en dat komt precies neer op wat hierboven is uitgelegd.

6.2 Inkleding. Volledige inductie ingekleed als bewijsregel (IND) —zie de schemas op blzz. 24 en 90— kan als volgt worden weergegeven:

$$\dfrac{\begin{array}{c}[E(n)]^1 \\ \vdots \\ E(0) \qquad E(n+1)\end{array}}{\forall n\, E(n)}\ \text{IND}-1$$

Een bewijs van een bewering van de vorm $\forall n\, E(n)$ m.b.v. volledige inductie heet een bewijs met inductie *naar* n. Het noemen van de *inductie parameter* n

is nuttig, i.h.b. als er nog andere parameters in de eigenschap E figureren. Volgens het hierboven weergegeven schema kan een conlcusie van de vorm $\forall n\, E(n)$ worden getrokken op grond van (i) een premisse, dat $E(0)$, en (ii) een afleiding van $E(n+1)$ uit de (inductie)hypothese $E(n)$. Bij het trekken van die conclusie wordt de hypothese ingetrokken.

In een gewone tekst kan een bewijs met inductie worden gestruktureerd d.m.v. de volgende aanheffen (zie ook Subsectie 2.1, blz. 15 e.v.).

Gegeven: ...
Te Bewijzen: $\forall n\, E(n)$.
Bewijs: Ik bewijs, met inductie naar n, dat voor alle n, $E(n)$.
(Kortweg: bewijs met inductie naar n.)
Basis.
Bewijs, dat $E(0)$: ..... (1)
Inductie stap.
Inductie hypothese (= nieuw *gegeven*):
Onderstel dat n een getal is, waarvoor $E(n)$ geldt.
Ik moet nu laten zien (= nieuw *te bewijzen*), dat $E(n+1)$.
Bewijs hiervan: ..... (2)
Uit (1) en (2) volgt nu, met Volledige Inductie, dat $\forall n\, E(n)$. ⊣

Inductie vanaf m. Een variant van inductie is *inductie vanaf* m. Laat $m \in \mathbb{N}$. Voor iedere $X \subset \mathbb{N}$ geldt: als (i) $m \in X$, en (ii) $\forall n \geqslant m\,[n \in X \;\Rightarrow\; n+1 \in X]$, dan geldt $\forall n \in \mathbb{N}[m \leqslant n \;\Rightarrow\; n \in X]$.

Er is een variant van volledige inductie, *Sterke Inductie*, die dingen kan waartoe gewone volledige inductie niet in staat is. Weer zijn twee formuleringen mogelijk: met verzamelingen en met eigenschappen. Hier is de variant met eigenschappen:

6.3 Sterke Inductie. *Voor iedere eigenschap E van natuurlijke getallen:*
als $\forall n \in \mathbb{N}\,[\,(\forall m < n\, E(m)) \;\Rightarrow\; E(n)\,]$, *dan geldt* $\forall n \in \mathbb{N}\, E(n)$.

Sterke inductie is een *stelling*, omdat je dit principe bewijzen kunt m.b.v. volledige inductie: zie hierna.

Bij het *gebruik* van sterke inductie is de conditie: $\forall m < n\, E(m)$ de *inductiehypothese* waaronder je $E(n)$ moet zien te bewijzen. De inductiehypothese is hier dus (althans, voor $n > 1$) sterker dan bij gewone inductie!

Merk op: bij het gebruik van volledige inductie moet je *twee* dingen laten zien: de *basis*, en de *inductehypothese*. Bij het gebruik van sterke inductie moet je maar *één* ding laten zien: er is hier alleen nog een "inductiestap": *sterke inductie kent geen basis*!

Bewijs. (van 6.3.) Onderstel, dat $\forall n \in \mathbb{N}\,[\,(\forall m < n\, E(m)) \;\Rightarrow\; E(n)\,]$. (1)
Definieer de verzameling X door: $X := \{n \mid \forall m < n\, E(m)\}$. Onderstelling (1) zegt juist, dat ieder element van X eigenschap E heeft. Het is dus voldoende om aan te tonen, dat ieder natuurlijk getal in X zit. Dit gebeurt met gewone

volledige inductie.
Basis. $0 \in X$.
D.w.z.: $\forall m < 0\, E(m)$. Uitgeschreven: $\forall m[m < 0 \Rightarrow E(m)]$. Dit spreekt "vanzelf", omdat er geen natuurlijke getallen m kleiner dan 0 zijn. Preciezer: de implicatie $m < 0 \Rightarrow E(m)$ is — ongeacht de waarde van m — *waar* omdat z'n linkerlid ($m < 0$) *onwaar* is: zie de waarheidstafel van het implicatie-teken. (Dit is weer één van die gevallen waarin een implicatie "triviaal waar" is.)
Inductiestap.
Onderstel, dat (*inductiehypothese*) $n \in X$. Dit betekent: $\forall m < n\, E(m)$. Onderstelling (1) impliceert nu, dat ook $E(n)$ geldt. Maar dan hebben we dus, dat $\forall m < n+1\, E(m)$. En dit betekent weer, dat $n+1 \in X$. De inductiestap is compleet.
Met volledige inductie volgt nu, dat $X = \mathbb{N}$. Volgens de opmerking aan het begin geldt nu dat $\forall n \in \mathbb{N}\, E(n)$, en dus is het bewijs klaar. ⊣

De toepassingen die van inductie worden gemaakt in Sectie 6.2 zijn meestal eenvoudig. Een aantal is gebaseerd op de versie van het inductie principe voor eindige verzamelingen zoals dat is geformuleerd in Opgave 98, blz. 73. Interessantere toepassingen zijn te vinden in Secties 6.3 en 7.4.

Een veelgebruikte versie van inductie is het minimaliteitsprincipe.

6.4 Minimaliteits Principe. *Iedere niet-lege verzameling van natuurlijke getallen heeft een kleinste element.*

Bewijs. Laat A een (niet-lege) verzameling van natuurlijke getallen zijn. Het is kennelijk voldoende om te laten zien dat voor iedere $n \in \mathbb{N}$ geldt:

$$n \in A \Rightarrow A \text{ heeft een kleinste element.}$$

(Immers, dat $A \neq \emptyset$ betekent dat er een $n \in A$ moet bestaan. *Dus* volgt uit deze implicatie, toegepast (∀E) op een dergelijk element n van A, dat A een kleinste element heeft.)
Hier volgt een bewijs van deze bewering, met sterke inductie naar n. T.b.v. de inductiestap mag je onderstellen dat n een getal is waarvoor je de volgende inductiehypothese kado krijgt:
Inductiehypothese: voor alle $m < n$: $m \in A \Rightarrow A$ heeft een kleinste element.
Te bewijzen: $n \in A \Rightarrow A$ heeft een kleinste element.
Bewijs: Onderstel, dat $n \in A$.
(i) n is ("toevallig") het kleinste element van A. Klaar!
(ii) n is *niet* kleinste element van A. Maar dat betekent dat een $m \in A$ bestaat met $m < n$. Inductiehypothese toepassend op m (∀E): A heeft (ook nu) een kleinste element. ⊣

Opmerking. Het bewijs kan ook worden uitgevoerd met de logica van Hoofdstuk 1. Dit is veel omslachtiger dan de hiervoor gegeven redenatie; maar het voordeel is, dat je ziet dat het Minimaliteitsprincipe en Sterke Inductie logisch gezien op hetzelfde neerkomen.

Merk op, dat Sterke Inductie het volgende bewering-schema is:

$$\forall n[\forall m < n\, E(m) \;\Rightarrow\; E(n)] \;\Rightarrow\; \forall n\, E(n).$$

Omdat dit geldt voor iedere eigenschap E geldt het i.h.b. voor *negaties* van eigenschappen. Dus:

$$\forall n[\forall m < n \neg E(m) \;\Rightarrow\; \neg E(n)] \;\Rightarrow\; \forall n \neg E(n).$$

Transformeer deze uitdrukking nu in vier stappen als volgt. Pas eerst contrapositie, dat is: Stelling 1.5.3, blz. 10, toe. Dan krijg je het equivalent

$$\neg\forall n \neg E(n) \;\Rightarrow\; \neg\forall n[\forall m < n \neg E(m) \;\Rightarrow\; \neg E(n)].$$

Pas nu Stelling 1.10.5 (blz. 12) (en Stelling 1.11, blz. 13) toe. Je krijgt het equivalent

$$\exists n\, E(n) \;\Rightarrow\; \exists n \neg[\forall m < n \neg E(m) \;\Rightarrow\; \neg E(n)].$$

Vervolgens gebruik je Stelling 1.5.2 (en Stelling 1.11). Dit leidt tot:

$$\exists n\, E(n) \;\Rightarrow\; \exists n[\forall m < n \neg E(m) \;\wedge\; \neg\neg E(n)].$$

Een drietal laatste transformaties (wet van dubbele negatie, commutativiteit conjunctie, een kwantor-manipulatie) leveren tenslotte het eindproduct:

$$\exists n\, E(n) \;\Rightarrow\; \exists n[E(n) \;\wedge\; \neg\exists m < n\, E(m)]$$

— en dit is precies het minimaliteitsprincipe (geformuleerd met eigenschappen).

Opgaven

83 ♣ In 6.2 wordt (i) Volledige Inductie gepresenteerd als bewijsregel, en (ii) de algemene gedaante beschreven waarin bewijzen met Volledige Inductie dienen te worden gegoten. Geef de bewijsregel en de algemene gedaante behorend bij Sterke Inductie 6.3.

84 ♣ Bewijs *Inductie vanaf m.*
Aanwijzing. Pas volledige inductie toe op de verzameling $Y := \{n \mid m + n \in X\}$.

85 ♣ Onderstel dat voor $X \subset \mathbb{N}$ geldt, dat $1 \in X$ en $\forall n \in \mathbb{N}(n \in X \;\Rightarrow\; n+2 \in X)$. Bewijs dat ieder oneven natuurlijk getal element is van X.

6.5 *Gefundeerd. Een relatie $\prec$ op een verzameling A heet *gefundeerd* of *welgefundeerd* als er geen oneindige dalende rij elementen $\cdots \prec a_2 \prec a_1 \prec a_0$ bestaat in A. Anders gezegd: iedere rij $a_0 \succ a_1 \succ a_2 \succ \cdots$ in A breekt af.

86 ♣ Bewijs dat $<$ gefundeerd is op $\mathbb{N}$: er is geen oneindige dalende rij natuurlijke getallen $n_0 > n_1 > n_2 > \cdots$.
Aanwijzing. Toon aan, met sterke inductie naar n, dat: voor alle $n \in \mathbb{N}$, $E(n)$; waarbij $E(n)$ betekent: er bestaat geen oneindige dalende rij natuurlijke getallen $n_0 = n > n_1 > n_2 > \cdots$ die begint bij n.

87 ♣ Onderstel dat $\emptyset \neq X \subset \mathbb{N}$, en dat X *begrensd* is, d.w.z.: dat een getal $m \in \mathbb{N}$ bestaat zódat voor alle $n \in X$, $n \leqslant m$. Bewijs, dat X een *maximum* heeft; d.i.: dat een *element* m *van* X bestaat zódat voor alle $n \in X$, $n \leqslant m$.
Aanwijzing. Inductie naar m. De eigenschap $E(m)$ is dus: iedere niet-lege verzameling $X \subset \mathbb{N}$ waarvoor geldt dat $\forall n \in X\ (n \leqslant m)$, heeft een maximum.

88 ♣ Onderstel, dat voor $f : \mathbb{N} \to \mathbb{N}$ geldt, dat $n < m \ \Rightarrow \ f(n) < f(m)$. Bewijs dat voor alle $n \in \mathbb{N}$: $n \leqslant f(n)$.
Aanwijzing. Onderstel (BO) dat een $n \in \mathbb{N}$ bestaat waarvoor niet $n \leqslant f(n)$, i.e., waarvoor $f(n) < n$. Dan bestaat volgens het Minimaliteits Principe 6.4 ook een *kleinste* dergelijke n. Leid hieruit, m.b.v. het gegeven, een tegenspraak af.

89 ♣ Hier is een bewijs met inductie, dat alle Amsterdammers evenveel haren op hun hoofd hebben. Dit volgt uit de volgende bewering voor $n = 850.000$ (of daaromtrent).
Bewering: in iedere verzameling van n mensen heeft iedereen evenveel haren op zijn/haar hoofd.
Bewijs. Inductie "naar n".
Basis. $n = 0$ (of $n = 1$): er valt hier niets te bewijzen.
Inductiestap. Inductiehypothese: het geldt voor verzamelingen van n mensen.
Laat A nu een $(n+1)$-elementige mensenverzameling zijn. Neem $p, q \in A$. $A - \{p\}$ en $A - \{q\}$ hebben n elementen en dus hebben alle mensen in deze verzamelingen evenveel haren op hun hoofd. Maar dan hebben p en q dat ook. (: Als $r \in A - \{p, q\}$ dan hebben r en q evenveel haren: $r, q \in A - \{p\}$; en hetzelfde geldt voor r en p. Dus hebben p en q evenveel haren.)
Verklaar het verschijnsel dat de hoofdbedekkingen van de Amsterdammers Patijn en Nordholt verschillend van dikte zijn.

6.2 Gelijkmachtigheid

Om na te gaan, of twee eindige verzamelingen evenveel elementen hebben, hoef je ze niet noodzakelijk te *tellen*: ze hebben evenveel elementen dan en slechts dan als er een bijectie tussen hen bestaat. (Soms is het simpeler om een bijectie te maken dan te tellen: om te weten of er evenveel mensen als stoelen in een volle zaal zijn laat je iedereen even gaan zitten!) Deze observatie motiveert de volgende definitie, die de basis van dit hoofdstuk vormt.

6.6 Gelijkmachtig. Verzamelingen A en B heten *gelijkmachtig* als er een bijectie van A naar B is. Notatie: $A \sim B$.

6.7 Flauw Maar Desondanks Belangrijk Voorbeeld. $\mathbb{N}$ is gelijkmachtig met z'n echte deelverzameling $\mathbb{N}^+ := \mathbb{N} - \{0\}$ door de bijectie (de *opvolger-functie*) gedefinieerd door $n \longmapsto n + 1$.

Gelijkmachtig te zijn met een echte deelverzameling is in feite karakteristiek voor oneindige verzamelingen: zie Opgave 152, blz. 104. Een echte deelverzameling van een *eindige* verzameling is nooit gelijkmachtig met die verzameling: Opgave 102, blz. 73. Toepassing van het gelijkmachtigheids-begrip op oneindige verzamelingen kan dus voor verrassingen zorgen.

De volgende makkelijke stelling zegt dat de relatie $\sim$ een equivalentie is op de collectie van alle verzamelingen. (Zie Definitie 8.17, blz. 110, voor de bijbehorende equivalentieklassen.)

6.8 Stelling. *Voor alle verzamelingen A, B, C geldt:*

1. $A \sim A$ *(reflexiviteit),*

2. $A \sim B \implies B \sim A$ *(symmetrie),*

3. $A \sim B \ \wedge \ B \sim C \implies A \sim C$ *(transitiviteit).*

Bewijs.
1. De identiteitsfunctie 1_A op A is een bijectie van A naar A.
2. Als $f : A \to B$ een bijectie is, dan is de inverse f^{-1} van f een bijectie van B naar A.
3. Als $f : A \to B$ en $g : B \to C$ bijecties zijn, dan is hun compositie $g \circ f = gf$ een bijectie van A naar C (zie Lemma 5.10.3/4, blz. 57). ⊣

Het prototype van een n-elementige verzameling is $\{0, \ldots, n-1\}$. ($\{1, \ldots, n\}$ is natuurlijk óók goed.) Dit motiveert onderdeel 1 van de volgende definitie.

6.9 Eindig, Oneindig.

1. Een verzameling A *heeft n elementen* als $A \sim \{0, \ldots, n-1\}$.
2. A heet *eindig* als een $n \in \mathbb{N}$ bestaat zódat A n elementen heeft.
3. Een verzameling A heet *oneindig* als hij niet eindig is, d.w.z.: als voor alle n, $A \not\sim \{0, \ldots, n-1\}$.

6.10 Voorbeeld.
1. $\emptyset$ heeft 0 elementen en is dus eindig: als $n = 0$ dan geldt immers dat $\{0, \ldots, n-1\} = \emptyset$.
2. Als de verzameling A eindig is (bijv. n elementen heeft) en x is een willekeurig ding, dan is $A \cup \{x\}$ eveneens eindig: deze verzameling heeft dan immers n of $n+1$ elementen, naar gelang x element is van A of niet.

De volgende stelling zal niet als een donderslag bij heldere hemel komen — maar het bewijs illustreert het gebruik van de definities en van inductie.

6.11 *Stelling. $\mathbb{N}$ *is oneindig.*

Bewijs. Met inductie naar n wordt aangetoond dat voor alle $n \in \mathbb{N}$ geldt: $\mathbb{N} \not\sim \{0, \ldots, n-1\}$. De inductiestap doet een een beroep op Opgave 90.
Basis.
Voor $n = 0$ geldt er $\{0, \ldots, n-1\} = \emptyset$. Een niet-lege verzameling ($\mathbb{N}$) is nooit gelijkmachtig met de lege verzameling. (Er is niets waar die bijectie de elementen van de niet-lege verzameling naar toe kan sturen.)

Inductiestap.
Inductiehypothese: $\mathbb{N} \not\sim \{0, \ldots, n-1\}$.
Te bewijzen: $\mathbb{N} \not\sim \{0, \ldots, n\}$.
Bewijs: Onderstel, dat tóch een bijectie van $\mathbb{N}$ naar $\{0, \ldots, n\}$ bestaat. (Zie regel ¬I van Hoofdstuk 2.) Volgens Opgave 90 mag je wel onderstellen, dat er dan óók een bijectie f van $\mathbb{N}$ naar $\{0, \ldots, n\}$ bestaat, waarvoor $f(0) = n$. De restrictie $f|(\mathbb{N} - \{0\})$ (Definitie 5.4 blz. 53) is dan een bijectie tussen $\mathbb{N} - \{0\}$ en $\{0, \ldots, n-1\}$. Nu geldt, dat $\mathbb{N} \sim (\mathbb{N} - \{0\})$ (*Flauw Maar Desondanks Belangrijk Voorbeeld* 6.7). Conclusie (Stelling 6.8.3): $\mathbb{N} \sim \{0, \ldots, n-1\}$. Tegenspraak met de inductiehypothese. ⊣

Opgaven

90 ♣ Onderstel dat $A \sim B$, $a \in A$ en $b \in B$.
Bewijs, dat een bijectie $f : A \to B$ bestaat zódat $f(a) = b$.
Aanwijzing. Omdat $A \sim B$ geldt bestaat een bijectie $g : A \to B$. Als toevallig geldt, dat $g(a) = b$, dan neem je natuurlijk $f := g$. Onderstel dus, dat $g(a) = b' \neq b$. Omdat g surjectief is bestaat $a' \in A$ zódat $g(a') = b$. Maak een plaatje van de situatie en kijk of je de gezochte functie f kan krijgen door g geschikt te modificeren.

91 ♣ Gegeven is, dat $A \sim B$. M.a.w.: *gegeven* wordt een bijectie $f : A \longrightarrow B$. Bewijs, dat $\wp(A) \sim \wp(B)$. M.a.w., *gevraagd* wordt een bijectie $\varphi : \wp(A) \to \wp(B)$.
Aanwijzing. Geef een definitie van de gezochte bijectie $\varphi : \wp(A) \to \wp(B)$ in de vorm: $\varphi(X) := \cdots$ (waarbij $X \in \wp(A)$ — je definitie zal vanzelfsprekend van de gegeven bijectie $f : A \to B$ gebruik moeten maken). (Er zijn feitelijk maar 1 of 2 kanonieke definities mogelijk!) Bewijs vervolgens dat "jouw" φ zowel in- als surjectief is.

92 ♣ Bewijs dat voor iedere verzameling A geldt: $\wp(A) \sim \{0, 1\}^A$.
Aanwijzing. Associeer met $X \subset A$ zijn *karakteristieke functie*, dat is de functie $\chi_X : A \to \{0, 1\}$ gedefinieerd door: $\chi_X(a) = 1$ d.e.s.d.a. $a \in X$. De afbeelding $X \mapsto \chi_X$ is de gezochte bijectie.

93 ♣ Onderstel dat de verzamelingen A en B gelijkmachtig zijn. Bewijs:

1. als A n elementen heeft, dan heeft B ook n elementen,
2. als A eindig is, dan is B ook eindig,
3. als A oneindig is, dan is B ook oneindig.

94 ♣ f is een functie. Bewijs, dat $f \sim Dom(f)$.

95 ♣ Gegeven zijn een verzameling A en een equivalentierelatie R op A. $V := A/R$ is de bijbehorende verdeling van A. Bewijs dat de verzameling van alle verdelingen van V gelijkmachtig is met de verzameling van alle equivalentierelaties Q op A waarvoor $R \subset Q$.

96 ♣♣ Gegeven is, dat $n, m \in \mathbb{N}$ en $n < m$. Bewijs, dat $\{0, \ldots, n-1\} \not\sim \{0, \ldots, m-1\}$.
Aanwijzing. Bewijs, met inductie naar m, dat voor alle m: $\forall n < m\ \{0, \ldots, n-1\} \not\sim \{0, \ldots, m-1\}$. Gebruik de bewijsmethode van Stelling 6.11.

97 ♣ Gegeven zijn $X \subset \mathbb{N}$ en $m \in \mathbb{N}$ zódat $\forall n \in X(n < m)$. Bewijs dat X eindig is.

Volgens Voorbeeld 6.10 is $\emptyset$ eindig en als A eindig is, en x is e.o.a. object, dan is $A \cup \{x\}$ eveneens eindig. In het Inductieprincipe van de volgende opgave komt tot uiting, dat zó alle eindige verzamelingen worden geproduceerd.

98 ♣♣ Bewijs het volgende inductie principe voor eindige verzamelingen (*Inductie "naar het aantal elementen" van zo'n eindige verzameling*):
Als E een eigenschap van verzamelingen is zódat
(i) $E(\emptyset)$,
en
(ii) voor iedere verzameling A en ieder ding $x \notin A$:
als $E(A)$ dan geldt ook $E(A \cup \{x\})$,
dan geldt E voor *iedere eindige* verzameling.
Aanwijzing. Pas volledige inductie toe op de eigenschap E' van getallen, gedefinieerd door: $E'(n) :\equiv \forall A[A \text{ heeft } n \text{ elementen } \Rightarrow E(A)]$.

99 ♣♣ Bewijs, dat iedere deelverzameling van een eindige verzameling eindig is.

100 ♣♣ Bewijs, dat de vereniging van twee eindige verzamelingen eindig is.

101 ♣♣ Onderstel, dat h een eindige injectie is met $Dom(h) \subset A$ en $Ran(h) \subset B$. Laat verder $A \sim B$. Bewijs dat een bijectie $f : A \rightarrow B$ bestaat zódat $f \supset h$. (Hoe zit dat, als niet wordt gegeven, dat h eindig is?)
Aanwijzing. Inductie naar het aantal elementen n van h. (Het geval $n = 1$ is Opgave 90.)

102 ♣♣ Bewijs, dat een *echt* deel van een *eindige* verzameling nooit gelijkmachtig is met die verzameling.
Aanwijzing. Inductie naar het aantal elementen van die verzameling.

103 ♣ Onderstel dat A en B eindige verzamelingen zijn en $f : A \rightarrow B$ een bijectie. Bewijs:

1. $(B - A) \sim (A - B)$,
2. er is een bijectie $g : A \cup B \rightarrow A \cup B$ zódat $f \subset g$.

Aanwijzing voor (i): inductie naar het aantal elementen van $A \cap B$.

104 ♣♣ Bewijs: een verzameling A is eindig d.e.s.d.a. aan de volgende conditie wordt voldaan door iedere collectie $E \subset \wp(A)$: als $\emptyset \in E$ en $\forall B \in E\, \forall a \in A\, (B \cup \{a\} \in E)$, dan geldt $A \in E$.

6.3 *Kombinatoriek

Als de meeste verzamelingentheorie "zachte" wiskunde is, dan is kombinatoriek dat gedeelte van de machtigheidstheorie waar de verzamelingentheorie op haar "hardst" wordt.

Hieronder volgen een aantal illustraties die allemaal draaien om de kloof die gaapt tussen *eindig* en *oneindig*.

De bewijzen zijn vaak van dien aard, dat uitschrijven via de bewijsregels van Hoofdstuk 2 het bewijs*idee* niet ten goede komt. Hoewel hier de logische plaats is voor de besproken onderwerpen, horen ze qua moeilijkheidsgraad eerder in Hoofdstuk 10.

6.3.1 Pigeon-hole Principes

105♣ Opgave. Bewijs: als I eindig is en iedere A_i $(i \in I)$ is eindig, dan is $\bigcup_{i \in I} A_i$ (Definitie 3.10 blz. 38) ook eindig.
Aanwijzing. Inductie naar het aantal elementen van I.

Een *pigeon-hole principe* heeft de vorm van de volgende observatie: als er "veel" duiven zitten in een duiventil met "weinig" vluchtgaten, dan zitten er "veel" achter één en hetzelfde gat. Opgave 105 kan worden geherformuleerd als het volgende eindig/oneindig pigeon-hole principe voor verdelingen (Definitie 4.9 blz. 47):

> Iedere verdeling van een oneindige verzameling in eindig veel componenten heeft minstens één oneindige component.

Een equivalente formulering die gebruik maakt van de functie-vermomming van een verdeling is de volgende. Hierin is A de verzameling duiven en f geeft de verdeling van duiven over vluchtgaten. Zie Opgave 69 (blz. 60) voor hoe een functie als verdeling kan worden opgevat.

> Als A oneindig is, I eindig, en $f : A \to I$,
> dan bestaan een element $i \in I$ en een oneindige deelverzameling $H \subset A$ zódat voor alle $a \in H$, $f(a) = i$.

Verderop kom je het aftelbaar/overaftelbaar pigeon-hole principe tegen (Opgave 162 blz. 107). Er zijn ook pigeon-hole principes die uitsluitend over *eindige* verzamelingen gaan. Bijvoorbeeld: als er 5 duiven zitten achter 2 gaten, dan zitten er (minstens) 3 achter één gat. Dit lijkt flauw, maar heeft toch een amusante toepassing in Opgave 107.

Opgaven

106♣ (Halmos) Op een bijeenkomst van 100 personen zijn —hoe kan het anders— sommigen kennissen van elkaar, terwijl anderen elkaar niet kennen. Beargumenteer, door een geschikt pigeon-hole principe te gebruiken, dat *tenminste twee* personen hetzelfde *aantal* kennissen (*niet*: dezelfde kenniseen) onder de aanwezigen hebben.

107♣♣ Geef een, liefst elegant, bewijs voor de volgende bewering: iedere groep van 6 personen heeft een sub-groep van 3 waarin hetzij iedereen, hetzij niemand, elkaar kent.
Aanwijzing. Het bewijs van Ramsey's stelling 6.12 volgt een methode waarmee deze opgave (ook) kan worden opgelost.
Geef een voorbeeld waaruit blijkt dat niet iedere groep van 5 personen een sub-groep van 3 heeft waarin hetzij iedereen, hetzij niemand elkaar kent.

108♣ Als $\{\varphi_i \mid i \in I\}$ een eindige verzameling formules is, dan staat $\bigvee_{i \in I} \varphi_i$ voor de disjunctie van de formules φ_i en $\bigwedge_{i \in I} \varphi_i$ voor hun conjunctie.

1. $A_1, \ldots, A_5$ zijn propositie variabelen. D is de verzameling van 3-elementige deelverzamelingen van $\{1, 2, 3, 4, 5\}$. (D heeft 10 elementen.)
   Toon aan, dat de formule $\bigvee_{X \in D}[\bigwedge_{i \in X} A_i \vee \bigwedge_{i \in X} \neg A_i]$ een logische geldigheid is in de propositiecalculus.

2. Gegeven zijn twintig propositie variabelen A_{ik} $(0 \leqslant i < 5,\ 0 \leqslant k < 4)$.
   Bewijs dat $\bigwedge_{i<5} \bigvee_{k<4} A_{ik} \longrightarrow \bigvee_{k<4} \bigvee_{i<j<5} (A_{ik} \leftrightarrow A_{jk})$ een logische geldigheid is in de propositiecalculus.
3. Gegeven zijn $m \times n$ propositie variabelen A_{ij} $(0 \leqslant i < n,\ 0 \leqslant j < m)$. D is de verzameling van alle p-elementige deelverzamelingen van $\{0, \ldots, m-1\}$. Bewijs dat de twee volgende beweringen equivalent zijn:
   (a) iedere verdeling van een m-elementige verzameling in n componenten heeft een component met tenminste p elementen,
   (b) de formule $\Phi(m,n,p) := \bigwedge_{i<m} \bigvee_{j<n} A_{ij} \longrightarrow \bigvee_{X \in D} \bigvee_{j<n} \bigwedge_{i \in X} A_{ij}$ is propositioneel logisch geldig.

6.3.2 Ramsey-stellingen

Het resultaat van Opgave 107 is een zgn. (eindige) *Ramsey*-stelling. Een oneindige versie hiervan zegt, dat iedere *oneindige* groep van mensen een *oneindige* subgroep heeft waarin hetzij iedereen, hetzij niemand elkaar kent. Hier is een kleine generalisatie. (De sociologische toepassing volgt hieruit door de elementen van $A = Dom(f)$ te vervangen door mensen, en voor $Ran(f)$ de 2-elementige verzameling $\{$*kennen, niet-kennen*$\}$ te nemen.) Door iteratie kan dit nog verder worden gegeneraliseerd naar verdelingen van 3, 4, ... -elementige deelverzamelingen (zie Opgave 110).

6.12 Ramsey's Stelling. *Als f een verdeling is van de twee-elementige deelverzamelingen van een oneindige verzameling A in eindig veel componenten, dan bestaat een oneindige verzameling $H \subset A$ waarvan alle twee-elementige deelverzamelingen in dezelfde component zitten.*

Bewijs. Het bewijs begint met de constructie van twee oneindige rijen: een rij $a_0, a_1, a_2, \ldots \in A$, en een dalende rij $A_0 \supset A_1 \supset A_2 \supset \cdots$ deelverzamelingen van A. (Als de constructie klaar is wordt de tweede rij, die alleen t.b.v. de constructie van belang is, weggegooid.)
Om te beginnen neem je $A_0 := A$, en $a_0 \in A_0$ willekeurig.
Definieer een verdeling van $A_0 - \{a_0\}$ door $a \longmapsto f(\{a_0, a\})$. Volgens het eindig/oneindig pigeon-hole principe is er een oneindige deelverzameling $A_1 \subset A_0 - \{a_0\}$ van elementen met hetzelfde beeld. Neem voor a_1 een willekeurig element van A_1.
Definieer nu een verdeling van $A_1 - \{a_1\}$ door $a \longmapsto f(\{a_1, a\})$. Weer is er een oneindige deelverzameling $A_2 \subset A_1 - \{a_1\}$ van elementen met hetzelfde beeld. Ga zo door.
Merk op: na afloop van deze constructie geldt voor de verkregen elementen $a_0, a_1, a_2, \ldots$ dat, als $i < j < k$, dan geldt (omdat $a_j, a_k \in A_{i+1}$) $f(\{a_i, a_j\}) = f(\{a_i, a_k\})$. D.w.z.: de f-waarde hangt alleen van het element a_i met de *kleinste* index af.
Definieer een laatste verdeling van $\{a_i \mid i \in \mathbb{N}\}$ door $a_i \longmapsto f(\{a_i, a_{i+1}\})$.
Het pigeon-hole principe levert nu een oneindige verzameling $H \subset A$ met de gewenste eigenschap: als $a_i, a_j, a_k, a_l \in H$, $i < j$ en $k < l$, dan geldt immers dat $f(\{a_i, a_j\}) = f(\{a_i, a_{i+1}\}) = f(\{a_k, a_{k+1}\}) = f(\{a_k, a_l\})$. ⊣

Opgaven

109 ♣ Onderstel, dat $r_0, r_1, r_2, \ldots \in \mathbb{R}$ een rij onderling verschillende reële getallen is. Bewijs: er zijn $n_0 < n_1 < n_2 < \cdots$ zódat hetzij $r_{n_0} < r_{n_1} < r_{n_2} < \cdots$, hetzij $r_{n_0} > r_{n_1} > r_{n_2} > \cdots$.

110 ♣ Onderstel dat f een verdeling is van de *drie*-elementige deelverzamelingen van een oneindige verzameling A in eindig veel componenten. Bewijs: er is een oneindige verzameling $H \subset A$ zódat alle drie-elementige delen van H in dezelfde component zitten.

111 ♣ Bewijs: bij iedere verdeling van de 2-elementige delen van een 32-elementige verzameling in 2 componenten bestaat een 4-elementig deel van die verzameling waarvan alle 2-elementige delen in dezelfde component zitten.
Aanwijzing. Gebruik de methode van het bewijs van Stelling 6.12.

112 ♣ Bewijs: bij alle $n \in \mathbb{N}$ bestaat een $m \in \mathbb{N}$ zódat bij iedere verdeling van de 2-elementige delen van een m-elementige verzameling in 2 componenten een n-elementig deel van die verzameling bestaat waarvan alle 2-elementige delen in dezelfde component zitten.
Je hebt gezien, dat $m = 6$ ($m = 32$) voldoet als $n = 3$ (resp., $n = 4$). Bepaal zo'n m voor het geval, dat $n = 5$.

6.3.3 Bomen

6.13 Bomen en Paden.

1. Een *pad* in een struktuur $\mathcal{B} = (B, \prec)$ is een eindige of oneindige rij elementen $b_0 \prec b_1 \prec b_2 \prec \cdots$

   Een eindig pad $b_0 \prec \cdots \prec b_n$ ($n \geqslant 0$) is een pad *van* b_0 *naar* b_n, gaat *door* $b_0, \ldots, b_n$, en heeft *lengte* $n + 1$.

2. Een *boom* is een struktuur $\mathcal{B} = (B, \prec, w)$, $\prec$ een relatie op B, $w \in B$, waarin voor ieder element $b \neq w$ precies één pad $b_0 = w \prec b_1 \prec b_2 \prec \cdots \prec b_n = b$ bestaat van w naar b.
   Het getal n heet de *hoogte* van b in $\mathcal{B}$. (De hoogte van w is dus 0.)

   De *hoogte* van een boom is de maximale lengte die een pad door de boom kan hebben. Bestaat zo'n maximum niet, dan is de hoogte *oneindig.*

3. Als $\mathcal{B} = (B, \prec, w)$ een boom is en $b \in B$, dan bepaalt b een *subboom* van $\mathcal{B}$, t.w. de boom $\mathcal{B}_b = (B_b, \prec, b)$ waarin B_b de verzameling van elementen van B is waarheen een pad van b leidt. (Dus, $\mathcal{B}_w = \mathcal{B}$.)

4. Een boom $\mathcal{B} = (B, \prec, w)$ is *eindig vertakkend* als bij iedere $b \in B$ hoogstens eindig veel $c \in B$ bestaan waarvoor $b \prec c$.

Zie Sectie 9.5 (blz. 127) voor een alternatieve definitie van bomen.
Van eindige bomen kun je plaatjes tekenen. Zie blzz. 79 en 85.

6.14 Terminologie. Boom-terminologie is een eigenaardige ratjetoe. Elementen van een boom heten *knopen*. In een boom $\mathcal{B} = (B, \prec, w)$ heet w de *wortel*; als $a \prec b$ geldt dan heet b *kind* van a, en — je raadt het — a *ouder* van b; kinderen van dezelfde ouder heten *broers*, en verdere genealogische terminologie spreekt voor zich.
Kinderloze elementen van $\mathcal{B}$ heten *toppen* of *bladeren*.
Een ouder kan verschillende kinderen hebben, maar ieder kind heeft precies één ouder. De wortel van een boom is de enige wees (ouderloze knoop).
Voor $b \in B$ geldt, dat b de wortel is van de subboom $\mathcal{B}_b$ van $\mathcal{B}$.

Voorbeelden. *Stambomen.* Familieverbanden leiden op twee natuurlijke manieren tot bomen. Onderstel dat de verzameling B bestaat uit w en al z'n ('r) nakomelingen. Het letterlijk nemen van $a \prec b$ als: b is kind van a, levert de *stamboom* $(B, \prec, w)$ van w. Maar, je kunt zo'n boom ook de andere kant op laten groeien: laat B nu bestaan uit w en al z'n voorouders. Definiëren van $a \lessdot b$ als: a is *kind* van b levert ook een boom $(B, \lessdot, w)$. Beide typen bomen zijn eindig vertakkend. In de tweede soort boom heeft een "ouder" (feitelijk: *kind*) altijd precies twee "kinderen" (feitelijk: *ouders*). Deze voorbeelden illustreren goed de relativiteit van de begrippen ouder en kind, en het feit dat het in eenzelfde situatie nuttig kan zijn bomen te hebben die verschillende kanten uit groeien.
Directory-bomen en Unix-commandos. Heb je een *account* in een computernetwerk, dan is een voorbeeld van een (eindig vertakkende) boom de *directory-struktuur* die aan je *home-directory* (de wortel van deze boom) hangt in het computersysteem; dit is een subboom van de directory-struktuur bij de wortel-directory `root` ofwel `/`. Bladeren van deze boom zijn (normaal gesproken) files. Verschillende *unix-commandos* stellen je in staat door deze boom te klimmen en haar naar wens te modificeren. Bijvoorbeeld, het commando `cd directoryname` verplaatst je van de ouder van de directory `directoryname` naar de directory `directoryname`, en `cd ../` verplaatst je van een kind-directory naar zijn ouder-directory. Het Unix-commando `pwd` toont je het (unieke!) pad van `root` naar de directory waarin je je bevindt, `ls` geeft je antwoord op de vraag, wat de kinderen (zowel files als directories) van deze directory zijn, en het commando `which filename` toont je het pad van `root` naar `filename`. Er zijn ook commandos waarmee je de boomstruktuur kunt wijzigen. Bijvoorbeeld, `rm filename` verwijdert het blad `filename`.

Over eindig vertakkende bomen gaat het volgende, klassieke, resultaat.

6.15 König's Lemma. *Iedere oneindige, eindig vertakkende boom heeft een oneindig pad.*

Bewijs. Laat $\mathcal{B} = (B, \prec, w)$ de betreffende boom zijn. De truc is om het pad zó te leggen, dat door iedere knoop van het pad oneindig veel eindige paden gaan. Het pad begint bij de wortel w. Merk op dat w zelf de gewenste eigenschap heeft: omdat $\mathcal{B}$ oneindig is, gaan er oneindig veel eindige paden door w: naar iedere knoop van $\mathcal{B}$ één. Ieder pad van w naar een knoop $c \neq w$ van B gaat

door één van de *eindig veel* kinderen $b \succ w$ van w. Eindig/oneindig pigeon-hole principe: *oneindig* veel paden gaan langs één zo'n kind $b \succ w$. Neem een dergelijk kind als tweede knoop van het te construeren oneindige pad. Iedere volgende knoop van het pad wordt netzo gevonden met een toepassing van het eindig/oneindig pigeon-hole principe. ⊣

Smullyan's balspel. *Smullyan's balspel* speel je in je eentje. Hierbij heb je een doos met eindig veel ballen nodig. Iedere bal is gemerkt met een natuurlijk getal. Naast de doos bevindt zich een zak met netzoveel (zonodig: oneindig veel) ballen als je maar wilt, en met ieder gewenst nummer gemerkt. Voer de volgende handeling uit.

> Kies een willekeurige bal in de doos. De bal draagt een nummer n. Gooi deze bal uit de doos. Kies eindig veel ballen uit de zak onder de restrictie dat ze allemaal nummers $< n$ moeten dragen. Leg deze ballen in de doos.

Het spel bestaat uit de voortdurende herhaling (zo lang als mogelijk is) van deze handeling.

6.16 Stelling van Smullyan. *Hoe je Smullyan's balspel ook speelt, onvermijdelijk komt er een moment dat je doos leeg is.*

Je laatste handeling kan dus niet anders zijn geweest dan het weggooien van een — onvervangbare! — bal met nummer 0. M.a.w.: de relatie tussen opvolgende dozen is *gefundeerd* (Definitie 6.5 blz. 69). Hier volgt een bewijs voor Stelling 6.16 via König's Lemma. Voor een ander bewijs, zie Opgave 113.

Bewijs. Gezien de spelregels mag je wel onderstellen dat jouw doos na één handeling is verkregen uit een eerdere doos die maar één bal bevat (met een voldoend groot nummer). Deze bal beschouw je als de wortel w van een boom $\mathcal{B} = (B, \prec, w)$; B is de verzameling van alle ballen die op zeker moment in de doos zijn (geweest); $b \prec c$ geldt per definitie als c één van de ballen is die de bal b heeft vervangen. $\mathcal{B}$ is dus eindig vertakkend. Als je doos nooit leeg raakt dan betekent dat, dat $\mathcal{B}$ oneindig is: "uiteindelijk" heb je immers oneindig veel ballen in de doos gedaan. (Eruit trouwens óók.) Pas König's lemma toe op deze boom. De nummers van de ballen van het oneindige pad vormen nu een oneindige dalende rij natuurlijke getallen, in strijd met het feit dat $(\mathbb{N}, <)$ gefundeerd is (Opgave 86). ⊣

Hercules en de Hydra. Hier is een, nog onwaarschijnlijker, generalisatie van Smullyan's balspel: het *gevecht tussen Hercules en de Hydra.*

Een *Hydra* is domweg een eindige boom $\mathcal{H} = (H, \prec, w)$. De *koppen* van een Hydra zijn de bladeren van de boom die de Hydra ook is.

Het gevecht tussen Hercules en de Hydra speelt zich af in een aantal (eindig of oneindig veel) *ronden.* In iedere ronde hakt Hercules de Hydra een kop af, en de Hydra kan hierop reageren door het laten aangroeien van nieuwe tentakels. De détails zijn als volgt.

De Hydra bij aanvang van het gevecht is de boom $\mathcal{H}^0 = \mathcal{H}$. Na de eerste ronde (onthoofding, plus eventuele regeneratie) is zijn gedaante getransformeerd in $\mathcal{H}^1$, enz. Onderstel dat n gevechtsronden zijn voltrokken. In de $(n+1)$-ste gevechtsronde hakt Hercules de Hydra, die dan de gedaante $\mathcal{H}^n$ heeft, de kop k_n af. De Hydra heeft nu de volgende opties.

(1) De Hydra ondergaat z'n onthoofding gelaten, doet niets, en het gevecht gaat naar een volgende ronde.

(2) De Hydra kiest een knoop b_n in $\mathcal{H}^n$ die de ouder of een voorouder is van k_n.

Laat a_n verder de ouder zijn van b_n in $\mathcal{H}^n$.

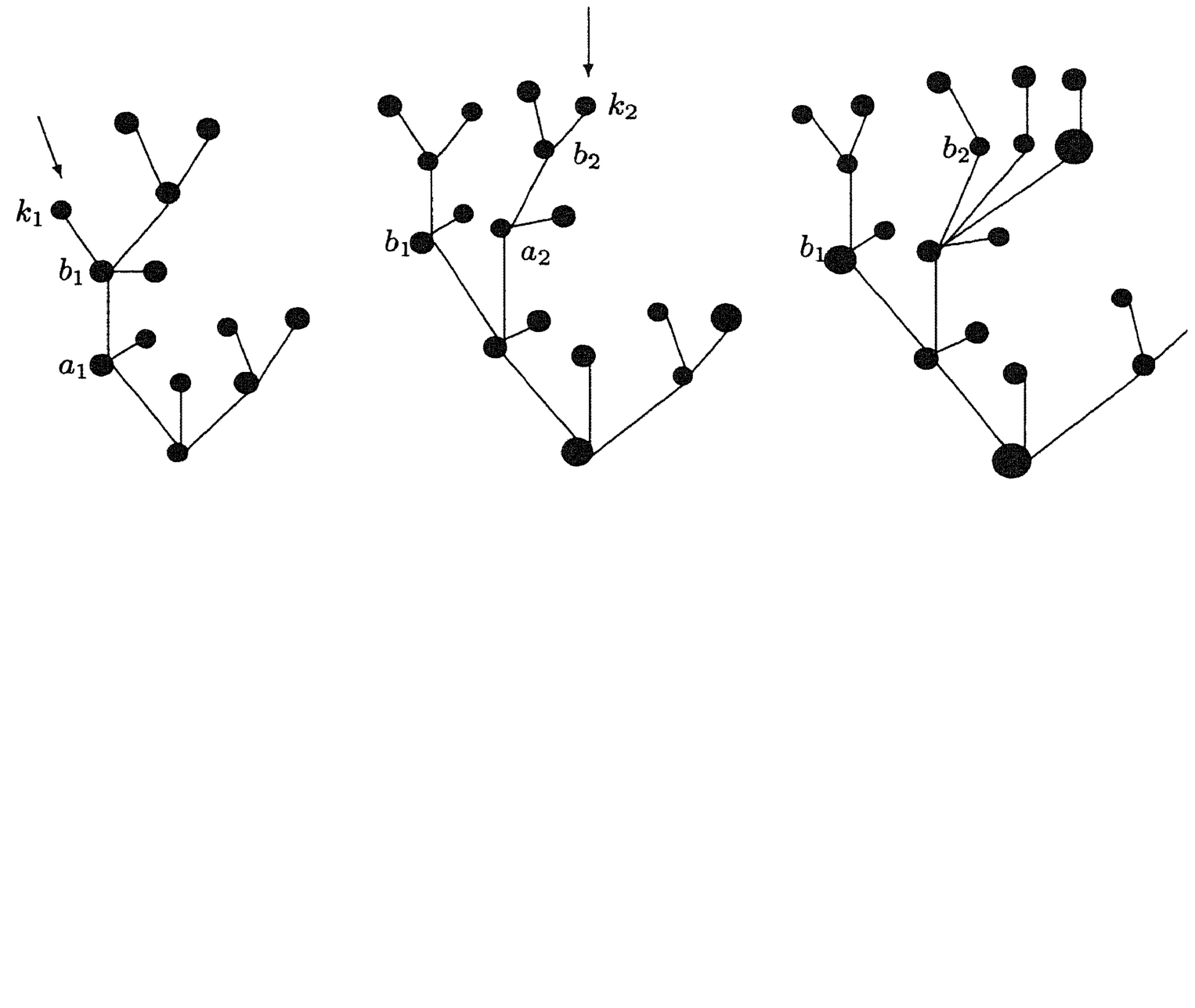
Het afhakken van k_n heeft de subboom H_{b_n} (met wortel b_n) van $\mathcal{H}^n$ getransformeerd in de nu onthoofde subboom $H^-_{b_n}$.

De Hydra regenereert, naast $H^-_{b_n}$, een willekeurig (maar eindig) aantal kopieën van $H^-_{b_n}$ vanuit de knoop a_n.

Merk op dat optie (2) alleen openstaat voor de Hydra in het geval dat k_n niet zijn wortel is (anders valt b_n niet te kiezen) en ook geen kind van de wortel (anders heeft b_n geen ouder a_n).

In het geval dat k_n de wortel is van $\mathcal{H}^n$ dan bestaat de Hydra kennelijk nog maar uit één knoop (anders kon k_n niet tegelijk een kop zijn), en dan is de Hydra door de onthoofding *vernietigd*.

Zie het plaatje voor twee eerste mogelijke ronden, waarbij de Hydra telkens de ouder van de afgehakte kop kiest als wortel van de te regenereren onthoofde subboom. Bij de eerste transitie wordt één gemutileerde subboom geregenereerd, bij de tweede transitie twee. De pijltjes wijzen de koppen aan die worden afgehakt.



Dat dit een *generalisatie* is van Smullyan's balspel wordt duidelijk als je bedenkt, dat een natuurlijk getal n kan worden *gekodeerd* als een eindige boom van hoogte $\leqslant 2$ met $n+1$ knopen: een wortel met n bladeren. Een doos met m ballen, gemerkt met de nummers $b_1, \ldots b_m$, kan dus worden voorgesteld als een eindige boom (Hydra) van hoogte $\leqslant 3$ waarvan de wortel m kinderen heeft die op hun beurt wortels zijn van subbomen die $b_1, \ldots b_m$ koderen. Het vervangen van de bal met nummer b_1 door $n+1$ ballen met nummer $b_1 - 1$ komt dan neer op: (i) het verwijderen van een blad van de boom-kode voor b_1, en (ii) het aanbrengen van n boom-kodes voor $b_1 - 1$ boven de wortel van de boom.

Een klein experiment doet al gauw het vermoeden ontstaan, dat Hercules voor een onmogelijke opgave staat, omdat het aantal tentakels van de Hydra, als gevolg van gevechtsronden van type (2), onrustbarend toeneemt. Maar:

6.17 *Stelling. *Hercules kan niet vermijden dat hij de Hydra op den duur vernietigt.*

Bewijs. Inductie naar de hoogte m (de lengte van het langste pad $h_0 = w \prec \cdots \prec h_{m-1}$) van de Hydra.
$m = 1$. De Hydra bestaat alleen uit een wortel en wordt vernietigd in de eerste ronde.
Je zou de inductie ook bij $m = 2$ kunnen laten beginnen. Dan is de Hydra dus kode van een getal k en alle k koppen zijn kind van de wortel. Omdat het afhakken van een kind van de wortel geen regeneratie tot gevolg heeft, is de Hydra na $k+1$ ronden vernietigd.
Ten overvloede nog het geval $m = 3$. Dan stelt de Hydra een Smullyanse doos voor en het argument heb je gezien.

$m > 1$. Dit verschilt niet wezenlijk van het Smullyan-argument.

Definieer $\mathcal{B}$ als de superboom waarvan de knopen zelf weer bomen zijn, te weten: alle bomen H_b die subboom zijn van een $\mathcal{H}^n$, waarbij de wortel b van H_b kind is van de wortel van $\mathcal{H}^n$. (Als in het gevecht kinderen van een wortel worden afgehakt — dat gebeurt — dan is het, t.b.v. de uniformiteit van het argument, handig om aan te nemen dat ook "lege bomen" element kunnen zijn van $\mathcal{B}$. Zie er maar even vanaf dat, volgens Definitie 6.13, bomen *nooit* leeg zijn.)

De ouder/kind-relatie van deze superboom $\mathcal{B}$ wordt als volgt gedefinieerd. (Voor een goed begrip moet je plaatjes tekenen!)

> H_c is *kind* van H_b d.e.s.d.a.:
>
> er is een $n \in \mathbb{N}$ zódat H_b subboom is van $\mathcal{H}^n$, H_c subboom is van $\mathcal{H}^{n+1}$,
>
> Hercules in de $(n+1)$-ste ronde $\mathcal{H}^n$ een kop k_n afhakt die ook een kop is van H_b,
>
> en zódat geldt (waarbij H_b^- het resultaat van H_b is na deze onthoofding):

(IA) ófwel de Hydra doet niets (geval (1)), en H_c is H_b^-,
ófwel de Hydra reageert wel (geval (2)) en:

(IB) a_n is de wortel van $\mathcal{H}^n$, $b_n = b$, en H_c is H_b^- of één van de geregenereerde kopieën van H_b^-, of

(II) a_n is een knoop van H_b en H_c is de subboom van $\mathcal{H}^{n+1}$ met wortel $c = b$ (die dus het resultaat is van het effect op H_b van de totale n-de ronde: onthoofding plus regeneratie).

Merk op: alle bomen in $\mathcal{B}$ hebben hoogte $< m$. Verder is $\mathcal{B}$ duidelijk eindig vertakkend; alleen geval (IB) is verantwoordelijk voor splitsingen in $\mathcal{B}$. (Het probleem dat $\mathcal{B}$ misschien een wortel mist kan, net als bij het Smullyaanse geval, worden opgelost door het tijdelijk toevoegen van een wortel. Het resultaat blijft eindig vertakkend: de kinderen van die nieuwe wortel zijn juist alle subbomen van de Hydra $\mathcal{H} = \mathcal{H}^0$ bij aanvang van het gevecht.)

In het geval dat het gevecht eeuwig voortduurt is $\mathcal{B}$ oneindig en levert König's lemma een oneindig pad $H_0, H_1, H_2, \ldots$, zódat, voor alle i, H_{i+1} kind is van H_i in de zin ((IA), (IB) of (II)) van $\mathcal{B}$.

Maar zo'n pad is kennelijk niets anders dan een eeuwig durend *nieuw* gevecht dat ditmaal begint met een boom (Hydra) H_0 van hoogte $< m$, kijk maar: transities (IA) en (IB) in het pad zijn niets anders dan gevechtsronden van type (1), en een transitie (II) in het pad is niets anders dan een gevechtsronde van type (2).

De inductiehypothese zorgt nu voor afronding van het argument. ⊣

Opgaven

113 ♣ Completeer de volgende bewijsschets voor Stelling 6.16.
Onderstel, dat n het grootste nummer is op enige bal in de doos. Dat de doos na eindig veel ronden leeg is bewijs je met sterke inductie naar n.
De inductiehypothese ziet er dus als volgt uit: een spel dat begint met een doos waarin het grootste voorkomende nummer $< n$ is, eindigt onvermijdelijk met een lege doos.
Laat m het aantal ballen in de doos zijn, dat dit grootste nummer n draagt. Pas nu *opnieuw* sterke inductie toe, nu naar m.
Je krijgt dan een tweede inductiehypothese: een spel dat begint met een doos met minder dan m grootste nummers n eindigt met een lege doos.
Tenslotte moet je laten zien dat een spel dat met m grootste nummers n begint, met de lege doos eindigt. Een spel dat niet zo eindigt sleept zich eeuwig voort. Onderscheid of in zo'n spel een bal met nummer n wordt vervangen (op dat moment is de tweede inductiehypothese van toepassing), of niet (dan blijven de m ballen met nummer n onaangeroerd; laat die weg en pas de eerste inductiehypothese toe).

114 ♣ Onderstel, dat f een verdeling is van de twee-elementige deelverzamelingen van een oneindige verzameling A in eindig veel componenten. Ramsey's Stelling 6.12 zegt, dat een oneindige verzameling $H \subset A$ en $i \in Ran(f)$ bestaan zódat voor alle $a, b \in H$ met $a \neq b$: $f(\{a, b\}) = i$. Het bewijs bestaat uit twee delen; het eerste deel produceert een oneindige rij $a_0, a_1, a_2, \ldots \in A$ zódat, voor $i < j < k$, $f(\{a_i, a_j\}) = f(\{a_i, a_k\})$. D.w.z.: de f-waarde hangt alleen van het *eerste* element af. Een dergelijke rij kan

ook worden vekregen door König's Lemma toe te passen op een geschikte boom $\mathcal{B} = (B, \prec, w)$. Deze boom wordt, tegelijk met een functie h op B, als volgt gedefinieerd.
1. $w := A$, $h(w)$ is een willekeurig element van w.
2. Onderstel, dat $X \in B$, $X \subset A$, en $h(X) \in X$. Definieer een verdeling van $X - \{h(X)\}$ door $x \longmapsto f(\{h(X), x\})$. De *kinderen* van X in $\mathcal{B}$ zijn de *componenten* van deze verdeling. Voor iedere dergelijke component $K \subset X - \{h(X)\}$ is $h(K) \in K$ een willekeurig element van K.
Ga de détails na.

115 ♣♣ Laat $\sim$ een symmetrische relatie zijn op een verzameling A zódat bij iedere $a, b \in A$ precies één $\sim$-pad $a_0 = a \sim a_1 \sim a_2 \sim \cdots \sim a_n = b$ bestaat $(n = 0, 1, 2, \ldots)$. Laat $w \in A$. Toon aan dat er precies één relatie $\prec$ bestaat zódat voor alle $a, b \in A$: $a \prec b \vee b \prec a \Leftrightarrow a \sim b$, en zódat $(A, \prec, w)$ een boom is met wortel w.

6.3.4 Wel-quasi-ordeningen

6.18 QO, goed, slecht, WQO.

1. Een relatie op een verzameling Q heet een *quasi-ordening* (afkorting: QO) op Q als hij reflexief is op Q en transitief.

2. Laat $\leqslant$ een relatie zijn op Q. Een oneindige rij $q_0, q_1, q_2, \ldots \in Q$ heet *goed* als $i, j \in \mathbb{N}$ bestaan, $i < j$, zódat $q_i \leqslant q_j$; een rij die niet goed is heet *slecht*.

3. Een *wel-quasi-ordening* (afkorting: WQO) is een QO waarin alle oneindige rijen goed zijn.

Vergelijk dit met Definitie 9.2 (blz. 119). Het verschil tussen een quasi-ordening en een reflexieve partiële ordening is dat de laatste ook nog antisymmetrisch is. Voor wat volgt is dat verschil nauwelijks van belang. Zie eventueel Opgave 208 blz. 122.

Zie de opgaven voor relaties tussen de noties *quasi-ordening* en *gefundeerdheid*. Iedere QO op een eindige verzameling is WQO. Iedere welordening (zie Sectie 10.5) is WQO.

6.19 Lemma. *In een WQO heeft iedere oneindige rij $q_0, q_1, q_2, \ldots$ een oneindige stijgende deelrij $q_{i_0} \leqslant q_{i_1} \leqslant q_{i_2} \leqslant \cdots$ $(i_0 < i_1 < i_2 < \cdots)$.*

Eerste bewijs. Verdeel de paren $\{q_i, q_j\}$ $(i < j)$ in twee componenten, al naar gelang $q_i \leqslant q_j$ of niet. Volgens Ramsey's stelling bestaan $q_{i_0}, q_{i_1}, q_{i_2}, \ldots$ $(i_0 < i_1 < i_2 < \cdots)$ zódat hetzij voor alle j, k met $j < k$: $q_{i_j} \leqslant q_{i_k}$, hetzij voor alle j, k met $j < k$: $q_{i_j} \not\leqslant q_{i_k}$. Maar het laatste wordt uitgesloten door het feit dat je met een WQO te maken hebt. ⊣

Tweede bewijs. Noem q_i *terminaal* als geen $j > i$ bestaat met $q_i \leqslant q_j$. Als het aantal terminale elementen in de rij oneindig is, dan vormen ze een slechte rij. Dus is hun aantal eindig. Kies q_{i_0} na het laatste terminale element. Omdat q_{i_0} niet terminaal is bestaat q_{i_1} $(i_1 > i_0)$ zódat $q_{i_0} \leqslant q_{i_1}$. Etc. ⊣

Onderstel, dat Q en Q' WQO's zijn. Je kunt een QO op de productverzameling $Q \times Q'$ definiëren door

$$(q, q') \leqslant (r, r') \;:\equiv\; q \leqslant r \;\wedge\; q' \leqslant r'.$$

(De drie optredens van $\leqslant$ staan voor drie verschillende relaties!)

Een toepassing van het vorige lemma is het volgende product lemma.

6.20 Product Lemma. *Ieder product van WQO's is WQO.*

Bewijs. Onderstel, dat Q en Q' WQO zijn. Laat $(q_0, q_0'), (q_1, q_1'), (q_2, q_2'), \ldots$ een rij zijn in $Q \times Q'$. Kies (Lemma 6.19) een stijgende deelrij $q_{n_0} \leqslant q_{n_1} \leqslant q_{n_2} \leqslant \cdots$ van de rij van eerste coördinaten $(n_0 < n_1 < n_2 < \cdots)$. De bijbehorende rij van tweede coördinaten $q'_{n_0}, q'_{n_1}, q'_{n_2}, \ldots$ is goed. Bijvoorbeeld, $q'_{n_i} \leqslant q'_{n_j}$, $i < j$. Dus, $(q_{n_i}, q'_{n_i}) \leqslant (q_{n_j}, q'_{n_j})$. ⊣

Onderstel, dat Q een QO is. Op de collectie van deelverzamelingen van Q kun je op de volgende manier een QO definiëren:

$$A \leqslant B \;:\equiv\; \text{er is een injectie } f : A \to B \text{ zódat } \forall q \in A\,(q \leqslant f(q)).$$

Het volgende lemma zegt dat deze relatie WQO is op de *eindige* deelverzamelingen van Q in het geval dat Q zelf WQO is.

6.21 Lemma. *De collectie van eindige deelverzamelingen van een WQO is WQO.*

Bewijs. Onderstel, dat Q WQO is, maar zijn collectie van eindige deelverzamelingen niet. Dan is er een slechte rij van eindige deelverzamelingen.

1. Kijk naar alle eindige delen van Q die *eerste element* zijn van zo'n slechte rij. Kies hieruit een verzameling A_0 die een minimaal aantal elementen heeft.
Er zijn slechte rijen die met A_0 beginnen. Kies een verzameling A_1 met een minimaal aantal elementen die optreedt als tweede element van zo'n slechte rij die begint met A_0.
Er zijn slechte rijen waarvan A_0 en A_1 de eerste twee elementen zijn. Kies nu een verzameling A_2 met een minimaal aantal elementen die optreedt als derde element van zo'n slechte rij die begint met A_0, A_1.
Enz.
Het resultaat is een oneindige rij $A_0, A_1, A_2, \ldots$ De rij is slecht, want ieder beginstuk ervan is beginstuk van een slechte rij.
2. Kies, voor iedere $i \in \mathbb{N}$, een element $q_i \in A_i$. (N.B.: $A_i \neq \emptyset$, want $\emptyset \leqslant A_{i+1}$!)
$B_i := A_i - \{q_i\}$.
3. Volgens Lemma 6.19 heeft de rij $q_0, q_1, q_2, \ldots$ een oneindige deelrij $q_{i_0} \leqslant q_{i_1} \leqslant q_{i_2} \leqslant \cdots$.
Bewering. De corresponderende rij $B_{i_0}, B_{i_1}, B_{i_2}, \ldots$ is goed.
Bewijs. Kijk anders naar de rij

$$A_0, \ldots, A_{i_0-1}, B_{i_0}, B_{i_1}, B_{i_2}, \ldots$$

Deze rij is dan ook slecht: als $A_j \leqslant B_{i_k}$, dan geldt immers ook dat $A_j \leqslant A_{i_k}$. Maar dit is in strijd met de keuze van A_{i_0}.
4. Bijvoorbeeld, $B_{i_j} \leqslant B_{i_k}$, $j < k$. Maar dan geldt ook $A_{i_j} \leqslant A_{i_k}$. ⊣

6.22 QO van bomen. Een *inbedding* tussen bomen $\mathcal{B} = (B, \prec, w)$ en $\mathcal{D} = (D, \prec', w')$ is een injectie $h : B \to D$ die aan de volgende eis voldoet:

> als $b_1, b_2 \in B$ *verschillende* kinderen zijn van $a \in B$, dan zijn er *verschillende* kinderen d_1, d_2 van $h(a) \in D$ zódat $h(b_1) \in D_{d_1}$ en $h(b_2) \in D_{d_2}$.

(Zie Definitie 6.13: D_d is de verzameling van knopen waarheen een pad van d leidt.) Anders gezegd: $h(a)$ is het *enige* element dat de paden van $h(a)$ naar $h(b_1)$ en van $h(a)$ naar $h(b_2)$ in $\mathcal{D}$ (die heel goed langer kunnen zijn dan de lengte-1 paden van a naar b_1 resp., b_2) gemeen hebben.
Schrijf $\mathcal{B} \leqslant \mathcal{D}$ ingeval er een inbedding is van $\mathcal{B}$ in $\mathcal{D}$.

Dat de inbedbaarheidsrelatie $\leqslant$ op de collectie van (eindige) bomen een QO is, is duidelijk. Het doel van de rest van deze sectie is een bewijs voor de volgende stelling.

6.23 Stelling van Kruskal. *De collectie van eindige bomen is WQO onder de inbedbaarheidsrelatie.*

Eerst krijg je in 6.24 uitgelegd hoe bomen ook *van boven naar beneden* ("top-down") kunnen groeien. Het nut hiervan is dat dit speciale groeiproces wordt gevolgd in het bewijs van Stelling 6.23 (feitelijk ook al in dat voor Stelling 6.16), en bovendien wordt het ook gebruikt in de formele definitie van de notie van een *afleiding* (Definitie 7.1 blz. 91).

6.24 Top-down Bomen.

(0) *Voor ieder ding w is de struktuur $(\{w\}, \emptyset, w)$ een eindige, zgn. rudimentaire, top-down boom.*

De notatie voor deze rudimentaire boom is kortweg w. In zo'n boom, die hoogte 1 heeft, is de knoop w zowel wortel als blad.

($\sum$) *Als $\{\mathcal{B}_i \mid i \in I\}$ ($\mathcal{B}_i = (B_i, \prec_i, w_i)$) een niet-lege verzameling van twee aan twee disjuncte top-down bomen is en $w \notin \bigcup_i B_i$, dan is de struktuur*

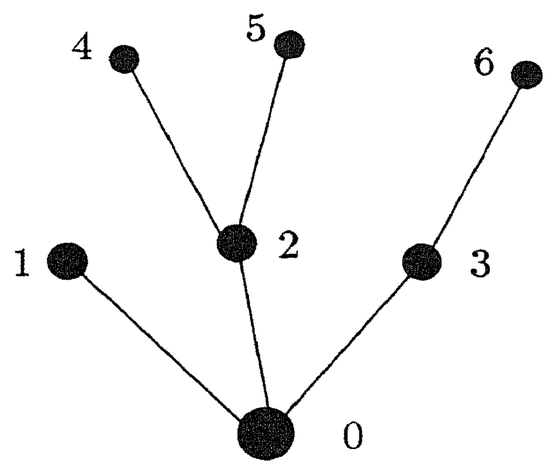
$$(\{w\} \cup \bigcup_{i \in I} B_i,\ \{(w, w_i) \mid i \in I\} \cup \bigcup_{i \in I} \prec_i,\ w)$$

óók een top-down eindige boom.

De notatie voor deze nieuwe boom is $w + \sum_{i \in I} \mathcal{B}_i$ (of ook, als $\{\mathcal{B}_i \mid i \in I\}$ uit maar één element $\mathcal{B}$ bestaat, $w + \mathcal{B}$). Hierin is w de wortel, de bladeren zijn de bladeren van alle $\mathcal{B}_i$ ($i \in I$); de kinderen van w zijn de wortels van de $\mathcal{B}_i$ en de kinderen van een knoop van een $\mathcal{B}_i$ in $w + \sum_{i \in I} \mathcal{B}_i$ zijn dezelfde als de kinderen van die knoop in $\mathcal{B}_i$. Als de hoogten van de bomen $\mathcal{B}_i$ een maximum m bereiken (maar dat hoeft niet het geval te zijn, ook al zijn deze bomen eindig) dan is $m + 1$ de hoogte van $w + \sum_{i \in I} \mathcal{B}_i$. ⊣

Het verband met Definitie 6.13 is als volgt: iedere top-down boom is ook een boom in de zin van 6.13, maar alleen de bomen van 6.13 die geen oneindige tak hebben zijn ook top-down bomen. Zie Opgave 116.

Een illustratie van de top-down groeiwijze is de ontstaansgeschiedenis van de eindige boom met knopen $0, 1, 2, 3, 4, 5, 6$, wortel 0, en ouder/kindrelatie $\{(0,1),(0,2),(0,3),(2,4),(2,5),(3,6)\}$.



Deze boom is top-down verkregen uit de rudimentaire bomen 1, 4, 5 en 6 als $0 + \sum_{i=1,2,3} \mathcal{B}_i$, waarbij $\mathcal{B}_1 = 1$, $\mathcal{B}_2 = 2 + \sum_{i=4,5} i$, en $\mathcal{B}_3 = 3 + 6$.

Bomen waarvan je een plaatje tekent zijn automatisch *geordend*; d.w.z.: de kinderen van een knoop zijn voorzien van de links–rechts ordening van de tekening. Voor dergelijke geordende, eindige bomen wordt de volgende notatie wel gebruikt. Onderstel, dat $\mathcal{T}$ een boom is met wortel f, en dat $f_1, \ldots, f_n$ de kinderen zijn van f in links–rechts volgorde. Als $t_1, \ldots, t_n$ de notaties zijn voor de subbomen $\mathcal{T}_1, \ldots, \mathcal{T}_n$ waarvan deze kinderen de wortels zijn, dus: $\mathcal{T} = f + \sum_{1 \leqslant i \leqslant n} \mathcal{T}_i$, dan is $f(t_1, \ldots, t_n)$ de notatie voor $\mathcal{T}$. Zo kan de boom van het plaatje worden aangegeven door $0(1, 2(4,5), 3(6))$. Hier wordt meestal gedaan of bomen ongeordend zijn. (Maar, zie Opgave 124.)

Een gevolg van deze beschouwingen is de volgende observatie.

6.25 Inbedbaarheid van Bomen. *Als* $\mathcal{B} = w + \sum_{i \in I} \mathcal{B}_i$ *en* $\mathcal{D} = w' + \sum_{j \in J} \mathcal{D}_j$ *bomen zijn, en*

$$f : \{\mathcal{B}_i \mid i \in I\} \longrightarrow \{\mathcal{D}_j \mid j \in J\}$$

is een injectie zódat voor alle $i \in I$, $\mathcal{B}_i \leqslant f(\mathcal{B}_i)$, *dan geldt* $\mathcal{B} \leqslant \mathcal{D}$.

Bewijs. Kies, voor alle $i \in I$, een inbedding $h_i : \mathcal{B}_i \longrightarrow f(\mathcal{B}_i)$. Nu is $\{(w, w')\} \cup \bigcup_{i \in I} h_i$ een inbedding van $\mathcal{B}$ in $\mathcal{D}$. ⊣

Bewijs van 6.23.

Er volgt hetzelfde patroon als het bewijs van 6.21; vergelijk dit aan de hand van de nummering 1–4.

Onderstel dat de collectie van eindige bomen *niet* WQO is.

1. *Constructie van een "minimale" slechte rij.*

Kies een boom T_0 met een minimaal aantal elementen die optreedt als eerste element van een slechte rij;

kies vervolgens een boom T_1 met een minimaal aantal elementen die optreedt als tweede element van een slechte rij die begint met T_0, enz.
De resulterende rij $T_0, T_1, T_2, \ldots$ is slecht.
2. *Decompositie.*
Laat, voor alle $i \in \mathbb{N}$, $\mathcal{B}_i$ de eindige verzameling van subbomen van T_i zijn waarvan de wortel een kind is van de wortel van T_i. ($\mathcal{B}_i$ ontstaat door het uiteenvallen van T_i als je z'n wortel w_i verwijdert; dat is: $T_i = w_i + \sum_{T \in \mathcal{B}_i} T$. Merk op, dat geen der $\mathcal{B}_i$ leeg — T_i rudimentair — kan zijn.)
$\mathcal{B} = \bigcup_{i \in I} \mathcal{B}_i$ is is de vereniging van alle $\mathcal{B}_i$, d.i.: de verzameling van alle in enige $\mathcal{B}_i$ voorkomende bomen.
3. *De decompositie is WQO.*
Onderstel eens, dat $\mathcal{B}$ niet WQO is. Kies een slechte rij $B_0, B_1, B_2, \ldots \in \mathcal{B}$. Selecteer hieruit een deelrij $B_{n_0}, B_{n_1}, B_{n_2}, \ldots$ zódat geldt — als de indices m_i worden bepaald door de stipulering dat $B_{n_i} \in \mathcal{B}_{m_i}$, dat is: B_{n_i} is subboom van T_{m_i} — dat $m_0 < m_1 < m_2 < \cdots$. (Dat kan!)
Nu is de rij

$$T_0, T_1, \ldots, T_{m_0-1}, B_{n_0}, B_{n_1}, B_{n_2}, \ldots$$

slecht (want als $T_i \leqslant B_{n_j}$, dan geldt ook — B_{n_j} is subboom van T_{m_j} — dat $T_i \leqslant T_{m_j}$), wat in strijd is met de keuze van T_{m_0}.
Conclusie: $\mathcal{B} \in WQO$.
4. *Terug naar 1.*
Dus (Lemma 6.21): de collectie van eindige deelverzamelingen van $\mathcal{B}$ is WQO.
I.h.b. is dus $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2, \ldots$ goed. Bijvoorbeeld, $i < j$ en $\mathcal{B}_i \leqslant \mathcal{B}_j$.
Laat $f : \mathcal{B}_i \to \mathcal{B}_j$ een injectie zijn zódat voor alle $T \in \mathcal{B}_i$, $T \leqslant f(T)$.
Wegens 6.25 geldt nu dat $T_i \leqslant T_j$. Tegenspraak. Het bewijs is af. ⊣

Opgaven

116 ♣ Bewijs:

1. iedere top-down boom is óók een boom in de zin van 6.13,
2. iedere boom in de zin van 6.13 die geen oneindige takken heeft is een top-down boom.

Oplossing van 2. Onderstel, dat $\mathcal{B}$ een boom is.
Bewering. Als $b \in \mathcal{B}$ en $\mathcal{B}_b$ is niet top-down, dan heeft b een kind c zódat $\mathcal{B}_c$ niet top-down is.
Bewijs. Direct uit de definitie van *top-down.*
Gevolg. Als $\mathcal{B}$ niet top-down is dan heeft $\mathcal{B}$ een oneindige tak.

117 ♣ Onderstel, dat R een relatie is op A. T is de verzameling van alle eindige rijtjes $(a_0, \ldots, a_{n-1})$ van elementen van A zódat voor $i < n-1$: $a_{i+1} R a_i$. Als $(a_0, \ldots, a_n)$ ook zo'n rijtje is schrijf je $(a_0, \ldots, a_{n-1}) \prec (a_0, \ldots, a_n)$. w is het lege rijtje. Bewijs:

1. $(T, \prec, w)$ is een boom,
2. als R gefundeerd is op A, dan is $(T, \prec, w)$ een top-down boom.

118 ♣ Bewijs:

1. als $\prec$ gefundeerd is op Q en $\prec' \subset \prec$, dan is $\prec'$ ook gefundeerd op Q,

2. als $\leqslant$ WQO is op Q, $\leqslant'$ QO is op Q en $\leqslant \subset \leqslant'$, dan is $\leqslant'$ WQO op Q.

119 ♣ Laat $\leqslant$ een QO zijn op Q. Definieer $p < q :\equiv p \leqslant q \wedge q \not\leqslant p$. Bewijs: $\leqslant$ is WQO op Q d.e.s.d.a. $<$ gefundeerd is op Q en er geen oneindige verzameling $A \subset Q$ bestaat zódat $\forall p \in A\, \forall q \in A\, (p \not\leqslant q)$.
Aanwijzing. Gebruik Ramsey's stelling.

120 ♣ Onderstel dat Q WQO is. Definieer de volgende QO op de collectie van eindige deelverzamelingen van Q (een modificatie van de in Lemma 6.21 gebruikte QO): $A \leqslant_m B :\equiv$ er is een (niet noodzakelijk injectieve) functie $f : A \to B$ zódat $\forall q \in A\, (q \leqslant f(q))$. Bewijs dat $\leqslant_m$ ook een WQO is.

121 ♣ (Higman's Stelling.) Onderstel, dat $\leqslant$ WQO is op Q. Definieer de QO $\preceq_1$ tussen eindige rijtjes uit Q door $(p_1, \ldots, p_n) \preceq_1 (q_1, \ldots, q_m) :\equiv$ er zijn $j_1, \ldots, j_n$ met $1 \leqslant j_1 < \cdots < j_n \leqslant m$ zódat, voor $1 \leqslant i \leqslant n$, $p_i \leqslant q_{j_i}$. Bewijs, dat $\preceq_1$ WQO is.
Aanwijzing. Modificeer het bewijs van 6.21.

122 ♣ Onderstel, dat $\sqsubseteq$ een relatie tussen top-down bomen is waarvoor geldt:

1. voor iedere rudimentaire boom w en iedere top-down boom $\mathcal{D}$ geldt $w \sqsubseteq \mathcal{D}$,
2. $w + \sum_{i \in I} \mathcal{B}_i \sqsubseteq \mathcal{D}$ geldt d.e.s.d.a.:
   $\mathcal{D} = w' + \sum_{j \in J} \mathcal{D}_j$, en $j \in J$ bestaat zódat $w + \sum_{i \in I} \mathcal{B}_i \sqsubseteq \mathcal{D}_j$, of er is een injectie $h : I \to J$ zódat voor alle $i \in I$ $\mathcal{B}_i \sqsubseteq \mathcal{D}_{h(i)}$.

(Merk op dat de inbeddingsrelatie tussen top-down bomen deze eigenschappen heeft.)
Bewijs dat voor alle eindige, of zelfs: top-down, bomen $\mathcal{B}$ en $\mathcal{D}$ geldt: $\mathcal{B} \leqslant \mathcal{D}$ d.e.s.d.a. $\mathcal{B} \sqsubseteq \mathcal{D}$.

123 ♣ De relatie $\leqslant_m$ tussen top-down bomen wordt gedefinieerd door in de de condities van Opgave 122 niet te eisen dat de functie h injectief is:

1. voor iedere rudimentaire boom w en iedere top-down boom $\mathcal{D}$ geldt $w \leqslant_m \mathcal{D}$,
2. $w + \sum_{i \in I} \mathcal{B}_i \leqslant_m \mathcal{D}$ geldt d.e.s.d.a.:
   $\mathcal{D} = w' + \sum_{j \in J} \mathcal{D}_j$, en $j \in J$ bestaat zódat $w + \sum_{i \in I} \mathcal{B}_i \leqslant_m \mathcal{D}_j$, of er is een functie $h : I \to J$ zódat voor alle $i \in I$ $\mathcal{B}_i \leqslant_m \mathcal{D}_{h(i)}$.

Bewijs dat $\leqslant_m$ WQO is op de klasse van eindige bomen.

124 ♣ Aan een inbedding tussen geordende bomen wordt de eis opgelegd dat de ordening van kinderen bewaard blijft. D.w.z. — zie 6.22 (blz. 84)— als $h : \mathcal{B} \to \mathcal{D}$ zo'n inbedding is, en het kind b_1 van $a \in \mathcal{B}$ is "links" van zijn broer b_2, dan is $h(b_1)$ element van een subboom D_{d_1} die "links" is van de subboom D_{d_2} waarvan $h(b_2)$ element is.
Bewijs Kruskal's stelling voor *geordende* eindige bomen.
Aanwijzing. Modificeer het gegeven bewijs. Gebruik Higman's Stelling i.p.v. Lemma 6.21.

125 ♣ Onderstel dat Q WQO is. Een Q-*boom* is een struktuur $\mathcal{T} = (T, \prec, w, l)$ waarbij $(T, \prec, w)$ een boom is en $l : T \to Q$ een functie van T naar Q. Een Q-inbedding tussen Q-bomen $\mathcal{T}_1 = (T_1, \prec_1, w_1, l_1)$ en $\mathcal{T}_2 = (T_2, \prec_2, w_2, l_2)$ is een inbedding h tussen de bomen $(T_1, \prec_1, w_1)$ en $(T_2, \prec_2, w_2)$ zódat voor alle $t \in T_1$, $l_1(t) \leqslant l_2(h(t))$. Toon aan: deze Q-inbeddingsrelatie tussen eindige (desgewenst: geordende) Q-bomen is WQO.
Aanwijzing. Wijzig het bewijs van Stelling 6.23 als volgt. Neem deel 1 letterlijk over, maar nu is $T_0, T_1, T_2, \ldots$ een "minimale" rij van geordende Q-bomen. In deel 2 is $\mathcal{B}_i$ nu

de door de ordening van T_i *geordende* verzameling (of eindige rij) van subbomen van T_i zódat $T_i = w_i + \sum \mathcal{B}_i - w_i$ de wortel van T_i. Deel 3 blijft onveranderd, maar nu pas je Higman's stelling toe: de verzameling der $\mathcal{B}_i$ is WQO. Productlemma: het product met $\{l(w_i) \mid i \in \mathbb{N}\}$ is WQO. Dus, de rij $(l(w_0), \mathcal{B}_0), (l(w_1), \mathcal{B}_1), (l(w_2), \mathcal{B}_2), \ldots$ is goed. Bijvoorbeeld, $l(w_i) \leqslant l(w_j)$ en $\mathcal{B}_i \leqslant \mathcal{B}_j$ $(i < j)$. Dus, $T_i = w_i + \sum \mathcal{B}_i \leqslant w_j + \sum \mathcal{B}_j = T_j$.

Samenvatting

Belangrijkste begrippen in Secties 6.1 en 6.2:

- Inductie, basis, inductiestap, inductiehypothese,
- gelijkmachtig,
- eindig/oneindig.

Literatuur

Inductie wordt, met goed gekozen voorbeelden, ook behandeld in Devlin [4].

Voor Ramsey-theorie, zie het boek van R.L. Graham, B.L. Rothschild en J.H. Spencer, *Ramsey theory*, 2e druk, Wiley 1990. Opgave 107 staat op de eerste bladzij van dat boek.

Smullyan's balspel is beschreven in R.M. Smullyan, Trees and ball games, *Ann. of the New York Ac. of Sci.* 321 (1979), 86–90. Het gevecht tussen Hercules en de Hydra (met de restrictie dat de Hydra altijd de ouder van de afgehakte kop kiest als wortel voor de te regeneren subboom, en dat in de n-de ronde precies n kopieën worden geregenereerd) staat in Laurie Kirby and Jeff Paris, Accessible independence results for Peano arithmetic, *Bull. London Math. Soc.*, 14 (1982), 285–293. Het bewijs daar voor Stelling 6.17 gebruikt de ordinalen van Sectie 10.5 en is dus minder elementair. Voor meer "tasks you cannot help finishing no matter how hard you try to block finishing them", zie M. Gardner, *Scientific American* 249 (Augustus 1983) 8–13.

Het hier opgenomen bewijs van Kruskal's stelling (Joseph B. Kruskal, Well-quasi ordering, the tree theorem, and Vazsonyi's conjecture, *TAMS* 95 (1960), 210–225), i.h.b. het gebruik van minimaal-slechte rijen, is van Nash-Williams (C.St.J.A. Nash-Williams, On well-quasi-ordering finite trees, *Proc. Cambridge Philos. Soc.* 59 (1963), 833–835).

Een diep resultaat in de theorie van wel-quasi-ordeningen is Laver's bewijs (1971) voor *Fraïssé's vermoeden*, dat de collectie van aftelbare lineaire ordeningen (Definitie 9.11) WQO is onder de *inbeddings*relatie (Definitie 10.4).

Hoofdstuk 7

Formele Bewijzen

In de wiskunde wordt de waarheid van een bewering gewoonlijk vastgesteld door een *bewijs*. Dit hoofdstuk is — vergeleken met de op praktijkgebruik gerichte formulering van de regels van Sectie 2.2, blz. 17 e.v. — van meer theoretische aard. Het geeft één van de vele mogelijke precieze definities van het met *bewijs* overeenkomende formele begrip *afleiding* in de context van de propositielogica. Met alleen 5 van de in Sectie 2.2 besproken 15 regels (voldoende voor de propositie-logica gebaseerd op $\rightarrow$, $\wedge$ en het nieuwe teken $\bot$) wordt precies gedefinieerd wat onder een *afleiding* wordt verstaan, en de relatie met de waarheidstafel-benadering wordt gelegd door een *betrouwbaarheids-* en een *volledigheids*stelling.

7.1 Natuurlijke Deductie

Het in Sectie 2.2 behandelde systeem van afleidingen heet *natuurlijke deductie*. Het is *natuurlijk* omdat zijn regels nauw aansluiten bij gangbaar "logisch gedrag".

De discussie wordt nu geprecizeerd, en daarom beperkt, tot de propositielogica met alleen de connectieven $\rightarrow$ en $\wedge$, en het nieuwe teken *falsum*, dat genoteerd wordt als $\bot$. Grammaticaal gedraagt $\bot$ zich als een propositieletter. Dat betekent dat je $\bot$ mag gebruiken als formule en als ingredient van andere formules. De *betekenis* van $\bot$ is *de onware zin*, d.w.z.: per definitie heeft $\bot$ de waarheidswaarde O (ONWAAR). (Soms wordt ook nog de constante $\top$, *verum*, voor *de ware zin* gebruikt.)

Dat je alleen $\bot$, $\rightarrow$ en $\wedge$ tot je beschikking hebt maakt de propositie-logica er niet armer op. Zo is eenvoudig na te gaan, dat een formule $\varphi \rightarrow \bot$ kan dienen als surrogaat voor $\neg\varphi$, want hij heeft dezelfde waarheidswaarde als $\neg\varphi$ onder iedere toekenning van waarheidswaarden aan de propositieletters (ga na). Deze definitie van negatie heeft tot gevolg, dat de negatie regels $\neg$E en $\neg$I overbodig worden: dit zijn nu speciale gevallen van $\rightarrow$E en $\rightarrow$I geworden. Je kunt verder ook $\vee$ simuleren: $\varphi \vee \psi$ is immers equivalent met $\neg\varphi \rightarrow \psi$, etc.

De afleidingen van het systeem van natuurlijke deductie hebben de vorm van een eindige boom. In de toppen van zo'n boom staan formules die "ingetrokken" kunnen zijn. Niet-ingetrokken formules in de boom-toppen heten de *hypothesen* van de afleiding. In de wortel van de boom staat één formule: de *afgeleide* formule of *conclusie*.

De afleidingsbomen worden geconstrueerd m.b.v. zes zgn. *afleidingsregels*, in Hoofdstuk 2 *bewijsregels* genoemd. Bijna ieder logisch teken heeft een *introductie-* en een *eliminatie-regel* (maar $\bot$ heeft geen introductieregel en $\wedge$ heeft twee eliminatieregels).

Deze afleidingsregels, in schema-vorm, staan in de tabel hierna. De betekenis van deze schemas wordt hier globaal (Sectie 2.2 is uitvoeriger), en in Definitie 7.1 precies, uitgelegd.

De afleidingsregels stellen de simpelste stappen voor die in afleidingen mogen worden gemaakt. De introductieregel voor $\wedge$ bijvoorbeeld zegt dat $\varphi \wedge \psi$ "direct afleidbaar" is uit φ en ψ. Rechte haken om formules en stippeltjes in $\bot$-eliminatie en $\rightarrow$-introductie betekenen het volgende. De laatste wil zeggen:

als er een afleiding ($\vdots$) van ψ is uit hypothesen waaronder (mogelijk) φ, dan geldt $\varphi \rightarrow \psi$ ook als afgeleid, maar dan zonder dat φ langer als hypothese telt. Haken om een formule stelt dus *intrekken* van een hypothese voor. (Maak je zelf een afleiding, dan kun je intrekken van een hypothese ook met doorstrepen van die hypothese aangeven.)

De introductieregel voor $\rightarrow$ correspondeert kennelijk met geaccepteerd wiskundig gedrag: wil je $\varphi \rightarrow \psi$ bewijzen, dan begin je met φ aan te nemen ("als hypothese"), en je probeert vervolgens ψ af te leiden. Lukt dat, dan kan $\varphi \rightarrow \psi$ als bewezen gelden.

Net zo correspondeert $\bot$-eliminatie met geaccepteerd gedrag ("bewijs uit het ongerijmde"): als je de "ongerijmdheid" $\bot$ kunt deduceren uit de hypothese $\neg\varphi$ (d.w.z.: $\varphi \rightarrow \bot$) d.i.: dat φ *niet* geldt, dan moet φ kennelijk tóch het geval zijn.

De twee regels voor $\rightarrow$ geven een operationele verklaring voor de logische functie van $\rightarrow$. Net zo doen de overige regels dit voor de andere tekens. Vergelijk deze tabel met die op blz. 24.

	introductie	*eliminatie*
$\bot$	geen	$\dfrac{\begin{array}{c}[\varphi \rightarrow \bot] \\ \vdots \\ \bot\end{array}}{\varphi}$
$\rightarrow$	$\dfrac{\begin{array}{c}[\varphi] \\ \vdots \\ \psi\end{array}}{\varphi \rightarrow \psi}$	$\dfrac{\varphi \quad \varphi \rightarrow \psi}{\psi}$
$\wedge$	$\dfrac{\varphi \quad \psi}{\varphi \wedge \psi}$	$\dfrac{\varphi \wedge \psi}{\varphi}$ $\quad$ $\dfrac{\varphi \wedge \psi}{\psi}$

7.2 Afleidingen

Een afleiding is een eindige boom waarvan de knopen formules zijn, en die op een speciale manier is verkregen.

Alles wat je hier van eindige bomen moet weten is wat terminologie (zie 6.14, blz. 77) en hun "omgekeerde groeiwijze" (zie Definitie 6.24, blz. 84).

Afleidingsbomen zijn *binair*, d.w.z.: in de constructen $w + \sum_{i\in I} \mathcal{B}_i$ van 6.24(Σ) geldt hier altijd, dat $\{\mathcal{B}_i \mid i \in I\}$ hoogstens *twee* elementen heeft. De wortel van een afleiding is zijn conclusie, maar het is niet zo dat al z'n bladeren hypothesen zijn: de hypothesen vormen een *deel* van de bladeren; wèlk deel dat is wordt precies aangegeven door de volgende definitie.

7.1 Afleiding, Conclusie, Hypothese.

(0) Een rudimentaire boom (Definitie 6.24(0)) bestaande uit één enkele formule is een (*rudimentaire*) afleiding.

De conclusie van zo'n afleiding is de formule zelf.
De enige hypothese is eveneens die formule.

(∧E) (∧*-eliminatie*) Als $\mathcal{D}$ een afleiding is met conclusie $\varphi \wedge \psi$, dan zijn de twee bomen die verkregen worden uit $\mathcal{D}$ door er φ danwel ψ onder te zetten eveneens afleidingen.

De eerste heeft conclusie φ, de tweede heeft conclusie ψ.
De hypothesen van de nieuwe afleidingen zijn dezelfde als die van $\mathcal{D}$.

(In de notatie van Definitie 6.24($\sum$) worden deze bomen weergegeven als $\varphi + \mathcal{D}$ en $\psi + \mathcal{D}$.)

(∧I) (∧ *-introductie*) Als $\mathcal{D}_1$ en $\mathcal{D}_2$ afleidingen zijn met conclusies φ en ψ (of andersom) dan is de boom verkregen door $\mathcal{D}_1$ en $\mathcal{D}_2$ naast elkaar te zetten en $\varphi \wedge \psi$ als nieuwe wortel eronder eveneens een afleiding.

De conclusie van deze afleiding is $\varphi \wedge \psi$.
De hypothesen zijn: alle hypothesen van $\mathcal{D}_1$ plus die van $\mathcal{D}_2$.

(In de notatie van 6.24($\sum$) is dit: $(\varphi \wedge \psi) + \sum_{i=1,2} \mathcal{D}_i$.)

(→E) (MP, *Modus Ponens*, →*eliminatie*) Als $\mathcal{D}_1$ en $\mathcal{D}_2$ afleidingen zijn met conclusies φ resp. $\varphi \to \psi$ (of andersom) dan is de boom verkregen door $\mathcal{D}_1$ en $\mathcal{D}_2$ naast elkaar te zetten en ψ als nieuwe wortel eronder eveneens een afleiding.

Deze heeft conclusie ψ.
Z'n hypothesen zijn: alle hypothesen van $\mathcal{D}_1$ plus die van $\mathcal{D}_2$.
(In de notatie van 6.24($\sum$) is dit: $\psi + \sum_{i=1,2} \mathcal{D}_i$.)

(→I) (D, *Deductie-regel*, →*-introductie*) Als $\mathcal{D}$ een afleiding met conclusie ψ is, en φ is een (willekeurige) formule, dan is de boom verkregen uit $\mathcal{D}$ door er $\varphi \to \psi$ onder te zetten eveneens een afleiding.

De conclusie van deze afleiding is $\varphi \to \psi$.
De hypothesen ervan zijn: die van $\mathcal{D}$ *minus* φ.
Dit heet: de hypothese φ van $\mathcal{D}$ wordt *ingetrokken*, d.w.z.: φ telt niet meer als hypothese van de nieuw gevormde afleiding.

(In de notatie van 6.24($\sum$) is de nieuw gevormde afleiding: $(\varphi \to \psi) + \mathcal{D}$.)

N.B.: φ hoeft niet daadwerkelijk in $\mathcal{D}$ voor te komen als hypothese. Hij mag ook meer dan ééns als hypothese voorkomen, en wordt dan op al die plaatsen ingetrokken.

$\perp$E (BO, *Bewijs uit het Ongerijmde*; $\perp$-regel) Laat $\mathcal{D}$ een afleiding zijn met conclusie $\perp$ en φ een (willekeurige) formule. De boom verkregen uit $\mathcal{D}$ door er φ onder te zetten is eveneens een afleiding.

Zijn conclusie is φ.
Z'n hypothesen zijn: die van $\mathcal{D}$, *minus* $\neg\varphi$ $(= \varphi \to \perp)$.
Dus: $\neg\varphi$ wordt door deze stap *ingetrokken.*

(In de notatie van 6.24($\sum$) is dit: $\varphi + \mathcal{D}$.)

N.B.: $\neg\varphi$ hoeft weer niet daadwerkelijk als hypothese in $\mathcal{D}$ voor te komen — in dat geval valt er dus niets in te trekken, maar hij kan ook op meer dan één plaats worden ingetrokken.

Er volgen een paar afleidingen ter illustratie van deze definitie. Iedere horizontale streep geeft het gebruik van een regel aan; welke regel dat is wordt naast de streep aangegeven. In de praktijk mag je wel strepen weglaten bij alle regels behalve $\wedge$I en MP: dit zijn de enige regels die vertakkingen tot gevolg hebben en waarmee dus twee afleidingen worden verbonden tot een nieuwe.

In het volgende stellen φ, ψ en η willekeurige formules voor.

7.2 Voorbeelden. De cijfers 1 en 2 verwijzen naar het intrekken van hypothesen (die na intrekking dus geen hypothese meer zijn in de nieuwe afleiding). Hier volgen een aantal afleidingen waarvan de eerste vier corresponderen met deductieproblemen uit Hoofdstuk 2.

1. Een afleiding van $\varphi \to \eta$ met hypothesen $\varphi \to \psi$ en $\psi \to \eta$.

$$\dfrac{\dfrac{\dfrac{[\varphi]^1 \qquad \varphi \to \psi}{\psi}\,\text{MP} \qquad \psi \to \eta}{\eta}\,\text{MP}}{\varphi \to \eta}\,\text{D}-1^{\,1}$$

2. (Zie Opgave 5 blz. 20.) Een afleiding van $\varphi \to \eta$ met hypothesen $\varphi \to \psi$ en $\varphi \to (\psi \to \eta)$.

$$\dfrac{\dfrac{\dfrac{[\varphi]^1 \qquad \varphi \to \psi}{\psi}\,\text{MP} \qquad \dfrac{[\varphi]^1 \qquad \varphi \to (\psi \to \eta)}{\psi \to \eta}\,\text{MP}}{\eta}\,\text{MP}}{\varphi \to \eta}\,\text{D}-1^{\,1}$$

3. (Zie Opgave 7.1 blz. 22.) Een afleiding van $\neg\psi \to \neg\varphi$ met hypothese $\varphi \to \psi$.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\varphi]^1 \qquad \varphi \to \psi}{\psi} \qquad [\neg\psi]^2}{\bot}}{\neg\varphi}}{\neg\psi \to \neg\varphi}\ \begin{matrix}\text{MP}\\ \text{MP}\\ \text{D-1}\\ \text{D-2}\end{matrix}$$

4. (Zie Opgave 7.2.) Een afleiding van $\varphi \to \psi$ met hypothese $\neg\psi \to \neg\varphi$. Vrijwel identitiek met voorafgaande, desondanks een beetje anders:

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg\psi]^1 \qquad \neg\psi \to \neg\varphi}{\neg\varphi} \qquad [\varphi]^2}{\bot}}{\psi}}{\varphi \to \psi}\ \begin{matrix}\text{MP}\\ \text{MP}\\ \text{BO-1}\\ \text{D-2}\end{matrix}$$

5. Een afleiding van $\neg\neg\varphi$ met hypothese φ.

$$\dfrac{\dfrac{\varphi \qquad [\neg\varphi]^1}{\bot}}{\neg\neg\varphi}\ \begin{matrix}\text{MP}\\ \text{D-1}\end{matrix}$$

6. Een afleiding van φ met hypothese $\neg\neg\varphi$. Vrijwel identitiek met voorafgaande maar weer een tikkeltje anders:

$$\dfrac{\dfrac{\neg\neg\varphi \qquad [\neg\varphi]^1}{\bot}}{\varphi}\ \begin{matrix}\text{MP}\\ \text{BO-1}\end{matrix}$$

De omstandigheid dat hypothesen kunnen worden ingetrokken maakt het mogelijk om afleidingen te construeren die helemaal geen hypothesen hebben.

7.3 Voorbeeld. De volgende afleiding heeft geen hypothese. N.B.: $\neg\neg\varphi$ is: $(\varphi \to \bot) \to \bot$.

$$\dfrac{\dfrac{\dfrac{[\neg\neg\varphi]^2 \qquad [\neg\varphi]^1}{\bot}}{\varphi}}{\neg\neg\varphi \to \varphi}\ \begin{matrix}\text{MP}\\ \text{BO-1}\\ \text{D-2}\end{matrix}$$

Nu volgen een aantal afleidingen die wat moeilijker zijn.

7.4 Voorbeeld. De volgende afleiding deduceert de conclusie $\varphi \to \bot$ — d.w.z., $\neg\varphi$ — uit de hypothese $(\psi \to \varphi) \to \bot$ — d.i.: $\neg(\psi \to \varphi)$.

$$\dfrac{\dfrac{\dfrac{[\varphi]^1}{\psi \to \varphi} \qquad (\psi \to \varphi) \to \bot}{\bot}}{\varphi \to \bot}\ \begin{matrix}\text{D}\\ \text{MP}\\ \text{D-1}\end{matrix}$$

Bij de eerste toepassing van D had ψ ingetrokken kunnen worden — maar die trad niet op als hypothese. De formule φ werd als hypothese ingetrokken bij de tweede (laatste) toepassing van D.
N.B.: een stap als de laatste ($\varphi \to \bot$ concluderen m.b.v. D) wordt vaak met een BO-toepassing verward, speciaal als je $\neg\varphi$ schrijft voor $\varphi \to \bot$. De laatste stap in deze afleiding had ook met BO kunnen worden gerechtvaardigd — maar dan zou je alleen $(\varphi \to \bot) \to \bot$ hebben kunnen intrekken als hypothese en niet φ. En de eerste formule komt niet als hypothese voor en de tweede wèl.

7.5 Voorbeeld. Dit is een afleiding van φ uit de hypothese $\neg(\varphi \to \psi)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\varphi \to \bot]^2 \qquad [\varphi]^1}{\bot}\,\text{MP}}{\psi}\,\text{BO}}{\varphi \to \psi}\,\text{D-1} \qquad (\varphi \to \psi) \to \bot}{\bot}\,\text{MP}}{\varphi}\,\text{BO-2}$$

Gedefinieerde connectieven. In het vervolg moeten $\neg$, $\vee$ en $\leftrightarrow$ altijd worden opgevat als afkortingen die eerst moeten worden uitgeschreven voordat we afleidingen kunnen gaan maken:

$$\begin{aligned} \neg\varphi &:= \varphi \to \bot \\ \varphi \vee \psi &:= \neg\varphi \to \psi \\ \varphi \leftrightarrow \psi &:= (\varphi \to \psi) \wedge (\psi \to \varphi) \end{aligned}$$

Merk op: de formules links hebben dezelfde waarheidstafel als de corresponderende formules rechts!

Waarschuwingen.

- Verwar BO (dat is: φ concluderen uit $\bot$ en tegelijkertijd $\neg\varphi$ intrekken) niet met het speciale geval van D dat $\neg\varphi$ concludeert uit $\bot$ en φ intrekt.
- Het ligt in de aard van de boom, dat takken naar boven toe niet aaneengroeien. Onderdruk de neiging om dat te doen en kopieer desnoods hele subbomen op verschillende plaatsen in je afleiding.
- Wees nauwkeurig bij het intrekken van hypothesen — één hypothese kan op meer plaatsen voorkomen — en houd boek in de marge.
  N.B.: hypothesen staan altijd in de *toppen* van de afleidingsboom!

Aanwijzingen. Hoewel de definitie van *afleiding* "top-down" is (d.w.z.: een afleiding wordt vlgs. de definitie van boven naar onder gevormd) worden afleidingen in de praktijk vaak gevonden door een proces dat kan oscilleren tussen "top-down" (als er een directe conclusie wordt getrokken: MP en de $\wedge$-regels) en (een soort) "bottom-up" (D en BO). De voorafgaande voorbeelden illustreren al een aantal taktieken die goede diensten bewijzen bij het construeren van

afleidingen. (Her)Lees Sectie 2.3, blz. 24. Een algemene taktiek is om altijd te proberen om een afleidingsprobleem voor zekere formules te vervangen door één met simpeler formules. Je moet dus zeker formules vermijden die ingewikkelder zijn dan de hypothesen en de conclusie.

Moet je $\varphi \to \psi$ afleiden uit de hypothesenverzameling Γ dan kun je dit probleem vervangen door het vinden van een afleiding van ψ uit $\Gamma \cup \{\varphi\}$: de gezochte afleiding volgt dan door een toepassing van de deductieregel D. I.h.b. is dit van toepassing op het geval waarin $\psi = \bot$ (dus $\varphi \to \psi$ is $\neg\varphi$).

Wil het afleiden van φ helemaal niet lukken, dan kun je altijd proberen of je met $\neg\varphi$ als extra hypothese verder komt en BO toepassen.

Opgaven

126 ♣ Geef hypothese-vrije afleidingen van de volgende logische geldigheden:

1. $\varphi \to (\psi \to \varphi)$,
2. $\neg\varphi \to (\varphi \to \psi)$,
3. $(\varphi \to \psi) \to ((\psi \to \sigma) \to (\varphi \to \sigma))$,
4. $(\varphi \to (\psi \to \sigma)) \to ((\varphi \to \psi) \to (\varphi \to \sigma))$.

127 ♣ Idem, voor:

1. $\varphi \to \neg\neg\varphi$,
2. $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$, $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$,
3. $\neg(\varphi \to \psi) \to \varphi$, $\neg(\varphi \to \psi) \to \neg\psi$,
4. $(\varphi \wedge \neg\psi) \to \neg(\varphi \to \psi)$, $\neg(\varphi \to \psi) \leftrightarrow (\varphi \wedge \neg\psi)$.

128 ♣ Idem, nu voor:

1. $(\varphi \wedge \psi) \to (\psi \wedge \varphi)$,
2. $(\varphi \wedge (\psi \wedge \sigma)) \to ((\varphi \wedge \psi) \wedge \sigma)$.

129 ♣ Idem, voor:

1. $\varphi \to \varphi$,
2. $\bot \to \varphi$,
3. $\varphi \to \neg\bot$.

130 ♣ Idem, voor:

1. $(\varphi \to \neg\varphi) \to \neg\varphi$,
2. $(\neg\varphi \to \varphi) \to \varphi$.

Aanwijzing. Een afleiding voor 2 kun je vinden als sub-afleiding in het volgende voorbeeld (neem $\psi = \bot$).

7.6 Voorbeeld. Hier is een hypothese-vrije afleiding van $((\varphi \to \psi) \to \varphi) \to \varphi$, de *wet van Peirce*. Probeer eerst eens zelf, en ontdek daarbij dat het bijvoeglijk naamwoord 'natuurlijke' in 'natuurlijke deductie' misschien tussen aanhalingstekens moet worden geplaatst.

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg\varphi]^2 \qquad [\varphi]^1}{\bot}\,\text{BO}}{\varphi\to\psi}\,\text{D-1} \qquad [(\varphi\to\psi)\to\varphi]^3}{\varphi}\,\text{MP} \qquad [\neg\varphi]^2}{\bot}\,\text{MP}$$
$$\dfrac{\dfrac{\bot}{\varphi}\,\text{BO-2}}{((\varphi\to\psi)\to\varphi)\to\varphi}\,\text{D-3}$$

Merk op, dat hier één hypothese (2) op twee plaatsen tegelijk is ingetrokken. Omdat $\to$ het enige connectief is in Peirce's wet, zou je kunnen denken dat alleen $\to$-regels nodig zijn voor de afleiding, maar zonder BO lukt het niet.

131 ♣♣ Geef een hypothese-vrije afleiding voor $((\varphi\to\psi)\to\psi)\to((\psi\to\varphi)\to\varphi)$.
Aanwijzing. Zie eventueel Opgave 145.

7.3 Afleidbaarheid

7.7 Afleidbaar. Een formule φ heet *afleidbaar uit* de formuleverzameling Γ, als er een afleiding bestaat *van* φ *uit* Γ, dat is: een afleiding met φ als conclusie, en waarvan iedere hypothese element is van Γ.

Notatie. Dat φ afleidbaar is uit Γ wordt genoteerd door: $\Gamma\vdash\varphi$. Als $\Gamma=\{\varphi_1,\ldots,\varphi_n\}$, dan kun je ook $\varphi_1,\ldots,\varphi_n\vdash\varphi$ schrijven. De notatie $\vdash\varphi$ betekent dat $\emptyset\vdash\varphi$: φ is (hypothese-vrij) afleidbaar. $\Gamma,\psi\vdash\varphi$ betekent: $\Gamma\cup\{\psi\}\vdash\varphi$.

7.8 Lemma. *Als* $\Gamma\vdash\varphi$ *en* $\Delta,\varphi\vdash\psi$, *dan geldt* $\Gamma\cup\Delta\vdash\psi$.

Opgaven

132 ♣ Bewijs Lemma 7.8.

De volgende opgaven vragen een aantal zgn. *afgeleide* regels te bewijzen.

133 ♣ Bewijs:

1. $\Gamma\vdash(\varphi\to\psi)\iff\Gamma,\varphi\vdash\psi$,
2. $\Gamma\vdash\varphi\wedge\psi\iff\Gamma\vdash\varphi$ en $\Gamma\vdash\psi$,
3. $\Gamma\vdash\neg\varphi\iff\Gamma,\varphi\vdash\bot$.

Voorbeeld.
1($\Rightarrow$): Onderstel, dat $\mathcal{D}$ een afleiding is van $\varphi\to\psi$ uit Γ. Voeg onderaan $\mathcal{D}$ een toepassing van modus ponens toe onder gebruikmaking van een nieuwe hypothese φ. Dit is de gezochte afleiding van ψ uit Γ en φ.
1($\Leftarrow$): Onderstel, dat $\mathcal{D}$ een afleiding is van ψ uit Γ met φ. Verleng $\mathcal{D}$ met de formule $\varphi\to\psi$ en trek φ als hypothese in (deductie-regel). Dit is de gezochte afleiding van $\varphi\to\psi$ uit Γ.
Merk op, dat onderdeel 3 het speciale geval van 1 is, met $\psi=\bot$.

134 ♣ Vgl. Opgave 133.2. Geldt $\Gamma \vdash \varphi \vee \psi$ d.e.s.d.a. $\Gamma \vdash \varphi$ of $\Gamma \vdash \psi$? Geef bewijs of tegenvoorbeeld.

135 ♣ Bewijs:

1. $\Gamma, \varphi \vdash \psi \implies \Gamma, \eta \to \varphi \vdash \eta \to \psi$,
2. $\Gamma, \varphi \vdash \psi \implies \Gamma, \psi \to \eta \vdash \varphi \to \eta$.

136 ♣ Bewijs:

1. Als $\Gamma, \varphi \vdash \neg\varphi$, dan geldt $\Gamma \vdash \neg\varphi$. Dw.z.: gegeven is een afleiding $\mathcal{D}$ van $\neg\varphi$ uit Γ, φ; gevraagd wordt een afleiding te construeren (die van $\mathcal{D}$ als sub-afleiding gebruik maakt) van $\neg\varphi$ uit Γ,
2. als $\Gamma, \neg\varphi \vdash \varphi$, dan geldt $\Gamma \vdash \varphi$.

137 ♣ Idem:

1. Als $\Gamma, \varphi \to \psi \vdash \bot$, dan geldt $\Gamma \vdash \neg\psi$,
2. als $\Gamma, \varphi \to \psi \vdash \bot$, dan geldt $\Gamma \vdash \varphi$.

Hint. Het probleem is hier, dat boven de hypothesen van de gegeven afleidingen afleidinkjes voor die hypothesen moeten komen.
Voorbeeld: 1. Onderstel, dat $\mathcal{D}$ een afleiding is van $\bot$ uit $\Gamma, \varphi \to \psi$. Dan is het volgende een afleiding van $\neg\psi$ uit Γ:

$$\cfrac{\cfrac{[\psi]^1}{\varphi \to \psi}\,\mathrm{D}\quad \mathcal{D}}{\bot}$$
$$\cfrac{\bot}{\neg\psi}\,\mathrm{D}-1$$

Natuurlijk kan $\varphi \to \psi$ meerdere keren als hypothese optreden; dan moet boven al die optredens een optreden van ψ worden geplaatst.

138 ♣♣ Idem:

1. Als $\Gamma, \varphi \vdash \chi$ en $\Gamma, \neg\varphi \vdash \chi$, dan geldt $\Gamma \vdash \chi$,
2. als $\Gamma, \varphi \vdash \chi$ en $\Gamma, \psi \vdash \chi$, dan geldt $\Gamma, \varphi \vee \psi \vdash \chi$.

Voorbeeld. Hier is een oplossing voor onderdeel 1. Die voor 2 is hier een kleine modificatie van.
Onderstel, dat $\mathcal{D}_1$ een afleiding is van χ uit Γ, φ en dat $\mathcal{D}_2$ er één is van χ uit $\Gamma, \neg\varphi$. Het volgende is een afleiding van χ uit Γ.

$$\cfrac{\cfrac{\cfrac{[\varphi]^1}{\mathcal{D}_1}\quad \chi \qquad [\neg\chi]^2}{\bot}\,\mathrm{MP}}{\neg\varphi}\,\mathrm{D}-1 \qquad \mathcal{D}_2$$
$$\cfrac{\chi \qquad\qquad [\neg\chi]^2}{\bot}\,\mathrm{MP}$$
$$\chi\,\mathrm{BO}-2$$

139♣ (Regel van Peirce.) Onderstel, dat $\Gamma, \varphi \to \psi \vdash \varphi$. Bewijs, dat $\Gamma \vdash \varphi$.

140♣ Vervang de afleidingsregel BO door de *dubbele negatie-regel* waarmee een afleiding met een conclusie $\neg\neg\varphi$ mag worden verlengd met de nieuwe conclusie φ. (Hierbij zijn de hypothesen van de nieuwe afleiding dezelfde als die van de oude.) Toon aan, dat de afleidbaarheidsrelatie $\vdash$ door deze modificatie niet wordt gewijzigd.

7.4 Verband tussen Waarheid en Afleidbaarheid

Hieronder wordt bewezen, dat *geldigheid* (benadering via waarheidstafels) en *bewijsbaarheid* (benadering met afleidingen) voor de propositie-logica samenvallen. Dat afleidbare formules geldig zijn (Gevolg 7.14) heet *betrouwbaarheid* van het afleidingssysteem; dat er voor iedere geldige formule een afleiding is (Stelling 7.15) heet *volledigheid* van het afleidingssysteem.

Dergelijke resultaten bestaan ook voor het zgn. eerste-orde fragment (blz. 142) van de kwantor-logica. Het volledigheidsresultaat daar is van Gödel (*Volledigheidsstelling*, 1930).

7.4.1 Betrouwbaarheid

Waarheidswaarden aan propositieletters toekennen gebeurt met *waarderingen*:

7.9 Waarderingen. Een *waardering* is een functie die waarheidswaarden (W, O) toevoegt aan propositieletters.

7.10 Vervullen. Onderstel dat γ een waardering is voor de propositieletters in de formule φ. In Sectie 1.3.2 (zie blz. 9 e.v.) is uitgelegd hoe je met γ een waarheidswaarde voor φ berekent. Als φ de waarheidswaarde W krijgt onder de waardering γ, dan zeg je: γ *vervult* φ. De notatie hiervoor is: $\gamma \models \varphi$.
γ *vervult* een verzameling van formules Γ als hij iedere formule in Γ vervult. Notatie: $\gamma \models \Gamma$.

De volgende stelling zegt dat de afleidingsregels het vervuld zijn van hypothesen doorgeven aan de uit deze hypothesen afgeleide formules.

7.11 Stelling. *Iedere vervulling van de hypothesen van een afleiding vervult ook de conclusie.*

Bewijs. Laat $\mathcal{D}$ de betreffende afleiding zijn. Pas sterke inductie toe naar het aantal *stappen* van $\mathcal{D}$, dat is: het aantal keren dat er een afleidingsregel is gebruikt in $\mathcal{D}$. (Het aantal stappen van $\mathcal{D}$ is gelijk aan het aantal knopen van $\mathcal{D}$ *minus* het aantal bladeren van $\mathcal{D}$.) (In plaats van sterke inductie naar het aantal stappen kun je ook gewone inductie naar de *hoogte* van $\mathcal{D}$ toepassen — zie Definitie 6.13 blz. 76.)
Onderstel dat n het aantal stappen is van $\mathcal{D}$. Dat je inductie gebruikt betekent, dat je vrijelijk over de volgende *inductiehypothese* kunt beschikken:

Voor iedere afleiding met minder dan n stappen geldt, dat iedere vervulling van de hypothesen óók de conclusie vervult.

Onderscheid al naar gelang de laatst in $\mathcal{D}$ toegepaste regel. Iedere afleidingsregel vergt dus een afzonderlijk argument; je volgt a.h.w. de onderdelen van Definitie 7.1. Als voorbeeld volgen gevallen 1, 4 en 6 van deze definitie.
1. ($\mathcal{D}$ is rudimentair.)
$\mathcal{D}$ is een op zichzelf staande formule φ waarvan hypothese zowel als conclusie φ zelf zijn.
De claim voor dit geval ("iedere waardering die φ vervult, vervult φ") spreekt vanzelf.
4. (De laatst toegepaste regel in $\mathcal{D}$ is Modus Ponens.)
Onderstel dat $\mathcal{D} = \psi + \sum_{i=1,2} \mathcal{D}_i$, met $\mathcal{D}_1$ een afleiding van φ uit hypothesen Γ_1, en $\mathcal{D}_2$ een afleiding van $\varphi \to \psi$ uit hypothesen Γ_2. De hypothese-verzameling van $\mathcal{D}$ is $\Gamma := \Gamma_1 \cup \Gamma_2$.
Onderstel nu, dat $\gamma \models \Gamma$; aangetoond moet worden, dat $\gamma \models \psi$. De inductiehypothese impliceert dat $\gamma \models \varphi$ (want $\gamma \models \Gamma_1$ en $\mathcal{D}_1$ heeft minder stappen dan $\mathcal{D}$) en dat $\gamma \models (\varphi \to \psi)$ (want $\gamma \models \Gamma_2$ en $\mathcal{D}_2$ heeft minder stappen dan $\mathcal{D}$). Uit de waarheidstafel voor $\to$ is dan direct zichtbaar, dat $\gamma \models \psi$.
6. (De laatst toegepaste regel in $\mathcal{D}$ is Bewijs uit het Ongerijmde.)
Onderstel, dat $\mathcal{D} = \varphi + \mathcal{D}'$, $\mathcal{D}'$ een afleiding van $\bot$ uit $\Gamma \cup \{\varphi \to \bot\}$, Γ de hypothese-verzameling van $\mathcal{D}$.
Onderstel, dat $\gamma \models \Gamma$. Aangetoond moet worden dat $\gamma \models \varphi$. Neem eens aan (als hypothese voor een bewijs uit het ongerijmde), dat $\gamma \models \varphi$ *niet* geldt. Dan voorziet γ beide leden van de implicatie $\varphi \to \bot$ van de waarheidswaarde O, en dus geldt (waarheidstafel $\to$) $\gamma \models (\varphi \to \bot)$. Er geldt nu dat $\gamma \models \Gamma \cup \{\varphi \to \bot\}$. De inductiehypothese toepassend op $\mathcal{D}'$ (die één stap minder heeft dan $\mathcal{D}$) vind je dat $\gamma \models \bot$. Maar, dit is onmogelijk! ($\bot$ krijgt per definitie altijd waarheidswaarde O.) Dus, de onderstelling, dat $\gamma \models \varphi$ *niet* geldt moet worden verworpen, en daarom geldt $\gamma \models \varphi$.
(Dus, om in te zien dat BO betrouwbaar is, is een bewijs uit het ongerijmde geleverd.)

Zie verder Opgave 141 ⊣

141 ♣ Opgave. Maak het bewijs van Stelling 7.11 af.

7.12 Logisch Gevolg. φ heet een *logisch gevolg* van de formuleverzameling Γ als iedere waardering die alle formules van Γ vervult, tevens φ vervult. Notatie: $\Gamma \models \varphi$. (Verwar dit gebruik van $\models$ niet met dat voor de vervulbaarheidsrelatie.)
φ heet *logisch geldig* (vgl. Definitie 1.3.2, blz. 9), notatie: $\models \varphi$, als φ wordt vervuld door iedere waardering, d.w.z. als $\emptyset \models \varphi$.

Stelling 7.11 zegt dus dat de conclusie van een afleiding logisch volgt uit de hypothesen van de afleiding. Het afleidingsbegrip is kennelijk *betrouwbaar* in de zin dat uitsluitend logische gevolgen kunnen worden afgeleid:

7.13 Betrouwbaarheid. *Als* $\Gamma \vdash \varphi$, *dan* $\Gamma \models \varphi$.

Bewijs. Dit is niets anders dan een herformulering van Stelling 7.11. ⊣

7.14 Gevolg. *Iedere hypothese-vrij afleidbare formule is logisch geldig: als* $\vdash \varphi$, *dan* $\models \varphi$. ⊣

7.4.2 *Volledigheid

De *Volledigheidsstelling* is de omkering van de betrouwbaarheidsstelling.

Laat γ een waardering zijn zódat $Dom(\gamma)$ eindig is. Dus, γ voorziet slechts eindig veel propositieletters van waarheidswaarden W en O. Associeer met γ de verzameling

$$[\gamma] := \{A \in Dom(\gamma) \mid \gamma(A) = W\} \cup \{\neg A \mid A \in Dom(\gamma), \gamma(A) = O\}$$

van de propositieletters die door γ van W worden voorzien, en de *negaties* van de propositieletters die door γ van O worden voorzien. De verzameling $[\gamma]$ geeft een soort *beschrijving* van γ. Het resultaat van de volgende opgave is cruciaal in het volledigheidsbewijs. Hierbij heet γ een waardering *voor* φ als iedere propositieletter in φ element is van $Dom(\gamma)$. Alweer wordt gebruik gemaakt van het inductie principe uit het Hoofdstuk 6: Stelling 6.3.

142 ♣♣Opgave. Bewijs, m.b.v. inductie naar het aantal connectieven in de formule φ, dat voor iedere waardering γ voor φ geldt:

1. $\gamma \models \varphi \;\Rightarrow\; [\gamma] \vdash \varphi$,
2. $\gamma \not\models \varphi \;\Rightarrow\; [\gamma] \vdash \neg\varphi$.

Aanwijzing. De inductie heeft vier gevallen: twee basis-gevallen ($\varphi = \bot$ en φ een letter, aantal connectieven is 0) en de eigenlijke twee inductie gevallen (φ een conjunctie en φ een implicatie). Voor ieder van die vier gevallen moeten de twee beweringen 1 en 2 worden bewezen. Hier volgen een paar voorbeelden.

$\varphi = \bot$.

1. Voor geen enkele γ hebben we, dat $\gamma \models \bot$; dit geval spreekt dus vanzelf. ("Triviaal-ware" implicatie.)

2. $\neg\bot$ is een afkorting van $\bot \to \bot$. Volgens Opgave 129.1, (blz. 95) is *iedere* implicatie $\varphi \to \varphi$ hypothese-vrij afleidbaar, dus $\neg\bot$ óók. Maar dan geldt $[\gamma] \vdash \neg\bot$, ongeacht γ.

$\varphi = (\chi \to \psi)$.

1. Onderstel, dat $\gamma \models \chi \to \psi$. Dan geldt (waarheidstafel $\to$) dat $\gamma \not\models \chi$ of $\gamma \models \psi$. Volgens inductiehypothese (als γ waardering is voor $\chi \to \psi$, dan is γ óók waardering voor χ en voor ψ) kan aangenomen worden dat aan de implicaties 1 en 2 wordt voldaan door χ zowel als door ψ. Het eerste geval ($\gamma \not\models \chi$) levert dus, dat $[\gamma] \vdash \neg\chi$. Nu geldt, dat $\neg\chi \vdash (\chi \to \psi)$ (ga na). Dus, $[\gamma] \vdash (\chi \to \psi)$. Het tweede geval ($\gamma \models \psi$) levert, dat $[\gamma] \vdash \psi$. Maar, $\psi \vdash (\chi \to \psi)$ (ga na). Dus, wéér geldt $[\gamma] \vdash (\chi \to \psi)$.

2. Onderstel, dat $\gamma \not\models \chi \to \psi$. Dan geldt (waarheidstafel $\to$) dat $\gamma \models \chi$ en $\gamma \not\models \psi$. Wegens inductiehypothese geldt dan $[\gamma] \vdash \chi$ en $[\gamma] \vdash \neg\psi$. Maar, $\chi, \neg\psi \vdash \neg(\chi \to \psi)$ (ga na). Dus, $[\gamma] \vdash \neg(\chi \to \psi)$.

Merk op: voor de afleidingen van Opgave 142 heb je de regel Bewijs uit het Ongerijmde *niet* nodig.

Het volgende resultaat keert Gevolg 7.14 om.

7.15 Zwakke Volledigheid. *Iedere logisch geldige formule is hypothese-vrij afleidbaar:*

$$\models \varphi \;\Rightarrow\; \vdash \varphi.$$

143 ♣ *Opgave. Bewijs Gevolg 7.15.
Aanwijzing. Laat de formule φ logisch geldig zijn. Onderstel, dat V de verzameling van alle in φ optredende propositieletters is. Bewijs dat voor iedere waardering γ met $Dom(\gamma) \subset V$ geldt, dat $[\gamma] \vdash \varphi$. I.h.b. volgt hieruit, voor $\gamma = \emptyset$ de lege waardering, het gevraagde. Gebruik inductie (ditmaal het Principe 6.1 van volledige inductie, blz. 65) naar het aantal elementen van $V - Dom(\gamma)$. De basis van de inductie ($V - Dom(\gamma) = \emptyset$, $V = Dom(\gamma)$) is precies Opgave 142.1. De inductiestap maakt gebruik van Opgave 138.1, blz. 97. (Deze opgave gebruikt de regel Bewijs uit het Ongerijmde.)

7.16 Gevolg. *Als Γ eindig is en $\Gamma \models \varphi$, dan geldt $\Gamma \vdash \varphi$.*

144 ♣ Opgave. Bewijs Gevolg 7.16.
Aanwijzing. Inductie naar het aantal elementen van Γ. Gebruik Opgave 133.1, blz. 96.

N.B.: de *Sterke Volledigheidsstelling* is de omkering van Gevolg 7.13, dat voor *willekeurige* Γ:

$$\Gamma \models \varphi \;\Rightarrow\; \Gamma \vdash \varphi.$$

Een bewijs hiervan wordt niet gegeven.

7.17 Consistent, Vervulbaar. Laat Γ een verzameling formules zijn.

1. Γ heet *consistent* als $\Gamma \nvdash \bot$.
2. Γ heet *vervulbaar* als er een waardering is voor de propositieletters in de formules van Γ die Γ vervult.

Opgaven

145 ♣ Maak Opgave 131 *alsnog.*
Aanwijzing. Gebruik de theorie van deze sectie. Twee toepassingen van de Deductie-regel reduceren het probleem tot het vinden van een afleiding van φ uit hypothesen $(\varphi \to \psi) \to \psi$ en $\psi \to \varphi$. De vraag is nu: wat is de laatste regel van de gezochte afleiding? Een eerste (redelijke) gissing is: Modus Ponens. Bijvoorbeeld, φ volgt direct uit ψ en $\psi \to \varphi$. De laatste formule is immers al beschikbaar als hypothese. Resteert het probleem om een afleiding te vinden van ψ uit hypothesen $(\varphi \to \psi) \to \psi$ en $\psi \to \varphi$. Maar, zo'n afleiding bestaat niet! Dit is een direct gevolg van de Betrouwbaarheidsstelling en het feit dat de waardering W voor φ en O voor ψ de twee hypothesen vervult maar de gewenste conclusie niet. Andere toepassingen van Modus Ponens en Conjunctie-eliminatie zien er weinig belovend uit. Blijft over Bewijs uit het Ongerijmde. Dit levert een derde hypothese $\neg\varphi$. Inderdaad is het zo, dat $\bot$ logisch volgt uit deze drie hypothesen (ga na), *dus* kan het overblijvende deductieprobleem volgens de Volledigheidsstelling worden opgelost. (Begin met $\varphi \to \psi$ af te leiden uit $\neg\varphi$.)

146 ♣ Bewijs: een *eindige* formuleverzameling is consistent d.e.s.d.a. hij vervulbaar is.

147 ♣ ♣ Voer het disjunctieteken $\vee$ weer in als zelfstandig connectief. Bedenk afleidingsregels voor $\vee$ zódat voor de resulterende afleidbaarheidsnotie weer een Betrouwbaarheids- en een Volledigheidsresultaat gelden.

Aanwijzing. Zie de regels voor $\vee$ gegeven in Sectie 2.2, blz. 22.

Samenvatting

Belangrijkste begrippen:

- afleidingsregel, afleiding, hypothese, conclusie,
- afgeleide regel,
- betrouwbaarheid en volledigheid.

Vragen:

- hoe bewijs je betrouwbaarheid? volledigheid?

Literatuur

Een (moeilijk) boek over natuurlijke deductie is Prawitz' [12]. Natuurlijke deductie komt ook aan de orde in het algemene boek over logica van van Dalen, [2]. Voor de uitbreiding van het hier behandelde deductie-apparaat tot de hele *eerste-orde logica* (zie Hoofdstuk 10 blz. 142), met de bewijzen van betrouwbaarheid en volledigheid, zie Doets [5].

Hoofdstuk 8

Oneindige Verzamelingen

Eén van de grote ontdekkingen van Cantor is dat er oneindige verzamelingen van verschillende grootte zijn. Hierover gaat dit hoofdstuk.

8.1 Ongelijkmachtig

Herinner je Definitie 6.6: verzamelingen A en B heten *gelijkmachtig* als er een bijectie van A naar B is (notatie: $A \sim B$).

8.1 Hoogstens gelijkmachtig. A heet *hoogstens gelijkmachtig* met B als er een injectie is van A in B. Notatie: $A \preceq B$.

Voorbeeld. $\mathbb{Z} \preceq \mathbb{R}^+$.

8.2 Stelling. *Voor iedere oneindige verzameling A geldt:* $\mathbb{N} \preceq A$.

Bewijs. Onderstel, dat A oneindig is. Een injectie $h : \mathbb{N} \to A$ zoals gevraagd wordt als volgt geproduceerd. Merk op: $A \neq \emptyset$ (want $\emptyset$ is eindig). Je kunt dus een element $h(0) \in A$ kiezen. Nu is $A \neq \{h(0)\}$ (want $\{h(0)\}$ is eindig). Dus bestaat een element $h(1) \in A - \{h(0)\}$. Nu is $A \neq \{h(0), h(1)\}$, etc. Deze argumentatie voortzettend zie je, dat onderling verschillende elementen $h(0), h(1), h(2), \ldots$ van A kunnen worden gevonden; de bijbehorende functie h is dus een injectie. ⊣

Dus, de machtigheid van $\mathbb{N}$ is de kleinste onder die van de oneindige verzamelingen.

Opgaven

148 ♣ Bewijs:

1. $A \preceq A$,
2. $A \sim B \implies A \preceq B$,

3. $A \preceq B \ \wedge \ B \preceq C \Longrightarrow A \preceq C$,
4. $A \subset B \Longrightarrow A \preceq B$,

149 ♣♣ Bewijs de omkering van Stelling 8.2: als $\mathbb{N} \preceq A$, dan is A oneindig.
Aanwijzing. Zie het bewijs van Stelling 6.11, blz. 71. Een kleine modificatie hiervan (waarvoor op zijn beurt een modificatie nodig is van Opgave 90) toont aan dat voor alle n, $\mathbb{N} \not\preceq \{0, \ldots, n-1\}$; en hieruit volgt het gevraagde.

150 ♣ Laat $h : A \to A$ een niet-surjectieve injectie zijn. Bijvoorbeeld, $b \in A - Ran(h)$. Definieer $f : \mathbb{N} \to A$ door: $f(0) = b$, $f(n+1) = h(f(n))$. Dus bijvoorbeeld: $f(3) = h(f(2)) = h(h(f(1))) = h(h(h(f(0)))) = h(h(h(b)))$.
Bewijs, dat $f(n)$ verschilt van $f(0), \ldots, f(n-1)$ $(n \in \mathbb{N})$. (Inductie naar n.)
Conclusie: f is een injectie, en $\mathbb{N} \preceq A$.

151 ♣ Bewijs: als $\mathbb{N} \preceq A$, dan is er een niet-surjectieve injectie $h : A \to A$.

152 ♣ Bewijs: een verzameling is oneindig d.e.s.d.a. hij gelijkmachtig is met een echte deelverzameling van zichzelf.
Aanwijzing. Gebruik Stelling 8.2 en Opgaven 149, 150 en 151.

153 ♣ Onderstel, dat A eindig is en dat $f : A \to A$. Bewijs: f is surjectief d.e.s.d.a. f injectief is.
Aanwijzing. $\Leftarrow$: gebruik Opgaven 149 en 150.
$\Rightarrow$: neem (Lemma 5.17 blz. 59) een rechts-inverse van f en gebruik Lemma 5.14 (blz. 58) en $\Leftarrow$.

8.2 Aftelbaar

Het prototype van een *aftelbaar oneindige* verzameling is de verzameling van natuurlijke getallen $\mathbb{N}$.

8.3 Aftelbaar.

1. A heet *aftelbaar* als $A \preceq \mathbb{N}$
2. A heet *aftelbaar oneindig* als $A \sim \mathbb{N}$.

8.4 Aftelling. Een *aftelling* van de verzameling A is een surjectie $f : \mathbb{N} \to A$.

Dus, f is een aftelling van A als $A = \{f(n) \mid n \in \mathbb{N}\}$. Dat betekent: we kunnen alle elementen van A in een oneindig lange rij zetten (die misschien herhalingen bevat): $f(0), f(1), f(2), \ldots$

Opgaven

De enige aftelbare verzameling zonder aftelling is $\emptyset$:

154 ♣ Bewijs dat een verzameling aftelbaar is d.e.s.d.a. hij leeg is of een aftelling heeft.
Aanwijzing. Gebruik de theorie van links- en rechts-inversen.

155 ♣ Bewijs: een deel van een aftelbare verzameling is aftelbaar.

156 ♣ Bewijs:

1. $\mathbb{Z}$ (de verzameling van gehele getallen) is aftelbaar,
2. Een vereniging van twee aftelbare verzamelingen is aftelbaar.

8.5 Stelling. $\mathbb{N}^2 = \{(n,m) \mid n,m \in \mathbb{N}\}$ *is aftelbaar oneindig.*

Bewijs. Definieer $S(p) := \{(n,m) \mid n+m=p\}$.
De verzamelingen $S(p)$ zijn twee aan twee disjunct, en $\mathbb{N}^2 = S(0) \cup S(1) \cup S(2) \cup \ldots$ Verder heeft $S(p)$ precies $p+1$ elementen: $(0,p)$,$(1,p-1)$,...,$(p,0)$. Ga na, dat de functie $j : \mathbb{N}^2 \to \mathbb{N}$ gedefinieerd door $j(n,m) := \frac{1}{2}(n+m)(n+m+1)+n$ de paren van de achtereenvolgende $S(p)$ opsomt in de aangegeven volgorde, en dus een bijectie is. ⊣

8.6 Stelling. $\mathbb{Q}^+$ *is aftelbaar oneindig.*

Bewijs. Identificeer iedere $q \in \mathbb{Q}^+$ met het paar $(n,m) \in \mathbb{N}^2$ waarvoor geldt: $q = \frac{n}{m}$ en $\frac{n}{m}$ is onvereenvoudigbaar (n en m relatief priem). Gebruik nu Stelling 8.5 en Opgave 155. ⊣

157 ♣ Bewijs dat de verzameling van *alle* rationale getallen $\mathbb{Q}$ aftelbaar is.

8.3 Overaftelbaar

8.7 Kleinere machtigheid. *A heeft machtigheid kleiner dan B* als zowel $A \preceq B$ als $A \not\sim B$. Notatie: $A \prec B$.

Dus:

$$A \prec B \iff A \preceq B \wedge A \not\sim B.$$

Voorbeelden. $\{0,\ldots,n-1\} \prec \mathbb{N}$ (Stelling 6.11);
$\mathbb{N} \prec \mathbb{R}$ (Stelling 8.9).

Waarschuwing. Dat $A \prec B$ *impliceert* wèl, maar is *niet equivalent met*: er is een niet-surjectieve injectie van A in B.

Dat $A \prec B$ betekent per definitie: $A \preceq B$ èn $A \not\sim B$. Dat $A \preceq B$ houdt in, dat een injectie $f : A \to B$ bestaat. Dat $A \not\sim B$ impliceert, dat er geen bijectie is tussen A en B; i.h.b., dat zo'n injectie f geen bijectie kan zijn.

Tegenvoorbeelden voor het omgekeerde: (Voorbeeld 6.7) de opvolger-functie $n \longmapsto n+1$ is een niet-surjectieve injectie : $\mathbb{N} \to \mathbb{N}$, maar natuurlijk geldt niet, dat $\mathbb{N} \prec \mathbb{N}$; de identiteitsfunctie $1_{\mathbb{N}}$ is een niet-surjectieve injectie van $\mathbb{N}$ in $\mathbb{Q}$, maar er geldt niet (Opgave 157), dat $\mathbb{N} \prec \mathbb{Q}$.

8.8 Overaftelbaar. A heet *overaftelbaar* als $\mathbb{N} \prec A$.

Als alle oneindige verzamelingen aftelbaar waren — en dat idee zou je van Opgave 157 gekregen kunnen hebben — dan had dit hoofdstuk weinig om het lijf. De volgende stelling is een fundamentele ontdekking van Cantor.

8.9 Stelling. $\mathbb{R}$ *is overaftelbaar.*

Bewijs. (i) Dat $\mathbb{N} \preceq \mathbb{R}$ is duidelijk (Opgave 148.3, $\mathbb{N} \subset \mathbb{R}$). (ii) Aangetoond moet dus nog worden, dat er geen bijectie $h : \mathbb{N} \to \mathbb{R}$ bestaat. In feite is er zelfs geen *surjectie*. Dat wil zeggen:

Bewering. Bij iedere functie $h : \mathbb{N} \to \mathbb{R}$ bestaat een reëel getal r met $r \notin Ran(h)$.

Bewijs. Onderstel, dat $h : \mathbb{N} \to \mathbb{R}$. Schrijf ieder getal $h(n)$, gebruik makend van decimaalontwikkelingen, in de vorm $h(n) = p_n + 0, r_0^n r_1^n r_2^n \cdots$, met $p_n \in \mathbb{Z}$, $p_n \leqslant h(n) < p_n + 1$, en decimalen $r_i^n \in \{0, 1, 2, \ldots, 9\}$. (Dus bijvoorbeeld, $-\sqrt{2} = -2 + 0,15\cdots$) Kies, bij iedere n, een getal $r_n \in \{0, 1, 2, \ldots, 9\}$ met $r_n \neq r_n^n$. Het getal $r = 0, r_0 r_1 r_2 \cdots$ verschilt dan van $h(n)$ in de n-de decimaal $(n = 0, 1, 2, \ldots)$.

Maar, zelfs als $p_n = 0$, hieruit volgt niet noodzakelijk, dat $r \neq h(n)$: een reëel getal kan immers *twee* decimaal-ontwikkelingen hebben; bijvoorbeeld, $0,5000\cdots = 0,4999\cdots$. Een staart nullen vs. een staart negens is ook het enige geval waarbij zich dit (een reëel getal met twee decimaal-ontwikkelingen) voordoet. Dat probleem kan dus worden geëlimineerd door de nieuwe decimalen r_n verschillend van 0 en 9 te kiezen. ⊣

Een bewijs voor deze stelling dat niet van decimaal-ontwikkelingen gebruik maakt (maar van de "sup-eigenschap" van de ordening van reële getallen) staat in Hoofdstuk 10; zie Gevolg 10.16, blz. 145.

Herinner, dat $\wp(A) := \{X \mid X \subset A\}$ de collectie is van alle deelverzamelingen van A (Definitie 3.9, blz. 37). De machtsverzamelingoperatie levert op een directe manier verzamelingen van grotere machtigheid: dat is de inhoud van Stelling 8.10.

In het bizonder is het dus *niet* zo, dat alle overaftelbare verzamelingen gelijkmachtig met $\mathbb{R}$ zijn!

8.10 Stelling. (Cantor) $A \prec \wp(A)$.

Bewijs. (i) De injectie $a \mapsto \{a\}$ van A in $\wp(A)$ toont aan, dat $A \preceq \wp(A)$.
(ii) Om te laten zien, dat $A \not\sim \wp(A)$ wordt, net als in het vorige bewijs, bij een willekeurige functie $h : A \to \wp(A)$, een element $D \in \wp(A) - Ran(h)$ geproduceerd: dat bewijst dat zo'n functie nooit een surjectie — laat staan een bijectie — is. Een dergelijk element is hier zelfs heel simpel te beschrijven: neem $D := \{a \in A \mid a \notin h(a)\}$. Zou je hebben dat $D \in Ran(h)$, dan bestond een origineel $d \in A$ met $D = h(d)$. Er zijn dan twee mogelijkheden: $d \in D$, of $d \notin D$. Maar, als $d \in D$, dan geldt, wegens definitie van D, dat $d \notin h(d) = D$: tegenspraak. En als $d \notin D$ dan geldt wegens $D = h(d)$ ook $d \notin h(d)$, en dus $d \in D$ wegens definitie van D: eveneens een tegenspraak. Conclusie: zo'n origineel d kan niet bestaan, en $D \notin Ran(h)$. ⊣

8.11 Gevolg.

1. $\mathbb{N} \prec \wp(\mathbb{N}) \prec \wp(\wp(\mathbb{N})) \prec \cdots$,

2. er is geen verzameling van grootste machtigheid. ⊣

Zie evt. Opgave 170 voor een vervolg.

Opgaven

158 ♣ Bewijs:

1. $A \not\prec A$,
2. $A \preceq B \iff A \prec B \vee A \sim B$,
3. $A \prec B \wedge B \sim C \implies A \prec C$.
4. Wat is er fout aan het volgende "*bewijs*" voor $2 \Rightarrow ?$:
   Gegeven is dat $A \preceq B$. Laat $f : A \to B$ een injectie zijn.
   (a) f is (toevallig) surjectief. Dan geldt dat $A \sim B$.
   (b) f is niet surjectief. Dan geldt $A \not\sim B$, en dus $A \prec B$.

159 ♣ Bewijs: als A eindig is, dan geldt $A \prec \mathbb{N}$.
(De omkering geldt ook: zie Opgave 171.)

160 ♣ Bewijs dat het reële interval $(0, \frac{2}{9}] := \{r \in \mathbb{R} \mid 0 < r \leqslant \frac{2}{9}\}$ overaftelbaar is.

161 ♣ Definieer $h : A \to \wp(A)$ door $h(a) := \{a\}$. Bepaal $\{a \in A \mid a \notin h(a)\}$.

162 ♣ Bewijs dat een vereniging van aftelbaar veel aftelbare verzamelingen weer aftelbaar is.
Dus (*aftelbaar/overaftelbaar pigeon-hole principe*): als $f : A \to I$, A overaftelbaar en I aftelbaar, dan bestaan een overaftelbare $H \subset A$ en een $i \in I$ zódat voor alle $a \in H$, $f(a) = i$.

163 ♣♣ Bewijs, dat $\mathbb{N} \prec \mathbb{N}^{\mathbb{N}}$. ($\mathbb{N}^{\mathbb{N}}$ is de verzameling van alle functies : $\mathbb{N} \to \mathbb{N}$.)
Aanwijzing. Produceer, bij een willekeurige afbeelding $\phi : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$, een functie $f \in \mathbb{N}^{\mathbb{N}} - Ran(\phi)$.

164 ♣ Een reëel getal is rationaal precies dan als z'n decimaalontwikkeling vanaf een zekere decimaal gaat repeteren. (Gebruik de somformule voor convergerende meetkundige reeksen.) Onderstel nu, dat $h : \mathbb{N} \to \mathbb{Q}$ een *surjectie* is. Wat kun je zeggen over het bijbehorende getal r dat door het bewijs van Stelling 8.9 wordt geproduceerd?

8.4 De Cantor-Bernstein Stelling

De volgende stelling is een belangrijk hulpmiddel bij bewijzen dat verzamelingen gelijkmachtig zijn. (Overigens deugt de naam niet: het is geen stelling van Cantor, en Bernstein's poging tot een bewijs was fout. Het eerste correcte bewijs is van Dedekind.)

8.12 Stelling. (Cantor-Bernstein) $A \preceq B \ \wedge \ B \preceq A \implies A \sim B$.

Het bewijs hiervan wordt nog even uitgesteld.

8.13 Gevolg. $A \preceq B \preceq \cdots \preceq Y \preceq Z \preceq A \implies A \sim B \sim \cdots \sim Y \sim Z$.

165 ♣ Opgave. Bewijs Gevolg 8.13.

Hier is een voorbeeld van het gebruik van Gevolg 8.13.

8.14 Stelling. $\mathbb{R} \sim \wp(\mathbb{N})$.

Bewijs. Hieronder wordt bewezen, dat $\mathbb{R} \preceq \wp(\mathbb{Q}) \sim \wp(\mathbb{N}) \sim \{0,1\}^{\mathbb{N}} \preceq \mathbb{R}$. Gevolg 8.13 levert dan de gewenste conclusie. (I.p.v. het hele alfabet heb je voldoende aan de vier letters A t/m D.)
1. $\mathbb{R} \preceq \wp(\mathbb{Q})$. De afbeelding $r \longmapsto \{q \in \mathbb{Q} \mid q < r\}$ is een injectie van $\mathbb{R}$ in $\wp(\mathbb{Q})$. (Het is geen bijectie.) Injectiviteit volgt uit het feit, dat tussen iedere twee reële getallen een rationaal ligt. Zie voor een bewijs van dit resultaat Voorbeeld 10.14 op blz. 143. Het injectiviteitsbewijs gaat nu als volgt. Onderstel, dat $r, s \in \mathbb{R}$ verschillende reële getallen zijn. Bijvoorbeeld, $r < s$. Kies een rationaal p tussen r en s. Dan geldt dat $p \notin \{q \in \mathbb{Q} \mid q < r\}$ en $p \in \{q \in \mathbb{Q} \mid q < s\}$, dus $\{q \in \mathbb{Q} \mid q < r\} \neq \{q \in \mathbb{Q} \mid q < s\}$.
2. $\wp(\mathbb{Q}) \sim \wp(\mathbb{N})$. Kies een bijectie $h : \mathbb{Q} \to \mathbb{N}$ (Opgave 157, blz. 105). Dan is de afbeelding $X \longmapsto h[X]$ een bijectie tussen $\wp(\mathbb{Q})$ en $\wp(\mathbb{N})$ (Opgave 91, blz. 72).
3. $\wp(\mathbb{N}) \sim \{0,1\}^{\mathbb{N}}$. Zie Opgave 92.
4. $\{0,1\}^{\mathbb{N}} \preceq \mathbb{R}$. Voor een injectie van $\{0,1\}^{\mathbb{N}}$ in $\mathbb{R}$: voeg aan een element $h : \mathbb{N} \to \{0,1\}$ van $\{0,1\}^{\mathbb{N}}$ toe het getal (in het interval $[0, \frac{1}{8})$) met decimaalontwikkeling $0, h(0)h(1)h(2)\cdots$. ⊣

***Continuum probleem en -hypothese.**
Nu je gezien hebt, dat $\mathbb{N} \prec \mathbb{R}$, is een voor de hand liggende vraag, of er verzamelingen A zijn met $\mathbb{N} \prec A \prec \mathbb{R}$. Als dat zo is, dan bestaat ook een dergelijke $A \subset \mathbb{R}$ (ga na) — dat is: een *overaftelbare* verzameling reële getallen *niet* gelijkmachtig met $\mathbb{R}$. De vraag heet Cantor's *Continuum Probleem.* (*Continuum* is een duur woord voor de verzameling $\mathbb{R}$.) Cantor's *Continuum Hypothese* (CH) zegt, dat zo'n verzameling *niet* bestaat. De gebruikelijke verzamelingstheoretische axiomas zijn niet in staat, om het continuum probleem op te lossen. Gödel bewees in 1938 dat de axiomas CH niet kunnen *weerleggen.* Wat dat betreft behoort CH dus tot de mogelijkheden. Cohen bewees in 1963 dat de axiomas CH ook niet kunnen *bewijzen.* Wat de axiomas betreft zou de machtigheid van $\mathbb{R}$ zelfs immens groot kunnen zijn en zouden er willekeurig veel verzamelingen $A, B, C, \ldots \subset \mathbb{R}$ kunnen bestaan zódat $\mathbb{N} \prec A \prec B \prec C \prec \cdots \prec \mathbb{R}$. Zie Sectie 8.6 (blz. 113) voor meer informatie.

Nu komt het bewijs van de Cantor-Bernstein stelling. Het volgende voorbeeld illustreert de gebruikte truc.

Voorbeeld. De reële intervallen $[0,1]$ en $[0,1)$ zijn gelijkmachtig.
Probeer dit eerst zelf te bewijzen, voordat je verder leest! Het eenvoudigst lijkt het (omdat $[0,1]$ en $[0,1)$ maar één getal schelen) om zoveel mogelijk getallen van $[0,1]$ op zichzelf af te beelden. Het probleem is dan: wat moet de bijectie doen met het getal 1? Natuurlijk kun je 1 wel afbeelden op een getal $r \in [0,1)$, maar dan kun je r niet meer op zichzelf afbeelden, en dus is de moeilijkheid

alleen maar verschoven naar r. Het volgende bewijs laat zien, dat als je dit probleem voor je uit blijft schuiven, het "vanzelf" verdwijnt. (Deze strategie, die bij oneindige verzamelingen werkt, heeft in het dagelijks leven weinig succes.)

Bewijs. Neem een willekeurige *in*jectie $f : [0,1] \to [0,1)$; bijvoorbeeld, $f(x) := \frac{1}{2}x$. De volgende afbeelding $h : [0,1] \to [0,1)$ is nu een bijectie: h beeldt 1 af op $f(1) = \frac{1}{2}$, $\frac{1}{2}$ op $f(\frac{1}{2}) = \frac{1}{4}$, $\frac{1}{4}$ op $f(\frac{1}{4}) = \frac{1}{8}$ etc.; en verder neem je $h(r) = r$ voor alle andere getallen $r \neq 2^{-n}$ in $[0,1]$. ⊣

Dus, f zorgt voor een "opschuif-procedure" die het probleem-geval 1 verschuift naar $\frac{1}{2}$, $\frac{1}{2}$ naar $\frac{1}{4}$, etc. en zó het probleem tenslotte elimineert.

Dit voorbeeld kan als volgt worden gegeneraliseerd: $[0,1]$ wordt A, $[0,1)$ wordt B, en $A - B$ kan nu meer dan één element hebben. Het resultaat is het volgende lemma, het speciale geval van Cantor-Bernstein waarbij één van de injecties een identiteitsfunctie is.

8.15 Lemma. *Als $A \preceq B \subset A$, dan geldt $A \sim B$.*

Bewijs. Laat $f : A \to B$ een injectie zijn. De gezochte bijectie $h : A \to B$ doet het volgende. h beeldt elementen x van $A - B$, $f[A - B]$, $f[f[A - B]]$,... af op hun f-beeld $f(x)$, en laat andere elementen op hun plaats. Zie Opgave 167. ⊣

Bewijs van de Cantor-Bernstein Stelling 8.12.
Onderstel, dat $f : A \to B$ en $g : B \to A$ injecties zijn. Dan is $g \circ f : A \to g[B] \subset A$ een injectie. Volgens Lemma 8.15 geldt nu $A \sim g[B]$. Maar natuurlijk geldt ook, dat $g[B] \sim B$. Dus, $A \sim B$. ⊣

Opgaven

166 ♣ Bewijs de volgende variaties op het feit, dat $[0,1] \sim [0,1)$:

1. $[0,1] \sim [0, \frac{2}{3})$,
2. $\{(x,y) \mid x^2 + y^2 \leqslant 1\} \sim \{(x,y) \mid x^2 + y^2 < 1\}$,
3. $\{(x,y) \mid x^2 + y^2 \leqslant 1\} \sim \{(x,y) \mid |x|, |y| < \frac{1}{2}\}$.

167 ♣ Ga de détails van het bewijs van Lemma 8.15 na.

168 ♣♣ Laat $A \subset \mathbb{R}$ aftelbaar zijn. Bewijs, dat $(\mathbb{R} - A) \sim \mathbb{R}$.

8.16 Gevolg. $(\mathbb{R} - \mathbb{Q}) \sim \mathbb{R}$. ⊣

De verzameling van irrationale getallen is gelijkmachtig met $\mathbb{R}$. Netzo kan worden bewezen, dat de verzameling van *transcendente* reële getallen gelijkmachtig is met $\mathbb{R}$; i.h.b., dat er dus *veel* transcendente getallen zijn. (Een getal dat niet algebraïsch is heet *transcendent*. Een reëel getal is *algebraïsch* als het nulpunt is van een polynoom in één variabele met gehele coëfficienten. Er zijn aftelbaar veel dergelijke polynomen; ieder polynoom heeft hoogstens eindig veel nulpunten, en dus zijn slechts aftelbaar veel reële getallen niet transcendent. Maar bewijzen, dat *concrete* getallen als e en π transcendent zijn, is in de regel lastig.)

169 ♣ Bewijs:

1. $A \prec B \implies \neg(B \prec A)$,
2. $A \prec B \wedge B \prec C \implies A \prec C$,
3. $A \preceq B \wedge B \prec C \implies A \prec C$,
4. $A \prec B \wedge B \preceq C \implies A \prec C$.

Aanwijzing. Al deze implicaties eisen Stelling 8.12.

170 ♣ Bewijs, dat de machtigheid van de oneindige vereniging $\mathbb{N} \cup \wp(\mathbb{N}) \cup \wp(\wp(\mathbb{N})) \cup \cdots$ groter is dan die van de verzamelingen $\mathbb{N}$, $\wp(\mathbb{N})$, $\wp(\wp(\mathbb{N}))$, ... afzonderlijk.
Aanwijzing. Gebruik Gevolg 8.11.

171 ♣♣ Bewijs de omkering van Opgave 159: $A \prec \mathbb{N} \;\Rightarrow\; A$ is eindig.

172 ♣♣ Bewijs:

1. Iedere oneindige deelverzameling van $\mathbb{N}$ is aftelbaar oneindig,
2. A is aftelbaar oneindig d.e.s.d.a. A aftelbaar is *en* oneindig,
3. A is aftelbaar d.e.s.d.a. $A \sim \mathbb{N}$ of A is eindig.

173 ♣♣ Gegeven zijn een verzameling A en een ding $b \notin A$. Bewijs:

1. Als A oneindig is, dan geldt $A \sim A \cup \{b\}$.
2. Als A eindig is, dan geldt $A \not\sim A \cup \{b\}$.

174 ♣ Onderstel, dat $a_0, a_1, a_2, \ldots$ onderling verschillende elementen zijn van de verzameling A.

1. Beschrijf een bijectie tussen A en $A - \{a_0\}$.
2. Idem tussen A en $A - \{a_0, a_1\}$.
3. Idem tussen A en $A - \{a_1, a_3, a_5, \ldots, a_{2n+1}, \ldots\}$.

175 ♣♣ Bewijs: er is geen verzameling $\mathfrak{C}$ van verzamelingen met de eigenschap dat voor iedere verzameling A er een verzameling $A' \in \mathfrak{C}$ bestaat zódat $A \sim A'$.

8.5 *Kardinaalgetallen

Je hebt gezien (Stelling 6.8), dat $\sim$ een equivalentie is op de collectie van alle verzamelingen.

8.17 Kardinaalgetallen. (Russell) Een *kardinaalgetal* is een equivalentieklasse van $\sim$. Het *kardinaalgetal van* A is de equivalentieklasse $|A|$ van A modulo $\sim$.

Uit deze definitie volgt direct (vgl. Lemma 4.7, blz. 46):

8.18 Lemma. $|A| = |B| \iff A \sim B$. ⊣

— en dit is het enige dat in de praktijk van de notie *kardinaalgetal* wordt gebruikt.

Het kardinaalgetal $|\{0, \ldots, n-1\}|$ van de n-elementige verzamelingen wordt meestal geïdentificeerd met het getal n.

8.19 Alef-nul. $\aleph_0 := |\mathbb{N}|$.[1]

Het begrip van een *kardinaalgetal* kan worden beschouwd als een generalisatie van het begrip *natuurlijk getal* in de zin van: *aantal.* Je kunt de definities van som, product en macht op een natuurlijke manier uitbreiden voor kardinaalgetallen en rekenregels bewijzen die de bekende regels voor $\mathbb{N}$ generaliseren.

Zo geldt $|A| + |B| = |A \cup B|$ (als $A \cap B = \emptyset$: alleen als A en B disjuncte verzamelingen zijn van n resp. m elementen heeft hun vereniging $n + m$ elementen), $|A| \times |B| = |A \times B|$ (het product $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$ heeft $n \times m$ elementen als A en B n resp. m elementen hebben) en $|A|^{|B|} = |A^B|$ (de functieverzameling A^B heeft n^m elementen als A en B n resp. m elementen hebben — zie Opgave 79, blz. 63).
N.B.: deze vergelijkingen kunnen zelfs worden opgevat als ("representant-onafhankelijke": zie Opgave 185) *definities* van optelling, vermenigvuldiging en machtsverheffing van kardinaalgetallen: zie de discussie onder 5.18 blz. 62.

Onder deze definities geldt kennelijk (Stelling 8.14), dat $|\mathbb{R}| = 2^{\aleph_0}$.

Kardinaalgetallen worden *geordend* (voor de notie van een ordening, zie Sectie 9.2 blz. 119) door de door $\prec$ en $\preceq$ geïnduceerde relaties die eveneens worden aangegeven met $\prec$ en $\preceq$: $|A| \prec |B| \Leftrightarrow A \prec B$; $|A| \preceq |B| \Leftrightarrow A \preceq B$. (Weer wordt dit gerechtvaardigd m.b.v. 5.18.)

$\aleph_0$ staat aan het begin van de onafzienbare rij van oneindige kardinaalgetallen genaamd *alefs*: $\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\omega < \cdots$; ($\aleph_\omega$ is het kleinste kardinaalgetal groter dan alle $\aleph_n$).

Het gebruik van kardinaalgetallen levert soms verbluffend compacte bewijzen op. Een voorbeeld is de volgende stelling van Cantor. (In Cantor's opinie was dit een belangrijker resultaat dan Stelling 8.9, dat $\mathbb{N} \prec \mathbb{R}$; vermoedelijk omdat bekend was dat er geen *continue* bijecties zijn tussen $\mathbb{R}$ en $\mathbb{R} \times \mathbb{R}$. Nu wordt anders naar dit relatieve belang gekeken.)

8.20 Stelling. *Het Euclidische vlak is gelijkmachtig met* $\mathbb{R}$.

Bewijs. D.w.z.: er is een bijectie tussen de punten in het vlak — $\mathbb{R} \times \mathbb{R}$ — en die op een lijn — $\mathbb{R}$. Want:

$$\begin{aligned} |\mathbb{R} \times \mathbb{R}| &= |\mathbb{R}| \times |\mathbb{R}| \\ &= 2^{\aleph_0} \times 2^{\aleph_0} \\ &= 2^{\aleph_0 + \aleph_0} \\ &= 2^{\aleph_0} \\ &= |\mathbb{R}|. \end{aligned}$$

De derde gelijkheid gebruikt een rekenregel voor kardinaalgetallen die de bekende regel: $n^p \times n^q = n^{p+q}$ voor getallen generaliseert — zie Opgave 188, blz. 114; de vierde gelijkheid gebruikt, dat $\aleph_0 + \aleph_0 = \aleph_0$, vgl. Opgave 156, blz. 105. ⊣

[1] $\aleph$ (alef) is de eerste letter van het Hebreeuwse alfabet.

8.6 *Keuze-axioma

Herlees het bewijs van Stelling 8.2, blz. 103. Merk op, dat je daar oneindig vaak een element moet kiezen in een niet-lege deelverzameling van de verzameling A. Deze willekeur kan worden geëlimineerd als je een functie hebt die dat voor je doet. Het *keuze-axioma* zegt, dat zulke functies er altijd zijn.

8.21 Keuze-axioma. Het *Keuze-Axioma*, afgekort: AC (voor: *Axiom of Choice*), is de bewering dat er een *keuze-functie* is voor iedere verzameling C van niet-lege verzamelingen, d.i.: een functie σ met $Dom(\sigma) = C$ zodat voor alle $X \in C$: $\sigma(X) \in X$.

Neem nu, in het bewijs van Stelling 8.2, $C := \{X \subset A \mid X \neq \emptyset\}$. Laat σ een keuze-functie zijn voor C. Een injectie $f : \mathbb{N} \to A$ zoals gewenst wordt dan kennelijk gedefinieerd door de conditie $f(n) = \sigma(A - \{f(0), \ldots, f(n-1)\})$.

Het keuze-axioma is een belangrijk verzamelingstheoretisch instrument dat overal in de wiskunde opduikt, soms in vermomming (zie Sectie 10.6: het *Lemma van Zorn*). Hieronder volgen een aantal illustraties, die duidelijk maken dat AC zelfs in sommige eenvoudige situaties niet kan worden gemist.

Opgaven

176 ♣ Bewijs, m.b.v. AC, dat een product $\prod_{i \in I} X_i$ van niet-lege verzamelingen X_i niet-leeg is. (Feitelijk is dit niets anders dan een *herformulering* van AC.)

177 ♣ Laat V een verdeling zijn van A. Bewijs, dat $V \preceq A$.
Aanwijzing. Iedere keuze-functie voor V is een injectie als gezocht.

178 ♣ Bewijs: iedere surjectie $h : A \to B$ heeft een rechts-inverse. (Dit is Lemma 5.17, blz. 59.)
Aanwijzing. Neem een keuze-functie voor $\{h^{-1}[\{b\}] \mid b \in B\}$.

179 ♣ Onderstel, dat $h : A \to B$ een surjectie is. Bewijs, dat $B \preceq A$.
Aanwijzing. Zie 5.17 en 5.14, blz. 59/58.

180 ♣ Bewijs *zonder* AC: als een surjectie $h : A \to B$ bestaat, dan geldt $\wp(B) \preceq \wp(A)$.

181 ♣♣ Bewijs *zonder* AC: als A oneindig is, dan geldt $\mathbb{N} \preceq \wp(\wp(A))$.

Een belangrijk gevolg van het keuze-axioma is de zgn. *Trichotomiestelling*:

8.22 Trichotomie. *Voor iedere twee verzamelingen A en B geldt één van drieën: óf $A \sim B$, óf $A \prec B$, óf $B \prec A$.* ⊣

182 ♣ Bewijs deze stelling voor het speciale geval, dat $B = \mathbb{N}$.
Aanwijzing. Gebruik Stelling 8.2.

Het *idee* van het bewijs van Stelling 8.22 is hetzelfde als dat van Stelling 8.2, maar er komen een paar details bij. Voor een volledig bewijs, zie Opgave 330 blz. 153.

Het keuze-axioma impliceert verder nog, dat *ieder* oneindig kardinaalgetal voorkomt in de rij van alefs. I.h.b. moet dus $|\mathbb{R}| = 2^{\aleph_0}$ erin voorkomen. Het Continuum-probleem in een andere formulering is dus de vraag: wààr staat $|\mathbb{R}|$ in de rij van alefs? De stelling van Cantor zegt, dat $|\mathbb{R}| \neq \aleph_0$ ($|\mathbb{R}|$ staat niet op de eerste plaats). Cantor's Continuum Hypothese is equivalent met: $|\mathbb{R}| = \aleph_1$ ($|\mathbb{R}|$ staat op de tweede plaats). De gebruikelijk verzamelingstheoretische axiomas impliceren wel, dat bijvoorbeeld $|\mathbb{R}| \neq \aleph_\omega$ (dit volgt uit Opgave 198, blz. 114). Maar (volgens Gödel en Cohen), mogelijkheden als $|\mathbb{R}| = \aleph_1$ (CH), $|\mathbb{R}| = \aleph_{10^{10}}$, $|\mathbb{R}| = \aleph_{\omega+1}$ (de eerstvolgende aleph na $\aleph_\omega$) etc. worden door diezelfde axiomas *niet* uitgesloten.

183 ♣ Onderstel dat voor alle verzamelingen A en B geldt, dat: $A \preceq B$ of $B \preceq A$. Bewijs hieruit, dat de Trichotomiestelling geldt.

184 ♣ Als in dit hoofdstuk voor concrete verzamelingen A en B moest worden bewezen, dat $A \prec B$, dan bleek het altijd mogelijk te zijn om te bewijzen dat er geen surjectie van A op B was ($A = \mathbb{N}$, $B = \mathbb{R}$; $B = \wp(A)$).
Onderstel, dat $B \neq \emptyset$. Bewijs dat equivalent zijn:

1. $A \prec B$,
2. $A \preceq B$, en er is geen surjectie : $A \to B$,
3. er is geen surjectie : $A \to B$.

Aanwijzing. Gebruik het keuze-axioma, of een gevolg daarvan.

*Opgaven

De resultaten van de eerstvolgende drie opgaven zijn vaak nodig om de resterende te kunnen maken.

185 ♣ Onderstel, dat $A_1 \sim A_2$ en $B_1 \sim B_2$. Bewijs:

1. als $A_1 \cap B_1 = A_2 \cap B_2 = \emptyset$, dan $A_1 \cup B_1 \sim A_2 \cup B_2$,
2. $A_1 \times B_1 \sim A_2 \times B_2$,
3. ♣ $A_1^{B_1} \sim A_2^{B_2}$.

186 ♣ Onderstel, dat $A_1 \preceq A_2$ en $B_1 \preceq B_2$. Bewijs:

1. als $A_2 \cap B_2 = \emptyset$, dan $A_1 \cup B_1 \preceq A_2 \cup B_2$,
2. $A_1 \times B_1 \preceq A_2 \times B_2$,
3. $\wp(A_1) \preceq \wp(A_2)$,
4. ♣ als $A_2 \neq \emptyset$, dan $A_1^{B_1} \preceq A_2^{B_2}$.

187 ♣ Geef tegenvoorbeelden voor de volgende implicaties.

1. $A_1 \prec A_2 \;\Rightarrow\; A_1 \cup B \prec A_2 \cup B$ ($A_1 \cap B = A_2 \cap B = \emptyset$),

2. $A_1 \prec A_2 \Rightarrow A_1 \times B \prec A_2 \times B$,
3. $A_1 \prec A_2 \Rightarrow A_1^B \prec A_2^B$,
4. $A_1 \prec A_2 \Rightarrow B^{A_1} \prec B^{A_2}$.

188 ♣ Bewijs:

1. als $B \cap C = \emptyset$, dan $A^{B \cup C} \sim A^B \times A^C$,
2. $(A \times B)^C \sim A^C \times B^C$
3. ♣ $(A^B)^C \sim A^{B \times C}$.

189 ♣ Bewijs ($n \geqslant 1$):

1. $\{0,1\}^{\mathbb{N}} \sim \{0,\ldots,n\}^{\mathbb{N}} \sim \mathbb{N}^{\mathbb{N}} \sim \mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$,
2. $\{0,1\}^{\mathbb{R}} \sim \{0,\ldots,n\}^{\mathbb{R}} \sim \mathbb{N}^{\mathbb{R}} \sim \mathbb{R}^{\mathbb{R}} \sim (\wp(\mathbb{R}))^{\mathbb{R}} \sim (\mathbb{R}^{\mathbb{R}})^{\mathbb{R}}$.

190 ♣ Bewijs, dat voor alle $n \in \mathbb{N}^+$ geldt: $\mathbb{N}^n \sim \mathbb{N}$ (n.b.: $\mathbb{N}^{\mathbb{N}} \not\sim \mathbb{N}$) en $\mathbb{R}^n \sim \mathbb{R}$ (n.b.: $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$).

191 ♣ Welke twee van de volgende verzamelingen zijn gelijkmachtig? Welke niet?: $\wp(\mathbb{R})^{\wp(\mathbb{R})}$; $(\wp(\wp(\mathbb{R})))^{\mathbb{R}}$; $\wp(\mathbb{R})$; $\wp(\wp(\mathbb{R}))$.

192 ♣ Toon aan dat de volgende twee verzamelingen gelijkmachtig zijn:
a. $\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leqslant 1 \wedge y > 0\}$; b. $\{(x,y) \in \mathbb{R}^2 \mid 1 < y \leqslant 2\}$.

193 ♣ Ga na, welke paren onder de verzamelingen $\mathbb{R}$, $\mathbb{N}^{\mathbb{N}}$, $\mathbb{N}^{\mathbb{R}}$; $\mathbb{R}^{\mathbb{N}}$; $\mathbb{R}^{\mathbb{R}}$ en $\wp(\mathbb{R})$ gelijkmachtig zijn. Bewijs je antwoorden.

194 ♣ A, B en C zijn niet-lege verzamelingen.

1. Bewijs dat $A^B \times A^{\mathbb{N}} \preceq A^{B \times \mathbb{N}}$.
2. Geef een bewijs of een tegenvoorbeeld voor de bewering, dat $A^{B \times C} \sim A^{(B^C)}$.

195 ♣ Ieder van de volgende verzamelingen 1–4 is gelijkmachtig met één van de volgende drie: $\mathbb{N}$, $\mathbb{R}$ en $\mathbb{R}^{\mathbb{R}}$. Zeg met welke van de drie, en geef een argumentatie:
1. $\mathbb{Q} - \mathbb{Z}$, 2. $\wp(\mathbb{Q})$, 3. $\wp(\wp(\mathbb{N}))$, 4. $\{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x + y \in \mathbb{Q}\}$.

196 ♣ Bewijs dat voor iedere oneindige verzameling A geldt, dat $A \sim (A \cup \mathbb{N})$.

197 ♣ Bewijs:

1. als geldt dat $\mathbb{N} \prec A$, dan is geen enkele functie $f : \mathbb{N} \to A$ een surjectie,
2. als $A \neq \emptyset$ en geen enkele functie $f : \mathbb{N} \to A$ is surjectief, dan geldt $\mathbb{N} \prec A$.

(Als je Opgave 184 oploste ben je natuurlijk klaar. Zoniet: probeer dit tóch.)

198 ♣ 1. Bewijs: voor iedere verzameling A geldt: $A \prec \mathbb{N}^A$.
2. ♣(König-Zermelo) Gegeven zijn verzamelingen $A_0, A_1, A_2, \ldots$ zódat $A_0 \prec A_1 \prec A_2 \prec \ldots$. Laat $A := \bigcup_{n \in \mathbb{N}} A_n$ de vereniging zijn van alle A_n. Bewijs, dat $A \prec A^{\mathbb{N}}$. (Omdat $\mathbb{R} \sim \mathbb{R}^{\mathbb{N}}$ kan $\mathbb{R}$ dus geen vereniging zijn van aftelbaar veel verzamelingen van stijgende machtigheid. In een precieze zin is dit het sterkste resultaat dat de gewone verzamelingstheoretische axiomas over de machtigheid van $\mathbb{R}$ kunnen bewijzen.)
Aanwijzing. Toon aan — net als in het bewijs van de stelling van Cantor — dat geen enkele functie $F : A \to A^{\mathbb{N}}$ surjectief is. Ga eerst na, dat geen enkele functie $f : A_i \to A$ surjectief is.

199 ♣ Bewijs: als A oneindig is en B eindig, dan geldt $(A - B) \cup (B - A) \sim A$.

Samenvatting

Belangrijkste begrippen:

- basisrelaties: $\preceq$, $\prec$,
- aftelbaar, overaftelbaar.

Vragen:

- geef voorbeelden van aftelbare verzamelingen; bewijs hun aftelbaarheid,
- geef voorbeelden van overaftelbare verzamelingen; bewijs hun overaftelbaarheid,
- zijn alle overaftelbare verzamelingen gelijkmachtig met $\mathbb{R}$?
- wat is de Cantor-Bernstein stelling? bewijs?
- bewijs $\mathbb{R} \sim \wp(\mathbb{N})$.

Literatuur

Er is veel literatuur op het gebied van de verzamelingentheorie, op allerlei niveau. Al genoemd zijn van Dalen, Doets, de Swart [3] en Halmos [6]. Twee van de vele inleidingen op een hoger niveau in het Engels zijn Vaught [14] en Henle [7]. Een zeer gedétailleerde (moeilijke) behandeling is Levy [9]. De beste inleiding in de (moeilijke) theorie van de verzamelingstheoretische onafhankelijkheidsresultaten (zoals continuum- en Suslin probleem) is Kunen [8]. Tenslotte, zie Moore [10] over de geschiedenis van het keuze-axioma.

Hoofdstuk 9

Ordeningen

Met de gewone ordeningen op de getalsverzamelingen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$ (gewoonlijk allemaal met hetzelfde teken $<$ aangegeven) ben je vermoedelijk vertrouwd. Dit hoofdstuk gaat over relaties op willekeurige verzamelingen die overeenkomstige eigenschappen hebben: de *ordeningsrelaties*.

9.1 Eigenschappen van Relaties

(Her)lees Hoofdstuk 4 Sectie 4.2; i.h.b. Definities 4.2 en 4.3 blz. 43 e.v. De volgende definitie introduceert een aantal veel voorkomende eigenschappen van relaties. Drie ervan kwam je al eerder tegen (in Definitie 4.5, blz. 45); deze werden gebruikt om de notie van een equivalentierelatie te definiëren. Netzo worden andere combinaties gebruikt voor definities van de ordeningsbegrippen. Elk van deze eigenschappen kan worden uitgedrukt door een eenvoudige formule.

9.1 Definities. Onderstel dat R een relatie is op de verzameling A. R heet:

- *reflexief op* de verzameling A als geldt dat $\forall x \in A(xRx)$,
- *irreflexief* als $\forall x\,(\neg xRx)$,
- *symmetrisch* als $\forall x, y\,(xRy \Rightarrow yRx)$,
- *asymmetrisch* als $\forall x, y\,(xRy \Rightarrow \neg yRx)$,
- *antisymmetrisch* als $\forall x, y\,(xRy \wedge yRx \Rightarrow x = y)$,
- *transitief* als $\forall x, y, z\,(xRy \wedge yRz \Rightarrow xRz)$.

Voorbeelden. De volgende tabel zegt van een aantal concrete relaties of ze al dan niet de genoemde eigenschappen hebben. Hierin is:
• $\emptyset$ de lege relatie op $\mathbb{N}$,
• $\Delta = \Delta_{\mathbb{N}} = \{(n, n) \mid n \in \mathbb{N}\}$ de identiteitsrelatie op $\mathbb{N}$,
• $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ de grootste relatie op $\mathbb{N}$,

- $<$ en $\leqslant$, de gewone ordeningsrelaties op $\mathbb{N}$,
- en tenslotte is $\subset$ de inclusierelatie op $\wp(\mathbb{N})$.

eigenschap:	*wèl:*	*niet:*
reflexief (op $\mathbb{N}$ resp. $\wp(\mathbb{N})$)	Δ, $\mathbb{N}^2$, $\leqslant$, $\subset$	$\emptyset$, $<$
irreflexief	$\emptyset$, $<$	Δ, $\mathbb{N}^2$, $\leqslant$, $\subset$
symmetrisch	$\emptyset$, Δ, $\mathbb{N}^2$	$<$, $\leqslant$, $\subset$
asymmetrisch	$\emptyset$, $<$	Δ, $\mathbb{N}^2$, $\leqslant$, $\subset$
antisymmetrisch	$\emptyset$, Δ, $<$, $\leqslant$, $\subset$	$\mathbb{N}^2$
transitief	$\emptyset$, Δ, $\mathbb{N}^2$, $<$, $\leqslant$, $\subset$	

Antisymmetrie van $<$ op $\mathbb{N}$ en van Δ is weer een geval van een triviaal-ware implicatie. $n < m$ en $m < n$ kunnen niet tegelijkertijd gelden (asymmetrie!), dus $n < m \wedge m < n$ is onwaar (voor alle n en m), en daarmee is $n < m \wedge m < n \Rightarrow n = m$ *waar*!
N.B.: *irreflexief* is niet hetzelfde als *niet-reflexief*. De relatie $\emptyset$ is zowel irreflexief als reflexief op de verzameling $\emptyset$. De relatie $\{(0,0)\}$ is niet reflexief op de verzameling $\{0,1\}$, en ook niet irreflexief.
Merk op: *reflexiviteit* van een relatie is altijd reflexiviteit *met-betrekking-tot* een verzameling. Als $R \subset A^2$ en $A \subset B$ dan geldt ook $R \subset B^2$; maar als R reflexief is op A en $A \subset B$ dan hoeft R nog niet reflexief op B te zijn. Voor de andere hier geïntroduceerde begrippen is de onderliggende verzameling niet van belang.

Opgaven

200 ♣ Ga na: een relatie R op A is

1. reflexief op A d.e.s.d.a. $\Delta_A \subset R$,
2. irreflexief d.e.s.d.a. $\Delta_A \cap R = \emptyset$,
3. symmetrisch d.e.s.d.a. $R^* \subset R$ ($R^* := \{(a,b) \mid bRa\}$ — Definitie 4.4 blz. 44),
4. asymmetrisch d.e.s.d.a. $R \cap R^* = \emptyset$,
5. antisymmetrisch d.e.s.d.a. $R \cap R^* \subset \Delta_A$.

201 ♣ Bewijs:

1. iedere transitieve, irreflexieve relatie is asymmetrisch,
2. iedere asymmetrische relatie is irreflexief en antisymmetrisch,
3. $\emptyset$ is de enige relatie die irreflexief, symmetrisch en transitief is.
   D.w.z., bewijs: (i) $\emptyset$ is irreflexief, symmetrisch en transitief, en (ii) een niet-lege relatie kan niet tegelijk irreflexief, symmetrisch en transitief zijn.

Aanwijzing. Geen van deze bewijzen gaat (veel) verder dan propositie logica. Bijvoorbeeld, onderdeel 1 (het bewijsprobleem is — asymmetrie is gegeven door een universele kwantificatie van een implicatie — al gereduceerd d.m.v. $\forall$-introductie en deductieregel):

Gegeven: R is transitief, irreflexief, en aRb;
Te bewijzen: $\neg bRa$.
Bewijs: Stel dat bRa. Dan ...

202 ♣ Laat R een relatie zijn op de verzameling A. Dan zijn $R \cup \Delta_A$ en $R - \Delta_A$ ook relaties op A. Bewijs:

1. als R asymmetrisch is, dan is $R \cup \Delta_A$ antisymmetrisch,
2. als R antisymmetrisch is, dan is $R - \Delta_A$ asymmetrisch.

203 ♣ (Zie Opgave 42 blz. 49.) Tel het aantal symmetrische relaties, het aantal asymmetrische relaties en het aantal antisymmetrische relaties op een verzameling met n elementen.

9.2 Ordeningsrelaties

Iedere ordeningsrelatie komt in twee "verschijningen": de reflexieve- en de irreflexieve versie.

Bekijk bijvoorbeeld de bekende relaties $<$ en $\leqslant$ op $\mathbb{N}$.
Merk op: $<$ is irreflexief en transitief (en dus asymmetrisch: Opgave 201); $\leqslant$ is reflexief, antisymmetrisch en transitief. Verder hangen deze relaties nauw samen. Er geldt:

$$n < m \iff n \leqslant m \wedge n \neq m,$$

$$n \leqslant m \iff n < m \vee n = m.$$

Deze situatie is algemeen bij zgn. (partiële) ordeningsrelaties. Eerst volgen de definities voor deze twee typen van relaties, en daarna hun verband.

9.2 Ordeningen. Onderstel, dat $R \subset A^2$.

1. R heet een *reflexieve* of *zwakke* (*partiële*) *ordening van* A als R
   - reflexief op A is,
   - antisymmetrisch
   - en transitief.
2. R heet een *irreflexieve* of *stricte* (*partiële*) *ordening van* A als R
   - irreflexief is
   - en transitief,

   (en *dus* ook asymmetrisch: Opgave 201.)

Voorbeelden van reflexieve partiële ordeningen uit de tabel boven zijn: $\Delta_{\mathbb{N}}$ (op $\mathbb{N}$), $\leqslant$ (idem) en $\subset$ (op $\wp(\mathbb{N})$); voorbeelden van irreflexieve partiële ordeningen zijn hier: $\emptyset$ en $<$ (op $\mathbb{N}$).

De gewone irreflexieve ordeningen van $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$ worden allen, als gebruikelijk, met $<$ aangegeven; de reflexieve relaties met $\leqslant$.

Merk op: de *lege* relatie is een partiële ordening van $\emptyset$ die zowel reflexief als irreflexief is.

In het vervolg wordt met een *ordening* altijd een *reflexieve* of een *irreflexieve partiële ordening* bedoeld.

Het eenvoudige (bijectieve) verband tussen de twee typen (reflexief/irreflexief ordeningsrelaties op een verzameling A wordt gegeven door het volgende lemma, dat zegt dat het verschil tussen de twee uitsluitend bestaat uit het omvatten van, of disjunct zijn met, de identiteitsrelatie Δ_A $(= \{(a, a) \mid a \in A\})$.

9.3 Lemma.

1. *Als R een irreflexieve partiële ordening is van A, dan is $R \cup \Delta_A$ een reflexieve partiële ordening van A.*

2. *Als S een reflexieve partiële ordening is van A, dan is $S - \Delta_A$ een irreflexieve partiële ordening van A.*

Bewijs. Opgave 204. ⊣

Reflexieve/Irreflexieve Compagnon. Als R een irreflexieve ordening is van A, dan heet $R \cup \Delta_A$ de *reflexieve compagnon* van R; omgekeerd, als S een reflexieve ordening is van A, dan heet $S - \Delta_A$ de *irreflexieve compagnon* van S.

Notaties, Conventies, Spraakgebruik.
Als $\leqslant$ een ordening is van A dan wordt aan de struktuur $(A, \leqslant)$ ook wel als *ordening* gerefereerd. Als wordt gezegd dat A een *geordende* verzameling is, dan moet de bedoelde ordeningsrelatie uit de context blijken.
In het vervolg worden irreflexieve ordeningen vaak aangegeven met $<$ (maar ook met $<'$, $<_A$, $\prec$ e.d.) of met $>$ (resp., $>'$, $>_A$, $\succ$) en reflexieve ordeningen met $\leqslant$ ($\leqslant'$, $\leqslant_A$, $\preceq$) of met $\geqslant$ (resp., $\geqslant'$, $\geqslant_A$, $\succeq$). Verwar in zulke gevallen $\prec$ en $\preceq$ niet met de machtigheidsrelaties van Hoofdstuk 8!

Uitdrukkingen '$a < b$', '$a \prec b$' enz. worden dan uitgesproken als: "a is kleiner (evt.: in de zin van $<$, $\prec$) dan b", "b is groter (idem) dan a"; '$a \leqslant b$', '$a \preceq b$' als: "a is kleiner dan of gelijk aan b", enz.

Als in één context $<$ en $\leqslant$ partiële ordeningen zijn van éénzelfde verzameling A (irreflexief resp. reflexief), dan wordt altijd aangenomen, dat $\leqslant$ de reflexieve compagnon is van $<$ (en $<$ dus de irreflexieve compagnon van $\leqslant$). D.w.z., voor $a, b \in A$:

- $a \leqslant b \iff a < b \vee a = b$,
- $a < b \iff a \leqslant b \wedge a \neq b$

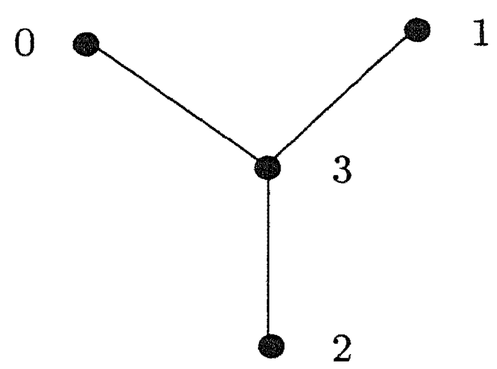
en netzo in het geval de andere notaties worden gebruikt. Verder worden de volgende afkortingen gehanteerd:

- $a \not\leqslant b \iff \neg a \leqslant b$,
- $a \not< b \iff \neg a < b$.

Plaatjes.
Partiële ordeningen op niet te grote, in ieder geval eindige, verzamelingen kunnen door een plaatje worden voorgesteld. De elementen van de verzameling worden dan weergegeven door punten; als $a < b$ geldt dan wordt b boven a getekend en met a verbonden door een lijntje. Een *pad* van lijnstukken telt nu ook als lijnstuk: wegens transitiviteit moet immers gelden, dat $a < b \wedge b < c \Longrightarrow a < c$. Dus, als al lijnstukken zijn getekend die a en b, resp. b en c verbinden, dan hoeft er geen extra lijnstuk meer te worden getekend tussen a en c.

Natuurlijk staat het plaatje van een irreflexieve ordening tegelijk voor de reflexieve compagnon.

9.4 Voorbeeld. Van de irreflexieve partiële ordening $\{(2,0),(2,1),(2,3),(3,0),(3,1)\}$ op de verzameling $\{0,1,2,3\}$ (maar tegelijk ook van zijn reflexieve compagnon
$\{(0,0),(1,1),(2,0),(2,1),(2,2),(2,3),(3,0),(3,1),(3,3)\}$) volgt hier het plaatje:



Opgaven

204 ♣ Bewijs Lemma 9.3.
Voorbeelden.
1: $R \cup \Delta_A$ is antisymmetrisch: onderstel, dat $a(R \cup \Delta_A)b$ (1) en dat $b(R \cup \Delta_A)a$ (2). Bewezen moet worden, dat $a = b$. (1) wil zeggen: aRb, of: $a\Delta_A b$, i.e., $a = b$. In het laatste geval ben je klaar; neem dus aan, dat aRb. Netzo zegt (2), dat bRa, of $b = a$; omdat je in het laatste geval weer klaar bent kun je onderstellen, dat bRa. Maar dat is onmogelijk, want R is asymmetrisch.
2: $S - \Delta_A$ is transitief: onderstel, dat $a(S-\Delta_A)b$ (1) en $b(S-\Delta_A)c$ (2). Bewezen moet worden, dat $a(S - \Delta_A)c$. Uit (1) volgt: aSb en $\neg a\Delta_A b$, d.w.z.: $a \neq b$. Netzo volgt uit (2) bSc en $\neg b\Delta_A c$, d.w.z.: $b \neq c$. Omdat S transitief is, volgt dat aSc. Resteert $a \neq c$: onderstel, dat $a = c$. Dan geldt (wegens aSb) dat cSb, en met bSc en antisymmetrie S: $b = c$. Tegenspraak.

205 ♣ Herinner, dat $R^* := \{(a,b) \mid bRa\}$ de inverse is van R (Definitie 4.4 blz. 44). Ga na: een relatie R op A is symmetrisch d.e.s.d.a. $R \subset R^*$ (d.e.s.d.a. $R = R^*$), asymmetrisch d.e.s.d.a. $R \cap R^* = \emptyset$, en antisymmetrisch d.e.s.d.a. $R \cap R^* \subset \Delta_A$.

206 ♣ Teken (graag: mooie) plaatjes van $(\wp(\{0\}), \subset)$, $(\wp(\{0,1\}), \subset)$, en van $(\wp(\{0,1,2\}), \subset)$.

207 ♣ Tel het aantal (zeg: irreflexieve) partiële ordeningen op een verzameling met resp. 0, 1, 2 en 3 elementen.

De relatie $\preceq$ tussen verzamelingen ("A heeft machtigheid hoogstens die van B") is een quasi-ordening (op de klasse van alle verzamelingen) (Definitie 6.18 blz. 82): reflexief en transitief. De relatie is niet antisymmetrisch. De bijbehorende relatie tussen kardinaalgetallen *is* een partiële ordening. De volgende opgave generalsieert dit.

208♣ Laat $\preceq$ een quasi-ordening zijn van Q. Definieer de relatie $\sim$ op Q door $q \sim q' :\equiv q \preceq q' \wedge q' \preceq q$.

1. Bewijs dat $\sim$ een equivalentierelatie is op Q.
2. Bewijs dat een relatie $\leqslant$ kan worden gedefinieerd op het quotient $Q/\sim$ zódat $|q| \leqslant |q'| \Leftrightarrow q \preceq q'$.
3. Bewijs dat $\leqslant$ een partiële ordening is van $Q/\sim$.

9.3 Isomorfie

Waarschijnlijk heb je bij het laatste onderdeel van Opgave 207 (tellen van het aantal ordeningen op een 3-elementige verzameling) de verschillende ordeningen ingedeeld al naar gelang hun plaatje. Op de verzameling $\{1,2,3\}$ heb je (i) de lege ordening; (ii) 6 ordeningen met hetzelfde plaatje als $\{(1,2)\}$; (iii) 3 ordeningen met hetzelfde plaatje als $\{(1,2),(1,3)\}$; (iv) idem voor $\{(2,1),(3,1)\}$; en tenslotte, (v) 6 ordeningen met hetzelfde plaatje als $\{(1,2),(1,3),(2,3)\}$; in totaal $1+6+3+3+6=19$ ordeningen.

Ordeningen heten *isomorf* als ze door eenzelfde plaatje kunnen worden voorgesteld. Dit is niet heel precies uitgedrukt; en bovendien: oneindige ordeningen hebben (tenzij in een geïdealiseerde zin) geen plaatje en kunnen toch isomorf zijn. Hier is de definitie.

9.5 Isomorfie. Onderstel dat $\mathcal{A} = (A, <)$ en $\mathcal{B} = (B, \prec)$ ordeningen zijn (reflexief dan wel irreflexief).

1. Een afbeelding $h : A \to B$ heet een *isomorfisme* of *isomorfie* tussen $\mathcal{A}$ en $\mathcal{B}$ als
   - h een bijectie is,
   - voor alle $a, a' \in A$: $a < a' \iff h(a) \prec h(a')$.

   Een isomorfisme tussen $\mathcal{A}$ en $\mathcal{A}$ heet een *automorfisme* van $\mathcal{A}$.
2. $\mathcal{A}$ en $\mathcal{B}$ heten *isomorf* als er een isomorfisme tussen hen is.
   Notatie: $\mathcal{A} \cong \mathcal{B}$.

9.6 Voorbeeld. Zie de partiële ordening van Voorbeeld 9.4, blz. 121. De ordening $\{(3,4),(3,1),(3,2),(4,1),(4,2)\}$ van $\{1,2,3,4\}$ heeft hetzelfde plaatje. (Tekenen!) Een isomorfisme tussen deze twee ordeningen is de functie $\{(0,1),(1,2),(2,3),(3,4)\}$. Een ander isomorfisme is $\{(0,2),(1,1),(2,3),(3,4)\}$.

Voor andere voorbeelden, zie Opgaven 210 en 217.

Omdat een isomorfie een bijectie is, zijn isomorfe ordeningen altijd gelijkmachtig. Dus geldt bijv., dat $(\mathbb{R}, <)$ niet isomorf is met $(\mathbb{N}, <)$ en niet met $(\mathbb{Q}, <)$. Maar, bijecties zijn natuurlijk niet altijd isomorfismen. Zo zijn de gelijkmachtige ordeningen $(\mathbb{N}, <)$ en $(\mathbb{Q}, <)$ niet isomorf: zie Opgave 211, blz. 123.

1_A is (altijd) een automorfisme van $(A, <)$: het *triviale* automorfisme.

9.7 Lemma. *De relatie $\cong$ is een equivalentie op de klasse van (reflexieve, resp., irreflexieve) ordeningen.*

Bewijs. Opgave 212. ⊣

Opgaven

209 ♣ De twee in Voorbeeld 9.6 gegeven isomorfismen zijn de enige isomorfismen tussen de betreffende ordeningen. Waarom is dat zo?

210 ♣ Bewijs:

1. $(\mathbb{N}, <) \cong (\mathbb{N}^+, <)$ (n.b.: $\mathbb{N}^+ := \{n \in \mathbb{N} \mid n > 0\}$),
2. $(\mathbb{R}, <) \cong (\mathbb{R}^+, <)$ (idem).

9.8 Voorbeeld. Een moeilijker geval van isomorfie is $(\mathbb{Q}, <) \cong (\mathbb{Q}^+, <)$. Waarschijnlijk werkt je oplossing voor Opgave 210.2 hier niet (omdat jouw isomorfisme geen rationaliteit bewaart). Een voorbeeld van een isomorfisme is de functie $f : \mathbb{Q} \to \mathbb{Q}^+$ gedefinieerd door:

$$f(q) = \begin{cases} q+1 & \text{als } q > 0 \\ \frac{1}{1-q} & \text{als } q \leqslant 0. \end{cases}$$

De functie f verschuift $\mathbb{Q} \cap (0, \infty)$ naar $\mathbb{Q} \cap (1, \infty)$ en comprimeert $\mathbb{Q} \cap (-\infty, 0]$ tot $\mathbb{Q} \cap (0, 1]$.

Nog moeilijker is het om te zien, dat $(\mathbb{Q}, <) \cong (\mathbb{Q} - \{0\}, <)$. (Zie Opgave 259 blz. 136.)

211 ♣ Bewijs, dat $(\mathbb{N}, <)$ en $(\mathbb{Q}, <)$ niet isomorf zijn.

212 ♣ Bewijs Lemma 9.7.

213 ♣ Geef (eenvoudige) ordeningen $(A, <)$ en $(B, \prec)$ en een bijectie $h : A \to B$ zódat voor alle $a, a' \in A$ geldt: $a < a' \;\Rightarrow\; h(a) \prec h(a')$, terwijl h *geen* isomorfie is. (Dus geldt niet voor alle $a, a' \in A$: $h(a) \prec h(a') \;\Rightarrow\; a < a'$.)

214 ♣ Geef (eenvoudige) ordeningen $(A, <)$ en $(B, \prec)$ en een surjectie $h : A \to B$ zódat voor alle $a, a' \in A$ geldt: $a < a' \;\Leftrightarrow\; h(a) \prec h(a')$, terwijl h *geen* isomorfie is. (Dus h is niet injectief.)

215 ♣ Toon aan: h is een isomorfisme tussen de irreflexieve partiële ordeningen $(A, <)$ en $(B, \prec)$ d.e.s.d.a. h een isomorfisme is tussen hun reflexieve compagnons $(A, \leqslant)$ en $(B, \preceq)$. (Het maakt dus niet uit voor de definitie of de reflexieve, dan wel irreflexieve ordeningsversies worden gehanteerd.)

Voor de formulering van de definitie van isomorfie 9.5 is het eigenlijk alleen van belang dat $<$ en $\prec$ relaties zijn; dat deze relaties ook nog ordeningen zijn doet niet terzake. Dus, een bijectie $h : A \to B$ heet ook een *isomorfie* tussen modellen $\mathcal{A} = (A, R)$ en $\mathcal{B} = (B, S)$ (waarbij $R \subset A^2$ en $S \subset B^2$) als voor alle $a, a' \in A$: $aRa' \iff h(a)Sh(a')$.

216 ♣ Onderstel, dat $h : A \to B$ een isomorfie is tussen $\mathcal{A} = (A, R)$ en $\mathcal{B} = (B, S)$. Bewijs:

1. Als R reflexief is op A, dan is S reflexief op B,
2. als R irreflexief is, dan is S irreflexief,
3. als R symmetrisch is, dan is S symmetrisch,
4. als R asymmetrisch is, dan is S asymmetrisch,
5. als R antisymmetrisch is, dan is S antisymmetrisch,
6. als R transitief is, dan is S transitief,
7. als R een (injectieve, surjectieve, bijectieve) functie van A naar A is, dan is S óók een (resp., injectieve, surjectieve, bijectieve) functie van B naar B.

Natuurlijk gelden van al deze implicaties ook de omkeringen; reden: Lemma 9.7.
Voorbeeld: 5.
Gegeven: Voor $b_1, b_2 \in B$ geldt zowel $b_1 S b_2$ als $b_2 S b_1$.
Te bewijzen: $b_1 = b_2$.
Bewijs: Kies (h surjectief) $a_1, a_2 \in A$ zódat $h(a_i) = b_i$ $(i = 1, 2)$. Er geldt (h isomorfisme) $a_1 R a_2$ en $a_2 R a_1$. Omdat R antisymmetrisch is, volgt dat $a_1 = a_2$. Dus, $b_1 = h(a_1) = h(a_2) = b_2$.

9.4 Definities en Opgaven

Herinner, dat $R^* := \{(a, b) \mid bRa\}$ de inverse is van R (Definitie 4.4 blz. 44).

9.9 Inversen. $(A, R)^* := (A, R^*)$.

In termen van plaatjes: $(A, R)^*$ is (A, R) "op z'n kop".

Notatie. Als in éénzelfde context $\leqslant$ en $\geqslant$ (en varianten als $\leqslant'$, $\geqslant'$; $\preceq$, $\succeq$, $\leqslant_A$, $\geqslant_A$) worden gebruikt voor reflexieve ordeningen op eenzelfde verzameling, dan wordt altijd aangenomen, dat $\leqslant^* = \geqslant$. Idem voor irreflexieve ordeningen $<$ en $>$ etc. (Dit sluit aan bij de notaties voor de gewone ordeningsrelaties van de bekende getalsverzamelingen.)

217 ♣ Bewijs:

1. $(\mathbb{Z}, <) \cong (\mathbb{Z}, <)^*$ (d.i.: $(\mathbb{Z}, <) \cong (\mathbb{Z}, >)$),
2. $(\mathbb{Q}, <) \cong (\mathbb{Q}, <)^*$,
3. $(\mathbb{R}, <) \cong (\mathbb{R}, <)^*$,
4. $(\wp(\mathbb{N}), \subset) \cong (\wp(\mathbb{N}), \subset)^*$.

218 ♣ Bewijs, dat $(\mathbb{N}, <) \ncong (\mathbb{N}, <)^*$.

219 ♣ Bewijs: de inverse van een (reflexieve, resp. irreflexieve) ordening is weer een (reflexieve, resp. irreflexieve) ordening.

220 ♣ Bewijs: ieder isomorfisme tussen $(A, <)$ en $(B, \prec)$ is óók een isomorfisme tussen $(A, <)^*$ en $(B, \prec)^*$.

9.10 Maximaal, Grootste. Laat $(A, \leqslant)$ een reflexieve partiële ordening zijn en $(A, <)$ de irreflexieve compagnon. Een element $a \in A$ heet

1. *maximaal* als geldt dat $\forall y \in A(a \leqslant y \Rightarrow a = y)$,
2. *grootste* of *laatste* element als geldt dat $\forall y \in A(y \leqslant a)$.

Merk op: maximaliteit van $a \in A$ is equivalent met: $\neg\exists y \in A(a < y)$ (ga na). D.w.z.: er is geen element in A, dat $<$-groter is dan a.

Verder: $a \in A$ is grootste element d.e.s.d.a. $\forall y \in A(y \neq a \Rightarrow y < a)$ (ga na).

In Voorbeeld 9.4, blz. 121, zijn 0 en 1 maximaal; er is geen grootste element. Een maximaal element is dus niet noodzakelijk grootste element.

221 ♣ Bewijs:

1. iedere ordening heeft hoogstens één grootste element,
2. een grootste element is altijd maximaal.
3. iedere niet-lege, *eindige* partiële ordening heeft tenminste één maximaal element.

222 ♣ Geef een voorbeeld van een partiële ordening met precies één maximaal element die geen grootste element heeft.

223 ♣ Onderstel, dat $h : A \to B$ een isomorfie is tussen de reflexieve ordeningen $(A, \leqslant)$ en $(B, \preceq)$. Bewijs:

1. als $a \in A$ maximaal is in $(A, \leqslant)$, dan is $h(a)$ maximaal in $(B, \preceq)$,
2. als $a \in A$ grootste element is van $(A, \leqslant)$, dan is $h(a)$ grootste element van $(B, \preceq)$.

224 ♣ Tegenover *maximaal* en *grootste* (*laatste*) staan *minimaal* en *kleinste* (*eerste*). Geef definities voor deze begrippen, zódat geldt: a is maximaal, resp. grootste element van $(A, \leqslant)$ d.e.s.d.a. a minimaal, resp. kleinste element is van $(A, \geqslant)$.

De lineaire ordeningen vormen een belangrijke ondersoort van de partiële ordeningen.

9.11 Lineaire Ordeningen. Een reflexieve ordening $\mathcal{A} = (A, \leqslant)$ heet *lineair* als geldt dat $\forall x, y \in A\,(x \leqslant y \vee y \leqslant x)$. Equivalent (in termen van de irreflexieve compagnon $<$): $\forall x, y \in A\,(x \neq y \Rightarrow x < y \vee y < x)$.

Dus: een ordening is lineair als iedere twee elementen vergelijkbaar zijn in de zin van de ordening. Lineariteit van ordeningen staat in zekere zin tegenover partialiteit; maar de terminologie is nu eenmaal zó, dat lineaire ordeningen speciale partiële ordeningen zijn: iedere lineaire ordening is ook een partiële ordening. Wèl duidt gebruik van het adjectief *partieel* in *partiële ordening* in de regel op niet-lineariteit: een lineaire ordening wordt nooit een partiële ordening genoemd, hoewel hij dat strict volgens de definitie dus wèl is.

Voorbeeld. De gewone ordeningen van $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$ zijn allen lineair.

De ordening van Voorbeeld 9.4 (blz. 121) is niet lineair: de elementen 0 en 1 zijn niet vergelijkbaar.

In een lineaire ordening is een element maximaal (resp., minimaal) d.e.s.d.a. het grootste (resp., kleinste) element is: ga na.

9.12 Eindpunten. Een *eindpunt* van een lineaire ordening is een kleinste of grootste element van die ordening.

225 ♣ Onderstel dat de irreflexieve partiële ordening $<$ van A lineair is. Bewijs dat $a \not< b \Leftrightarrow b \leqslant a$. Geef nauwkeurig aan, waar je de diverse eigenschappen van $<$ (irreflexiviteit, transitiviteit, lineariteit) gebruikt.

226 ♣ Laat $(A, <)$ een lineaire ordening zijn. Bewijs: er geldt dat $(A, <)^* = (A, <)$, d.e.s.d.a. A hoogstens één element heeft.

227 ♣ Gegeven is, dat $h : A \to B$ isomorfie is tussen de ordeningen $(A, <)$ en $(B, \prec)$, en dat $(A, <)$ lineair is. Bewijs, dat $(B, \prec)$ óók lineair is. (Dus: een lineaire ordening is nooit isomorf met een niet-lineaire ordening.)

228 ♣ Geef een eenvoudige nodige en voldoende voorwaarde op de verzameling A waaronder $\subset$ een lineaire ordening is van $\wp(A)$.

229 ♣ Bewijs dat de inverse van een lineaire ordening weer een lineaire ordening is.

230 ♣ Bewijs dat een element in een lineaire ordening kleinste (grootste) is d.e.s.d.a. het minimaal (resp. maximaal) is.

9.13 (Directe) Voorganger/Opvolger. In een irreflexieve partiële ordening $(A, <)$ heet $a \in A$ een *voorganger* van $b \in A$ en b een *opvolger* van a als $a < b$. Een element a heet een *directe voorganger* van b en b een *directe opvolger* van a als a een voorganger is van b en er verder geldt dat $\neg\exists c \in A(a < c \wedge c < b)$.

231 ♣ Onderstel, dat $a \in A$ directe voorganger is van $a' \in A$ in de partiële ordening $(A, <)$, en dat $h : A \to B$ isomorfie is tussen $(A, <)$ en $(B, \prec)$. Bewijs, dat $h(a)$ directe voorganger is van $h(a')$ in $(B, <)$.

232 ♣ De relatie $S = \{(0, 1), (0, 2)\}$ is een irreflexieve partiële ordening van de verzameling $A = \{0, 1, 2\}$. Geef alle lineaire ordeningen van A waarvan S een deelverzameling is.

Laat (A, S) nu een willekeurige, maar *eindige* partiële ordening zijn. Bewijs dat een lineaire ordening S^+ van A bestaat met $S \subset S^+$.

Aanwijzing. Inductie naar het aantal elementen van A.

N.B.: dit resultaat geldt ook voor *oneindige* partiële ordeningen: zie Opgave 329.

233 ♣ (Zie Opgave 213, blz. 123.) Bewijs: als $(A, <)$ een *lineaire* irreflexieve ordening is, $(B, \prec)$ een irreflexieve partiële ordening, en $h : A \to B$ een bijectie zódat voor alle $a, a' \in A$ geldt: $a < a' \Rightarrow h(a) \prec h(a')$, dan is h een isomorfie.

9.5 *Bomen als Partiële Ordeningen

Zie Definitie 6.13 blz. 76 voor de notie van een boom en aanverwante.

De volgende drie opgaven maken duidelijk dat bomen ook kunnen worden gedefinieerd als partieel geordende verzamelingen met een kleinste element waarvan voorgangerverzamelingen altijd eindig en lineair geordend zijn.

234 ♣ Onderstel, dat $(B, \prec, w)$ een boom is. Definieer de relatie $\leqslant$ op B door $a \leqslant b$ d.e.s.d.a. er een pad van a naar b is.
Bewijs: $\leqslant$ is een reflexieve partiële ordening van B zódat voor alle $b \in B$, $\{a \in B \mid a < b\}$ een eindige verzameling is die door $<$ lineair wordt geordend, en w is het $\leqslant$-kleinste element van B.

235 ♣ Onderstel dat $\leqslant$ is een reflexieve partiële ordening van B is zódat voor alle $b \in B$, $\{a \in B \mid a < b\}$ een eindige verzameling is die door $<$ lineair wordt geordend en dat $w \in B$ $\leqslant$-kleinste element is van B. Definieer $\prec$ op B door $a \prec b$ d.e.s.d.a. b directe $<$-opvolger is van a.
Bewijs dat $(B, \prec, w)$ een boom is.

9.6 Isomorfie en Equivalentie

In het voorgaande ben je verschillende instanties van het algemene verschijnsel tegen gekomen, dat isomorfe strukturen dezelfde eigenschappen hebben (*equivalent* zijn). (Zie Opgaven 216, 223, 227, 231) De volgende bewijs-loze "pseudo-stelling" vat dit samen. (*Pseudo*, want een bewijs wordt niet gegeven, en de "stelling" is bovendien niet eens waar!—zie hieronder.)

9.14 *Als* $\mathbf{A} \cong \mathbf{B}$ *en* $\mathbf{A}$ *heeft eigenschap* E*, dan heeft* $\mathbf{B}$ *eveneens eigenschap* E*.*

De contrapositie hiervan is misschien nog belangrijker. Die zegt: om te bewijzen dat twee strukturen niet isomorf zijn, is het voldoende één eigenschap op te sporen waarin ze verschillen.

Bijvoorbeeld, $(\mathbb{N}, <) \ncong (\mathbb{N}, >)$ (Opgave 218), want de eerste struktuur heeft een kleinste element en de tweede niet. (Weet je nog een andere, hier bruikbare, eigenschap?) En vermoedelijk was dit ook het idee achter je oplossing van Opgave 218.

Voor iedere "geschikte" eigenschap E levert het schema 9.14 een stelling. Het probleem is: wat is "geschikt"? In ieder geval zijn wèl geschikt eigenschappen als: hebben van een kleinste element, hebben van een element zonder directe voorganger, rigiditeit (zie Definitie 9.17, blz. 129, Opgave 246) etc.; maar bijv. *niet* de eigenschap, dat 0 element van de ordening is (waarom niet?).

In het algemeen kan worden gezegd, dat alle eigenschappen toelaatbaar zijn die formuleerbaar zijn in termen van de (ordenings) relatie(s) van de struktuur alléén.

236 ♣ **Opgave.** Bewijs, dat de volgende ordeningseigenschappen invariant zijn onder isomorfie — d.w.z.: toelaatbaar zijn in 9.14.

1. hebben van een kleinste element,

2. hebben van een maximaal element,
3. hebben van een element a zonder directe voorganger
   (d.w.z.: $\forall b < a\ \exists c < a\ (b < c)$),
4. de eigenschap dat ieder element een directe opvolger heeft.

Voorbeeld: uitwerking van onderdeel 3.
Gegeven: h is een isomorfie is tussen $(A, <)$ en $(B, \prec)$, $a \in A$ heeft geen directe voorganger.
Te bewijzen: B heeft een element zonder directe voorganger.
Bewijs. Voldoende is ($\exists$I), om te laten zien, dat $h(a)$ geen directe voorganger heeft. Dat gaat als volgt: Onderstel, dat $b \prec h(a)$. Gevraagd een element $c \in B$ zódat geldt $b \prec c \prec h(a)$. Zo'n element vind je als volgt. Onderstel, dat $b = h(b')$ (h is surjectief). Dan geldt $b' < a$ (h is een isomorfie). Omdat b' geen directe voorganger van a kan zijn bestaat een element $c' \in A$ met $b' < c' < a$. Maar dan geldt $h(b') = b \prec h(c') \prec h(a)$ (h is een isomorfie). $c := h(c')$ is dus het gezochte element.

9.7 Ordetype

Omdat $\cong$ een equivalentierelatie is op de klasse van ordeningen (Lemma 9.7) kun je equivalentieklassen vormen.

9.15 Ordetypen. Een *ordetype* is een equivalentieklasse van (zeg: irreflexieve) partiële ordeningen onder isomorfie.

Het ordetype van $\mathcal{A}$ wordt aangegeven door $|\mathcal{A}|$.

Dat betekent: $|\mathcal{A}|$ is de klasse van alle met $\mathcal{A}$ isomorfe ordeningen, en een ordetype is een klasse van de vorm $|\mathcal{A}|$, waarbij $\mathcal{A}$ een irreflexieve partiële ordening is. Het ordetype van de reflexieve compagnon $(A, \leqslant)$ van $(A, <)$ is per definitie gelijk aan dat van $(A, <)$.

Er geldt dus het volgende lemma (zie Lemma 4.7, blz. 46):

9.16 Lemma. *Voor ordeningen $\mathcal{A}$ en $\mathcal{B}$ geldt:*
$|\mathcal{A}| = |\mathcal{B}|$ *d.e.s.d.a.* $\mathcal{A} \cong \mathcal{B}$. ⊣

Notaties. (Zie het Griekse alfabet op blz. 159.)

- Ieder natuurlijk getal $n \in \mathbb{N}$ staat ook voor het ordetype van de lineaire ordeningen met n elementen (die zijn onderling isomorf!),
- $\omega := |(\mathbb{N}, <)|$,
- $\zeta := |(\mathbb{Z}, <)|$,
- $\eta := |(\mathbb{Q}, <)|$,
- $\lambda := |(\mathbb{R}, <)|$,
- als α het ordetype is van $(A, <)$, dan is α^* het ordetype van de inverse ordening $(A, <)^* = (A, >)$.

Je hebt gezien, dat $\eta^* = \eta$ (d.w.z.: $(\mathbb{Q}, <) \cong (\mathbb{Q}, >)$); $\lambda = \lambda^*$ ($(\mathbb{R}, <) \cong (\mathbb{R}, >)$) en $\zeta^* = \zeta$ ($(\mathbb{Z}, <) \cong (\mathbb{Z}, >)$). Verder zijn ω, ω^*, ζ, η en λ twee aan twee verschillend. (Voor $\omega \neq \omega^*$: zie Opgave 218, blz. 124, voor $\omega \neq \eta$: zie Opgave 211, blz. 123.)

Opgaven

237 ♣ Tel het aantal ordetypen van ordeningen op een verzameling met resp. 0, 1, 2, 3 en 4 elementen.
Aanwijzing. Maak plaatjes! Om alle 16 ordetypen van 4 elementen te vinden is enige systematiek gewenst.

238 ♣ Laat $(A, <)$ een irreflexieve partiële ordening zijn. Definieer $h : A \to \wp(A)$ door $h(a) := \{b \in A \mid b < a\}$. Bewijs dat h een isomorfie is tussen $(A, <)$ en $(Ran(h), \subset)$. (Dus: iedere partiële ordening is isomorf met de inclusie-relatie op een geschikte collectie van verzamelingen.)

239 ♣

1. Onderstel, dat $(A, \leqslant_1)$ en $(B, \leqslant_2)$ reflexieve partiële ordeningen zijn. Definieer de relatie $\preceq$ op $A \times B$ door

$$(a, b) \preceq (x, y) \equiv a \leqslant_1 x \wedge b \leqslant_2 y.$$

   Bewijs, dat $(A \times B, \preceq)$ een reflexieve partiële ordening is.
2. Teken een overzichtelijk plaatje van deze ordening voor het geval dat $A = \{0, 1, 2\}$ (met de gewone ordening: $0 < 1 < 2$) en $B = \{0, 1\}$ (idem).
3. Wat is het "plaatje" van deze ordening als $A = B = \mathbb{Z}$?

240 ♣

1. Gegeven zijn de reflexieve partiële ordening $(A, \leqslant)$ en de verzameling B. Op de verzameling A^B van alle functies $f : B \to A$ wordt de relatie $\preceq$ gedefinieerd door: $f \preceq g :\equiv \forall a \in A\, (f(a) \leqslant g(a))$. Bewijs, dat $\preceq$ een partiële ordening is van A^B.
2. Maak een overzichtelijk plaatje van deze ordening voor het geval, dat $A = \{0, 1, 2\}$ (met $0 < 1 < 2$) en $B = \{0, 1\}$.

241 ♣ Zie Opgave 240 voor de definitie van een partiële ordening $\preceq$ van A^B als $(A, \leqslant)$ een gegeven partiële ordening is en B een verzameling. Laat $\leqslant$ de gewone partiële ordening zijn van $A = \{0, 1\}$ (dus $0 < 1$). Bewijs, dat $(\{0, 1\}^B, \preceq) \cong (\wp(B), \subset)$.
Teken het plaatje van $(\{0, 1\}^B, \preceq)$ voor het geval, dat $B = \{0, 1, 2\}$.

242 ♣

1. Laat $h : A \to B$ een bijectie zijn. Bewijs dat de functie $H : \wp(A) \to \wp(B)$ gedefinieerd door $H(X) := h[X]$ een isomorfie is tussen $(\wp(A), \subset)$ en $(\wp(B), \subset)$.
2. Laat $H : \wp(A) \to \wp(B)$ een isomorfie zijn tussen $(\wp(A), \subset)$ en $(\wp(B), \subset)$. Bewijs dat een bijectie $h : A \to B$ bestaat zódat voor alle $X \subset A$: $H(X) = h[X]$.

9.17 *Rigiditeit. $\mathcal{A} = (A, <)$ heet *rigide* als 1_A het *enige* automorfisme is van $(A, <)$.

243 ♣ Laat zien, dat $(\mathbb{Z}, <)$ en $(\{x \in \mathbb{R} \mid 0 \leqslant x\}, <)$ *niet* rigide zijn.

244 ♣ Bewijs, dat $(\mathbb{N}, <)$ rigide is.

245 ♣ Bewijs: voor een element $f \in A^B$ in de ordening van Opgave 240.2 zijn equivalent:

1. voor ieder automorfisme π van A^B geldt $\pi(f) = f$,
2. $f(0) = f(1)$.

246 ♣ Gegeven is, dat $h : A \to B$ een isomorfie is tussen de ordeningen $(A, <)$ en $(B, \prec)$, en dat $(A, <)$ rigide is. Bewijs dat $(B, \prec)$ óók rigide is. (Dus: een rigide ordening is nooit isomorf met een niet-rigide ordening.)
Aanwijzing. Neem aan, dat $f : B \to B$ een automorfisme is van $(B, \prec)$ dat van 1_B verschilt. Laat zien, dat $h^{-1}fh : A \to A$ een automorfisme is van $(A, <)$ dat van 1_A verschilt.

247 ♣ Onderstel dat $(B, \prec)$ een partiële ordening is en $h : A \to B$ een bijectie. Gevraagd wordt een definitie te geven van een partiële ordening $<$ van A zódat h isomorfie is tussen $(A, <)$ en $(B, \prec)$.

248 ♣ Geef een (eenvoudig) voorbeeld van een eindige partiële ordening met precies 2 automorfismen. Geef er ook één met 4.

249 ♣♣ Geef (een plaatje van) een eindige partiële ordening met precies 3 automorfismen.

250 ♣ Bewijs dat iedere eindige lineaire ordening rigide is.

251 ♣♣ Bepaal de machtigheid van de verzameling van alle automorfismen van

1. $(\mathbb{Z}, <)$,
2. $(\mathbb{Q}, <)$,
3. $(\mathbb{R}, <)$.

252 ♣ Gegeven is een niet-triviaal automorfisme h van de lineaire ordening $(A, <)$. Definieer *oneindig veel* automorfismen van $(A, <)$. (Dus: iedere niet-rigide lineaire ordening heeft oneindig veel automorfismen.)

253 ♣ Geef een voorbeeld van een oneindige rigide lineaire ordening die niet isomorf is met $(\mathbb{N}, <)$ en ook niet met $(\mathbb{N}, >)$.

254 ♣♣ Gegeven is een oneindige lineaire ordening $(A, \prec)$. Bewijs: er is òfwel een oneindige *stijgende* rij $a_0 \prec a_1 \prec a_2 \prec \cdots$ in $(A, \prec)$, òfwel een oneindige *dalende* rij $\cdots \prec a_2 \prec a_1 \prec a_0$ in $(A, \prec)$. (Allebei kan natuurlijk óók.)
Aanwijzing. Behalve een direct bewijs is er ook een eenvoudige oplossing mogelijk d.m.v. Ramsey's stelling 6.12 (blz. 75). Kies willekeurig $b_0, b_1, b_2, \ldots \in A$ (Stelling 6.11). Verdeel de 2-elementige deelverzamelingen van $\mathbb{Z}$ in twee componenten: de paren $\{i, j\}$ met $(i < j)$ $b_i \prec b_j$, en die waarvoor $b_j \prec b_i$.

255 ♣♣ Gegeven is een oneindige partiële ordening $(A, \prec)$. Bewijs: er is een oneindige *stijgende* rij $a_0 \prec a_1 \prec a_2 \prec \cdots$ in $(A, \prec)$, of: er is een oneindige *dalende* rij $\cdots \prec a_2 \prec a_1 \prec a_0$ in $(A, \prec)$, of: er is een oneindige verzameling $B \subset A$ van twee aan twee onvergelijkbare elementen, d.i.: zódat voor alle $a, b \in B$: als $a \neq b$, dan geldt $a \not\prec b$ en $b \not\prec a$.

Samenvatting

Belangrijkste begrippen:

- irreflexief, asymmetrisch, antisymmetrisch,
- reflexieve/irreflexieve (partiële/lineaire) ordening,
- isomorfie,
- inverse, maximaal/minimaal, grootste/kleinste, (directe) opvolger/voorganger,
- ordetypen ω, ζ, η, λ.

Vraag:

- isomorfe strukturen hebben dezelfde eigenschappen; leg dit uit en geef voorbeelden.

Hoofdstuk 10

Ordeningen van $\mathbb{N}$, $\mathbb{Q}$ en $\mathbb{R}$

10.1 De Ordening van $\mathbb{N}$

De lineaire ordening $(\mathbb{N}, <)$ heeft een kleinste element 0, ieder element n heeft een directe opvolger $n+1$, en $(\mathbb{N} <)$ heeft de *inductie-eigenschap*, uitgedrukt door het Principe van Volledige Inductie 6.1 (blz. 65):

> Voor iedere verzameling $X \subset \mathbb{N}$ geldt:
> als $0 \in X$ en $\forall n \in \mathbb{N}(n \in X \ \Rightarrow \ n+1 \in X)$, dan geldt $X = \mathbb{N}$.

Deze drie eigenschappen *karakteriseren* de ordening $(\mathbb{N}, <)$ op isomorfie na:

10.1 Stelling. *Een lineaire ordening $(A, \prec)$ heeft type ω — d.i.: is isomorf met $(\mathbb{N}, <)$ — d.e.s.d.a.:*

1. *$(A, \prec)$ heeft een kleinste element 0_A,*
2. *ieder element $a \in A$ heeft een directe opvolger a^+, en*
3. *$(A, \prec)$ voldoet aan het inductie principe:*
   als voor $X \subset A$ geldt dat $0_A \in X$ en $\forall a \in A(a \in X \ \Rightarrow \ a^+ \in X)$, dan geldt $X = A$.

Bewijs. Nodig: zie Opgave 256.
Voldoende: Onderstel, dat $(A, \prec)$ de gestelde eigenschappen heeft. Definieer $h : \mathbb{N} \to A$ door de stipulatie, dat n wordt afgebeeld op de n-de directe opvolger van 0_A: $h(n) = 0_A^{+\cdots+}$ (n optredens van $^+$). Dus, $h(0) = 0_A$, $h(1) = 0_A^+$, $h(2) = 0_A^{++}$, etc. Het is duidelijk, dat h een injectie is die de ordening bewaart. Dat h een surjectie is volgt uit geldigheid van het inductie principe. Laat $X := Ran(h)$. Er geldt dat $0_A \in X$ en $\forall a \in A(a \in X \ \Rightarrow \ a^+ \in X)$, en dus (inductie) $Ran(h) = A$, d.w.z.: h is surjectief. ⊣

In Hoofdstuk 6 heb je gezien dat het principe van sterke inductie alles kan wat volledige inductie kan (en meer). Maar dit principe is niet in staat conditie

3 te vervangen in Stelling 10.1. Voorbeeld: definieer de lineaire ordening $\prec$ van $\mathbb{Z}$ door

$$n \prec m :\equiv (n, m \geqslant 0 \wedge n < m) \vee (n, m < 0 \wedge m < n) \vee (n \geqslant 0 \wedge m < 0).$$

In het "plaatje" van $(\mathbb{Z}, \prec)$ staan de natuurlijke getallen onderaan in hun *gewone* volgorde, gevolgd door de negatieve gehele getallen in *tegengestelde* volgorde: $0, 1, 2, \ldots, -1, -2, -3, \ldots$

Het ordetype van deze ordening is $\omega + \omega$ (zie Sectie 10.3 voor sommen van ordetypen). $(\mathbb{Z}, \prec) \ncong (\mathbb{N}, <)$.

De lineaire ordening $(\mathbb{Z}, \prec)$ heeft een kleinste element (0), ieder element n heeft een directe opvolger (t.w.: $n+1$ als $n \geqslant 0$, en $n-1$ als $n < 0$), en als voor een verzameling $X \subset \mathbb{Z}$ geldt dat $\forall n \in \mathbb{Z}(\forall m \prec n(m \in X) \Rightarrow n \in X)$, dan volgt noodzakelijk dat $\mathbb{Z} \subset X$ (ga na).

Door het principe van sterke inductie worden de zgn. *welordeningen* gekarakteriseerd (zie Sectie 10.5, i.h.b. Opgave 316).

Opgaven.

Het resultaat van de volgende opgave is weer een instantie van 9.14 (blz. 127).

256♣ Onderstel, dat $(A, \prec) \cong (\mathbb{N}, <)$. Bewijs, dat $(A, \prec)$ een kleinste element 0_A heeft, dat ieder element $a \in A$ een directe opvolger a^+ heeft, en dat $(A, \prec)$ voldoet aan het inductie principe: als voor $X \subset A$ geldt dat $0_A \in X$ en $\forall a \in A(a \in X \Rightarrow a^+ \in X)$, dan geldt $X = A$.

257♣♣ Produceer een karakterisering van de ordening $(\mathbb{Z}, <)$ in de geest van Stelling 10.1.

10.2 Ordening van $\mathbb{Q}$

De eigenschap van een lineaire ordening, *dicht geordend* te zijn, wordt gedefinieerd door de formule van blz. 3.

10.2 Dichtheid. De lineaire ordening $(A, <)$ heet *dicht*, en A heet *dicht geordend door* $<$, als tussen iedere twee elementen van A een derde ligt, d.w.z. als geldt dat $\forall x, z \in A\,[x < z \rightarrow \exists y \in A\,(x < y \wedge y < z)]$.

Voorbeelden. $(\mathbb{Q}, <)$ en $(\mathbb{R}, <)$ zijn dichte ordeningen. Bijvoorbeeld, als $p, q \in \mathbb{Q}$ en $p \neq q$, dan is het gemiddelde $\frac{p+q}{2}$ van p en q een rationaal tussen p en q.
Een eindige lineaire ordening is ("triviaal") dicht dan en slechts dan als hij 0 of 1 elementen heeft.
$(\mathbb{N}, <)$ is *niet* dicht geordend.

10.3 Stelling. (Cantor) *Een niet-lege lineaire ordening $(A, \prec)$ heeft type η — d.i.: is isomorf met $(\mathbb{Q}, <)$ — d.e.s.d.a. $(A, \prec)$:*

1. *eindpuntloos,*
2. *dicht, en*
3. *aftelbaar is.*

De conditie dat de ordening *niet-leeg* is moet er bij: de lege ordening is immers aftelbaar, dicht (!) en heeft geen eindpunten.

Bewijs. Dat ieder isomorf van $(\mathbb{Q}, <)$ aan de condities van de stelling voldoet, volgt uit o.m. Opgave 258.
Omgekeerd, onderstel dat $(A, \prec)$ aan de condities van de stelling voldoet. Kies (herhalings-vrije) aftellingen $A = \{a_0, a_1, a_2, \ldots\}$ en $\mathbb{Q} = \{q_0, q_1, q_2, \ldots\}$ van A resp. $\mathbb{Q}$.
De volgende argumentatie (een voorbeeld van de zgn. *héén-en-wéér-methode*) maakt van deze aftellingen gebruik om een isomorfisme tussen $(A, \prec)$ en $(\mathbb{Q}, <)$ te produceren van de vorm $h = \{(b_i, r_i) \mid i \in \mathbb{N}\}$.
Opdat een dergelijk construct een isomorfisme is moet kennelijk aan de volgende voorwaarden zijn voldaan:

1. $A = \{b_i \mid i \in \mathbb{N}\}$, $\mathbb{Q} = \{r_i \mid i \in \mathbb{N}\}$,
2. voor $i \neq j$ geldt
   - $b_i = b_j \Leftrightarrow r_i = r_j$,
   - $b_i \prec b_j \Leftrightarrow r_i < r_j$.

Om te zorgen dat aan conditie (1) wordt voldaan nemen we domweg altijd $b_{2k} = a_k$ en $r_{2k+1} = q_k$. De overige b_{2k+1} en r_{2k} worden in de volgorde $r_0, b_1, r_2, b_3, r_4, b_5, \ldots$ zorgvuldig zó gekozen, dat aan (2) wordt voldaan.
(Dit levert het *héén-en-wéér*-karakter van de constructie:
r_0 is *h-beeld* van $b_0 = a_0$,
b_1 is *h-origineel* van $r_1 = q_0$,
r_2 is *h-beeld* van $b_2 = a_1$,
b_3 is *h-origineel* van $r_3 = q_1$, etc.)
r_0:
Neem $r_0 = q_0$.
b_1:
Omdat $q_0 = r_0$ moeten we wegens eis (2) wel $b_1 = b_0 = a_0$ nemen.
Dat schiet niet echt op, maar straks wordt dat beter.
r_2:
Omdat de aftelling van A geen herhalingen heeft (dus $b_2 = a_1 \neq a_0 = b_0 = b_1$) en de ordening $\prec$ lineair is kunnen, voor de keuze van r_2, twee gevallen worden onderscheiden, al naar gelang de positie van b_2 t.o.v. $b_0 = b_1$.
(i) $b_2 \succ b_0 = b_1$.
Kies dan $r_2 > r_0 = r_1$. Dat kan, want $(\mathbb{Q}, <)$ heeft geen grootste element.
(Je kunt de keuze van r_2 éénduidig maken door bijvoorbeeld het eerste element in de aftelling van $\mathbb{Q}$ te nemen dat $> r_0$ is.)

(ii) $b_2 \prec b_0 = b_1$.
Neem dan $r_2 < r_0$.
b_3:
Voor de keuze van b_3 kunnen weer een aantal gevallen worden onderscheiden, al naar gelang de positie van r_3 t.o.v. $r_0 = r_1$ en r_2.
(i) $r_3 < r_0 = r_1, r_2$. Kies $b_3 \prec b_0 = b_1, b_2$. (Dat kan: $(A, \prec)$ heeft geen kleinste element.)
(ii) $r_3 = r_2$. Neem $b_3 = b_2$.
(iii) $r_3 > r_0 = r_1, r_2$. Kies $b_3 \succ b_0 = b_1, b_2$. ($(A, \prec)$ heeft geen grootste element.)
(iv) r_3 ligt tussen $r_0 = r_1$ en r_2. Kies b_3 tussen $b_0 = b_1$ en b_2. (Dat kan: $(A, \prec)$ is dicht.)
Het algemene patroon is hopelijk nu duidelijk. Bijvoorbeeld, voor het kiezen van b_{2i+1} wordt gekeken naar de ligging van $r_{2i+1} = q_i$ t.o.v. $r_0 = r_1, \ldots, r_{2i}$. Geldt $r_{2i+1} = r_j$ (voor een zekere $j = 0, \ldots, 2i$), dan is de keuze $b_{2i+1} = b_j$ onvermijdelijk; geldt $r_{2i+1} < r_0 = r_1, \ldots, r_{2i}$, kies dan (gebruikmakend van het feit dat A geen kleinste element heeft) $b_{2i+1} \prec b_0 = b_1, \ldots, b_{2i}$; geldt er $r_{2i+1} > r_0 = r_1, \ldots, r_{2i}$, kies dan (gebruikmakend van het feit, dat A geen grootste element heeft) $b_{2i+1} \succ b_0 = b_1, \ldots, b_{2i}$; en, in het overblijvende geval, geldt $r_j < r_{2i+1} < r_k$ (waarbij $j, k \leqslant 2i$ zódanig gekozen zijn dat voor $m = 0, \ldots, 2i$ hetzij $r_m \leqslant r_j$, hetzij $r_k \leqslant r_m$), kies dan (gebruikmakend van het feit dat $(A, \prec)$ dicht is) b_{2i+1} zódat $b_j \prec b_{2i+1} \prec b_k$. ⊣

Opgaven

258 ♣ Bewijs: een lineaire ordening die isomorf is met een dichte ordening, is óók dicht.

259 ♣ Ga na dat de verzamelingen $(0,1) \cap \mathbb{Q}$ en $\mathbb{Q} - \{0\}$, onder de gewone ordening, beide ordenings-isomorf zijn met $\mathbb{Q}$. (Bij de eerste is nog wel een isomorfisme aan te geven — zie Voorbeeld 9.8 blz. 123; voor de laatste lijkt het gebruik van Stelling 10.3 onvermijdelijk.)

260 ♣ Hoeveel ordetypen zijn er van lineaire ordeningen die zowel aftelbaar zijn als dicht?

10.4 *Beperking, Submodel, Inbedding. Laat $\mathcal{A} = (A, R)$ een model (Definitie 1.2, blz. 4) zijn, en $B \subset A$.
De *beperking van R tot B* is de relatie $R' := R \cap B^2$.
$\mathcal{B} = (B, S)$ heet een *submodel* van $\mathcal{A}$ als $B \subset A$ en S de beperking is van R tot B.
Een submodel van een ordening heet een sub-ordening of deel-ordening van die ordening.
Een *inbedding* van $\mathcal{B}$ *in* $\mathcal{A}$ is een isomorfisme tussen $\mathcal{B}$ en een submodel van $\mathcal{A}$. D.w.z., h is een inbedding van (B, S) in (A, R) als $h : B \to A$ een injectie is terwijl voor alle $b, b' \in B$ geldt: $bSb' \Leftrightarrow h(b)Sh(b')$.

Bij lineaire ordeningen wordt (in de notatie) vaak geen onderscheid gemaakt tussen een ordening en zijn beperkingen. Bijvoorbeeld, je schrijft: $(\mathbb{N}, <) \subset$

$(\mathbb{Z},<) \subset (\mathbb{Q},<) \subset (\mathbb{R},<)$, hoewel hier strict genomen $<$ voor *vier* verschillende lineaire ordeningen staat.

261 ♣ Bewijs: een submodel van een (lineaire) ordening is weer een (lineaire) ordening.

262 ♣♣ Laat $(A,\prec)$ een aftelbare lineaire ordening zijn. Bewijs: er is een inbedding van $(A,\prec)$ in $(\mathbb{Q},<)$.

10.5 *Notatie. Je schrijft $|\mathcal{A}| \leqslant |\mathcal{B}|$ als er een inbedding bestaat van $\mathcal{A}$ in $\mathcal{B}$.

Eigenlijk moet deze definitie/notatie worden gerechtvaardigd door te laten zien dat de vraag, of $|\mathcal{A}| \leqslant |\mathcal{B}|$, niet van de gekozen representanten $\mathcal{A}$ en $\mathcal{B}$ van de ordetypen $|\mathcal{A}|$ en $|\mathcal{B}|$ afhangt; zie 5.18 blz. 62. Dit komt neer op: als $\mathcal{A} \cong \mathcal{A}'$, $\mathcal{B} \cong \mathcal{B}'$ en $\mathcal{A}$ is inbedbaar in $\mathcal{B}$, dan is $\mathcal{A}'$ ook inbedbaar in $\mathcal{B}'$; en dat is niet moeilijk na te gaan.

Opgave 262 zegt, dat $\alpha \leqslant \eta$ geldt voor ieder aftelbaar ordetype α.

263 ♣♣ Onderstel, dat de lineaire ordening $(A,<)$ dicht is en minstens twee elementen heeft. Bewijs dat $(\mathbb{Q},<)$ kan worden ingebed in $(A,<)$.
Aanwijzing. Verwijder eerst evt. eindpunten van $(A,<)$. Ga na, dat een dichte ordening zonder eindpunten resteert. Het precieze bewijs vergt gebruik van het keuze-axioma.

264 ♣ Geef een verzameling $X \subset \mathbb{Q}^+$ van positieve rationale getallen zódat $(X,<)$ het type ζ van $(\mathbb{Z},<)$ heeft. (Met $<$ wordt de gewone ordening van $\mathbb{Q}$ resp. $\mathbb{Z}$ bedoeld.)

265 ♣♣ Beschrijf de verzameling $\{\alpha \mid \alpha \leqslant \omega\}$ van ordetypen. Idem: $\{\alpha \mid \alpha \leqslant \zeta\}$.

266 ♣ Onderstel, dat p en q twee rationale getallen zijn. Bewijs, dat een automorfisme h van $(\mathbb{Q},<)$ (dat is: een isomorfisme tussen $(\mathbb{Q},<)$ en zichzelf; zie Definitie 9.5 blz. 122) bestaat zódat $h(p) = q$.
Algemener: onderstel, dat $p_1 < \cdots < p_n$ en $q_1 < \cdots < q_n$ twee eindige rijtjes rationale getallen zijn van dezelfde lengte n. Bewijs, dat een automorfisme h van $(\mathbb{Q},<)$ bestaat zódat $h(p_i) = q_i$ $(i = 1,\ldots,n)$.

10.3 Geordende Sommen en Producten

Het plaatje van de geordende som $(A,<_A)+(B,<_B)$ van twee partiële ordeningen $(A,<_A)$ en $(B,<_B)$ krijg je op de volgende simpele manier: (i) teken het plaatje van $(B,<_B)$ boven dat van $(A,<_A)$, (ii) trek lijntjes zódat ieder element van A verbonden wordt met ieder element van B. Deze intuïtieve definitie werkt beter dan de volgende formele. Doe eerst eens Opgave 267!

10.6 Som van Ordeningen. Onderstel, dat $(A,<_A)$ en $(B,<_B)$ (partiële) ordeningen zijn zódat $A \cap B = \emptyset$. Definieer de relatie $<$ op $A \cup B$ door $< := <_A \cup <_B \cup (A \times B)$. De struktuur $(A \cup B,<)$ heet de *geordende som* van $(A,<_A)$ en $(B,<_B)$. Notatie: $(A,<_A)+(B,<_B)$.

De definitie van $<$ "handhaaft" de ordeningen $<_A$ en $<_B$ op A resp. B en maakt (wegens de component $A \times B$ in $<$) ieder element van A $<$-kleiner dan ieder element van B.
$(A,<_A)$ en $(B,<_B)$ zijn beide submodel van $(A,<_A)+(B,<_B)$.

Opgaven

267 ♣ Laat $A = \{1, 2, 3\}$, $<_A = \{(2, 1), (3, 1)\}$; $B = \{0\}$, $<_B = \emptyset$.
Bepaal $(A, <_A) + (B, <_B)$ en $(B, <_B) + (A, <_A)$. Merk op: deze modellen zijn niet isomorf. Maak plaatjes!

268 ♣ Een geordende som van lineaire ordeningen is weer een lineaire ordening.

269 ♣ Bewijs: als $(A, <) \cong (A', <')$, $(B, \prec) \cong (B', \prec')$ en $A \cap B = A' \cap B' = \emptyset$, dan geldt $(A, <) + (B, \prec) \cong (A', <') + (B', \prec')$.

Het resultaat van deze opgave rechtvaardigt de volgende definitie van som-van-ordetypen. Zie zonodig de discussie 5.18 blz. 62; merk op dat 5.18 hier geen volledige rechtvaardiging vormt vanwege de eis dat de gekozen representanten disjunct moeten zijn.

10.7 Som van Typen. $|(A, <_A)| + |(B, <_B)| := |(A, <_A) + (B, <_B)|$ (mits $A \cap B \neq \emptyset$).

D.w.z.: de som van twee ordetypen is het ordetype van de som van representanten van deze ordetypen. Maar: om deze representanten te kunnen sommeren, moeten ze disjunct zijn volgens Definities 10.6 en 10.7. Je kunt altijd representanten kiezen die disjunct zijn, en dus is de som van ordetypen altijd gedefinieerd.

Uit de definities is direct duidelijk, dat voor typen α, β en γ geldt, dat $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$. Daarom kun je haakjes in sommen weglaten.

Voorbeeld. $\zeta = \omega^* + \omega$. Want: $(\mathbb{Z}, <)$ is de geordende som van de ordening van de negatieve gehele getallen (en die heeft type ω^*) en $(\mathbb{N}, <)$.

270 ♣ Geef een verzameling $X \subset \mathbb{Q}^+$ van positieve rationale getallen zódat $(X, <)$ het type $\zeta + \zeta$ heeft. (Met $<$ wordt de gewone ordening van $\mathbb{Q}$ bedoeld.)

271 ♣ Ga na dat voor alle ordetypen α en β geldt, dat: $(\alpha + \beta)^* = \beta^* + \alpha^*$.

272 ♣ Laat $n \in \mathbb{N}^+$. Bewijs:

1. $n + \omega = \omega$,
2. $\omega + n \neq \omega + \omega^*$.

Aanwijzing. Kies concrete, simpele ordeningen van het betreffende ordetype. Bijv., $\{-n, \ldots, -1, 0, 1, 2, \ldots\}$ heeft, onder de gewone ordening, type $n + \omega$. In plaats van gelijkheid van typen bewijs je nu isomorfie; in plaats van ongelijkheid van typen bewijs je dat een isomorfisme niet bestaat.

273 ♣♣ Bewijs, dat $\eta + \lambda \neq \lambda + \eta$.

274 ♣♣

1. Geldt voor willekeurige ordetypen α, β en γ altijd de volgende implicatie: $\gamma + \alpha = \gamma + \beta \Rightarrow \alpha = \beta$? Zoja, bewijs dat; zonee, geef een tegenvoorbeeld.
2. Bewijs, dat $\omega + \alpha = \omega + \beta \Rightarrow \alpha = \beta$.

275 ♣ Bekijk de relatie $\prec$ op $\mathbb{Z}$ gedefinieerd door $n \prec m :\equiv n < m < 0 \ \vee \ 0 \leqslant n < m \ \vee \ m < 0 \leqslant n$. Bewijs, dat dit een lineaire ordening is van $\mathbb{Z}$. Beschrijf het ordetype van de ordening $(\mathbb{Z}, \prec)$.

276 ♣ Laat zien, dat $\eta + \eta$ het ordetype van $(\mathbb{Q} - \{0\}, <)$ is, en $\lambda + \lambda$ het ordetype van $(\mathbb{R} - \{0\}, <)$.
Wat is het ordetype van $(\mathbb{Z} - \{0\}, <)$?

277 ♣ Bewijs, dat: $\eta + \eta = \eta$, en dat: $\eta + 1 + \eta = \eta$.

In contrast: wèl geldt $\lambda + 1 + \lambda = \lambda$, maar $\lambda + \lambda \neq \lambda$, want ordeningen van type $\lambda + \lambda$ voldoen niet aan de "sup-eigenschap": zie Opgave 299 blz. 144.

10.8 *Gegeneraliseerde Som van Ordeningen. Onderstel, dat $(A, \prec)$ een lineaire ordening is, en dat voor iedere $a \in A$ een lineaire ordening $\mathcal{B}_a = (B_a, <_a)$ is gegeven, zódat de verzamelingen B_a twee aan twee disjunct zijn. Dan wordt met $\sum_{a \in A} \mathcal{B}_a$ de struktuur $\mathcal{B} = (B, <)$ bedoeld, waarbij $B = \bigcup_{a \in A} B_a$, en waarbij $<$ is gedefinieerd door $x < y :\equiv (\alpha_x \prec \alpha_y) \ \vee \ (\alpha_x = \alpha_y \ \wedge \ x <_{\alpha_x} y)$. Hierin is $\alpha : \bigcup_{a \in A} B_a \to A$ de functie die aangeeft tot welke B_a een element van $\bigcup_{a \in A} B_a$ behoort, d.w.z., waarvoor geldt dat $b \in B_{\alpha_b}$.
N.B.: merk op dat de som-notatie de ordening $\prec$ van A niet noemt hoewel die wel degelijk van belang is.
Een opsplitsing van $\mathcal{B}$ als $\mathcal{B} = \sum_{a \in A} \mathcal{B}_a$ in niet-lege deel-ordeningen $\mathcal{B}_a$ via een ordening $(A, \prec)$ heet een *condensatie* van $\mathcal{B}$. $|(A, \prec)|$ heet het *type* van de condensatie.
Als β_a het ordetype is van $\mathcal{B}_a$, dan wordt het ordetype van $\sum_{a \in A} \mathcal{B}_a$ aangegeven met $\sum_{a \in A} \beta_a$. (Zie, voor de rechtvaardiging hiervan, 5.18 blz. 62.)

Aanschouwelijk kan $\sum_{a \in A} \mathcal{B}_a$ verkregen worden gedacht door in $(A, \prec)$ ieder element a te vervangen door de corresponderende ordening $\mathcal{B}_a$. Op die manier ontstaat de som door alle ordeningen $\mathcal{B}_a$ achter elkaar te "lijmen" in de volgorde gegeven door (de elementen van) $(A, \prec)$.

Natuurlijk kan het weer voorkomen, dat je ordeningen wilt optellen die niet disjunct zijn. Strict volgens de definitie is dit onmogelijk. Om toch op te kunnen tellen moet je eerst disjuncte kopieën (isomorfen) nemen van de op te tellen ordeningen. De gewoonte is, om dat stilzwijgend te doen. Hoe je deze isomorfe kopieën kiest doet er feitelijk weinig toe: de uiteindelijke som is — tenminste, op isomorfie na — uniek bepaald. Als een uniforme oplossing voor het vinden van zulke kopieën zou je bijvoorbeeld kunnen nemen, om iedere $\mathcal{B}_a = (B_a, <_a)$ te vervangen door $(B_a \times \{a\}, <'_a)$ (de elementen van B_a zijn hier a.h.w. "gemerkt" met de index a), waarbij $<'_a$ is gedefinieerd door $(b_1, a) <'_a (b_2, a) :\equiv b_1 <_a b_2$. Dan is de uiteindelijke som niet een ordening van de vereniging $\bigcup_{a \in A} B_a$, maar van de verzameling paren $\{(b, a) \mid b \in B_a\}$.

278 ♣ ♣ Bewijs, dat een som $\sum_{a \in A} \mathcal{B}_a$ van lineaire ordeningen $\mathcal{B}_a$ via een lineaire ordening $(A, \prec)$ weer een lineaire ordening is.

De gewone geordende som is een speciaal geval van de gegeneraliseerde som:

279 ♣♣ Onderstel dat $\mathcal{B}_0$ en $\mathcal{B}_1$ lineaire ordeningen zijn. Ga na, dat (als je $\{0,1\}$ van de gewone ordening voorziet, waarbij dus $0 \prec 1$) $\mathcal{B}_0 + \mathcal{B}_1 = \sum_{i\in\{0,1\}} \mathcal{B}_i$.

10.9 *Convex. Een deelverzameling $X \subset B$ van een lineaire ordening $(B,<)$ heet *convex* als voor alle $a,b,c \in B$: als $a<b<c$ en $a,c \in X$, dan $b \in X$.

280 ♣♣ Bewijs: als $(B,<) = \sum_{a\in A}(B_a,<_a)$ een condensatie is van $(B,<)$, dan is $\{B_a \mid a \in A\}$ een verdeling (Definitie 4.9 blz. 47) van B in convexe verzamelingen.
Omgekeerd, laat $\mathcal{C}$ een verdeling zijn van B in convexe deelverzamelingen. Definieer de relatie $\prec$ op $\mathcal{C}$ door: $X \prec Y :\equiv \forall x \in X\, \forall y \in Y\, (x<y)$.
Bewijs: $\prec$ is een lineaire ordening van $\mathcal{C}$.
Bewijs: $(B,<) = \sum_{X\in\mathcal{C}}(X,<)$.
Concluderend: een condensatie is "hetzelfde" als een verdeling in convexe verzamelingen.

De volgende opgave geeft één manier om condensaties te produceren.

281 ♣ Gegeven is een lineaire ordening $\mathcal{B} = (B,<)$. Definieer de relatie $\sim$ op B door: $a \sim b :\equiv$ er liggen hoogstens *eindig veel* elementen van B tussen a en b. Bewijs: $\sim$ is een equivalentie met convexe equivalentieklassen.
Beschrijf de bijbehorende condensatie, i.h.b.: geef het ordetype van de verdeling, voor het geval dat (i) $\mathcal{B} = (\mathbb{Z},<)$, (ii) $\mathcal{B} = (\mathbb{Q},<)$, (iii) $|\mathcal{B}| = \zeta + \zeta$.

Een som van onderling gelijke ordeningen is een product:

10.10 *Product van Ordeningen. Het *product* van de lineaire ordeningen $(A,\prec)$ en $(B,<)$, $(B,<) \times (A,\prec)$ (let op de volgorde van de factoren!), is de gegeneraliseerde som $\sum_{a\in A}(B,<)$.
N.B.: alle op te tellen ordeningen zijn hier hetzelfde, en dus is van disjunctheid geen sprake. Er moeten daarom net zoveel onderling disjuncte kopieën van $(B,<)$ worden gebruikt als A elementen heeft.
Als α en β de ordetypen zijn van $(A,\prec)$ en $(B,<)$, dan wordt het ordetype van $(B,<) \times (A,\prec)$ aangegeven met $\beta \cdot \alpha$. Voor de rechtvaardiging hiervan: 5.18, blz. 62.
Tenslotte, $\alpha^2 := \alpha \cdot \alpha$.

282 ♣ Bewijs, dat $\eta \cdot \eta = \eta$.

283 ♣ Bewijs, dat (voor lineaire ordetypen α, β en γ):

1. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$,
2. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Geef een tegenvoorbeeld voor de andere distributie-wet $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$.

284 ♣ Noteer het type van de condensatie gedefinieerd in Opgave 281 van een lineaire ordening van type α door α/fin.
Bepaal ζ/fin, ζ^2/fin, ζ^3/fin, enz.
Definieer $\omega^\omega := \omega + \omega^2 + \omega^3 + \cdots$. Bepaal ω^ω/fin.

10.4 Ordening van $\mathbb{R}$

10.4.1 Ordeningsvolledigheid

Eén kenmerkende eigenschap van de ordening van de reële getallen is de *sup-eigenschap.*

10.11 Bovengrens, Supremum, Sup-eigenschap. Laat $(A, \leqslant)$ een lineaire ordening zijn en $X \subset A$. Een element $a \in A$ heet

1. *bovengrens* van X als $\forall b \in X(b \leqslant a)$,

2. *supremum* van X, notatie: $a = sup(X)$, als a de kleinste bovengrens is van X:
   $\forall b \in X(b \leqslant a) \wedge \forall a' \in A[\forall b \in X(b \leqslant a') \Rightarrow a \leqslant a']$.

$(A, \leqslant)$ heet *ordeningsvolledig* of *heeft de sup-eigenschap*, als iedere niet-lege deelverzameling van A die minstens één bovengrens heeft, ook een *sup* heeft.

Alle elementen van $\{0\} \cup \mathbb{R}^+$ zijn bovengrens van $X := \mathbb{R}^-$ in $(\mathbb{R}, <)$. Dus een verzameling kan veel bovengrenzen hebben. Maar van een *sup* is er hoogstens één: als a en a' beide *sup* zijn van X, dan geldt zowel $a \leqslant a'$ (a is kleinste onder de bovengrenzen, waaronder a') als $a' \leqslant a$ (idem) en dus geldt $a = a'$ wegens antisymmetrie.

Merk op: als $(A, <)$ een kleinste element heeft, dan is dit de *sup* van $\emptyset$; als $(A, <)$ een grootste element heeft, dan is dit de *sup* van A.

Voorbeelden. $(\mathbb{Q}, <)$ heeft de sup-eigenschap *niet*: denk aan bijv. $\{q \in \mathbb{Q} \mid q < \sqrt{2}\}$. Net zo geeft ieder irrationaal een voorbeeld van een begrensde, sup-loze deelverzameling van $\mathbb{Q}$.
$(\mathbb{R}, <)$ heeft wél de sup-eigenschap: dit is één van zijn twee typische kenmerken. Hier is een argument dat van decimaalontwikkelingen gebruik maakt. Onderstel, dat X een niet-lege verzameling reële getallen is met een bovengrens $b \in \mathbb{R}$. Schrijf ieder getal $r \in X$ in decimaal-notatie $n_r + 0, d_1^r d_2^r d_3^r \cdots$ waarbij $n_r \in \mathbb{Z}$ en $d_i^r \in \{0, \ldots, 9\}$. Laat $n := max\{n_r \mid r \in X\}$. (Dat maximum *bestaat*, want $n_r < b$.) Er kunnen erg veel $r \in X$ zitten waarvoor $n_r = n$. Van die r neem je nu het maximum van de eerste decimalen: $d_1 := max\{d_1^r \mid n_r = n\}$. (Dat maximum bestaat wéér, want $d_1^r \leqslant 9$.) Verder ziftend neem je de maximale tweede decimaal van de $r \in X$ waarvoor $n_r = n$ en $d_1^r = d_1$: $d_2 := max\{d_2^r \mid n_r = n \wedge d_1^r = d_1\}$. Etc. etc.; het getal $n + 0, d_1 d_2 d_3 \cdots$ dat zó wordt bepaald is (kennelijk) het gezochte supremum.
In Subsectie 10.4.4 zul je zien, dat je $(\mathbb{R}, <)$ verkregen kunt denken uit $(\mathbb{Q}, <)$ door het toevoegen van suprema voor niet-lege begrensde verzamelingen die zo'n supremum nog niet hadden.
Tenslotte, $(\mathbb{N}, <)$ en $(\mathbb{Z}, <)$ hebben de sup-eigenschap: zie Opgave 285.

Opgaven

285 ♣ Bewijs dat $(\mathbb{N}, <)$ en $(\mathbb{Z}, <)$ de sup-eigenschap hebben.
Aanwijzing voor $\mathbb{N}$: gebruik Opgave 87 blz. 70.

286 ♣ Definieer, duaal m.b.t. *bovengrens* en *supremum*, de begrippen *ondergrens* en *infimum* (*inf*).

10.12 Gaten. Een *gat* in een lineaire ordening $(A, <)$ is een tweetal niet-lege deelverzamelingen $L, R \subset A$ zódat $L \cap R = \emptyset$, $L \cup R = A$, $\forall a \in L\, \forall b \in R\, (a < b)$, waarbij L geen grootste- en R geen kleinste element heeft.

287 ♣ Bewijs: een lineaire ordening $(A, <)$ heeft de sup-eigenschap d.e.s.d.a. hij geen gaten heeft.

De sup-eigenschap is equivalent met de *inf-eigenschap*:

288 ♣ Bewijs: een lineaire ordening $(A, <)$ heeft de sup-eigenschap d.e.s.d.a. iedere niet-lege deelverzameling met ondergrenzen een *inf* heeft.

289 ♣♣ Twee isomorfe lineaire ordeningen hebben ofwel beide de sup-eigenschap, ofwel geen van beide. D.w.z., voor: E :=*sup-eigenschap*, wordt aan 9.14 (blz. 127 voldaan.

***Eerste-orde, tweede-orde en hogere-orde logica.**
Als de kwantoren van een formule variabelen binden die alleen naar *elementen* van (universa van) mogelijke strukturen verwijzen, dan heet die betreffende formule van *eerste-orde*. De theorie van eerste-orde formules is tamelijk overzichtelijk. In Hoofdstuk 9 zijn een aantal instanties van 9.14 ("isomorfe strukturen hebben dezelfde eigenschappen") opgenomen waarbij de cruciale eigenschap E uitgedrukt kan worden d.m.v. zo'n eerste-orde formule. Als er ook gekwantificeerd wordt over variabelen voor deelverzamelingen van (of zelfs relaties, functies over) het universum van in aanmerking komende strukturen, dan heb je te maken met een *tweede-orde* formule. Voor eigenschappen die door eerste- of zelfs tweede-orde formules worden uitgedrukt gaat 9.14 op. Voorbeelden van zulke eigenschappen zijn rigiditeit, de inductie-eigenschap, de sup-eigenschap, en separabiliteit. Zoals je zult merken (zie je oplossing voor Opgave 289) heb je voor de corresponderende instanties van 9.14 een nieuw bewijs-idee nodig. Behalve eerste- en tweede-orde eigenschappen zijn er ook nog derde-, vierde-... orde eigenschappen (het uitdrukken waarvan kwantificatie over variabelen voor collecties van deelverzamelingen e.d. eist), maar voorbeelden daarvan vind je hier niet. In tegenstelling tot de eerste-orde logica is de theorie van tweede- en hogere-orde logica minder ontwikkeld en zelfs, door haar essentieel verzamelingstheoretisch karakter, problematisch. Bijvoorbeeld: ieder betrouwbaar deductie-apparaat voor de tweede-orde logica is noodzakelijk onvolledig. (De begrippen *betrouwbaar* en *volledig* werden besproken in Sectie 7.4 in de context van de propositie-logica.) De eerste-orde logica heeft wèl een betrouwbaar en volledig deductie-apparaat (Dat is de inhoud van Gödel's volledigheidsstelling).

290 ♣ Bewijs, dat de ordeningen $(\mathbb{R}-\{0\},<)$ (ordetype $\lambda+\lambda$) en $(\mathbb{R},<)$ (ordetype λ) niet isomorf zijn. (Contrasteer dit met Opgave 259, blz. 136!)

291 ♣ Gegeven zijn twee disjuncte lineaire ordeningen $\mathcal{A}$ en $\mathcal{B}$ met de sup-eigenschap; $\mathcal{B}$ heeft bovendien een kleinste element. Bewijs dat $\mathcal{A}+\mathcal{B}$ óók de sup-eigenschap heeft.

10.4.2 Separabiliteit

De tweede kenmerkende eigenschap van de ordening van de reële getallen is *separabiliteit.*

10.13 Dicht-in, Separabel. Laat $\mathcal{A}=(A,<)$ een lineaire ordening zijn.

1. $D\subset A$ *ligt dicht in* of *is dicht in* de lineaire ordening $(A,<)$, als tussen iedere twee elementen van A een element van D ligt: $\forall a,a'\in A[a<a' \Rightarrow \exists x\in D(a<x<a')]$.

2. Een lineaire ordening heet *separabel* als hij een aftelbare, dichtliggende deelverzameling heeft.

Verwar *dichtheid-in* van een deelverzameling niet met dichtheid van de ordening *zelf.* (Zie Opgave 292.)

10.14 Voorbeeld. $\mathbb{Q}$ ligt dicht in de ordening van de reële getallen: tussen iedere twee reële getallen ligt een rationaal. $\mathbb{Q}$ is aftelbaar. Dus, de reële ordening $(\mathbb{R},<)$ is separabel. Het bizondere hieraan is, dat $\mathbb{R}$ overaftelbaar is.

Hier is een argument voor de separabiliteit van het reële interval $(0,1)$ dat van decimaal-ontwikkelingen gebruik maakt. Onderstel, dat p en q reële getallen in $(0,1)$ zijn zódat $p<q$. Gezocht wordt een rationaal r tussen p en q. Neem gemakshalve aan dat $0<p<q<1$. Onderstel, dat $p=0,p_1p_2p_3\ldots$ en $q=0,q_1q_2q_3\ldots$ decimaalontwikkelingen zijn van p en q. Er moet een eerste plaats zijn, waar deze verschillen; bijvoorbeeld, voor $i<n$ geldt nog, dat $p_i=q_i$, terwijl $p_n<q_n$. Als $p_n+1<q_n$, dan voldoet $r:=0,p_1p_2\ldots p_{n-1}(p_n+1)$. Als niet alle decimalen q_j $(j>n)$ gelijk aan 0 zijn, dan voldoet ook $r:=0,q_1q_2\ldots q_n$. Als tenslotte $p_n=8$, $q_n=9$ en alle q_j $(j>n)$ gelijk aan 0, dan zijn niet alle decimalen p_j $(j>n)$ gelijk aan 9 (want dan was $p=q$). Laat p_k de eerste dergelijke decimaal zijn. Dan voldoet $r:=0,p_1p_2\ldots p_{k-1}(p_k+1)$.

Opgaven

292 ♣ $\mathcal{A}=(A,<)$ is een lineaire ordening. Bewijs:

1. als $(A,<)$ een dicht liggende deelverzameling heeft, dan is $(A,<)$ dicht geordend,
2. als $D\subset A$ dicht ligt in $(A,<)$, dan is $(D,<)$ dicht geordend,
3. A is zelf dicht in $(A,<)$ d.e.s.d.a. $(A,<)$ een dichte ordening is,
4. als $B\subset A$ dicht ligt in $(A,<)$, en $D\subset B$ ligt dicht in de deel-ordening $(B,<)$ van $(A,<)$, dan ligt D óók dicht in $(A,<)$.

293 ♣ Geef een aftelbare verzameling $D \subset \mathbb{R}$ die dicht ligt in $(\mathbb{R}, <)$ en zódat $D \cap \mathbb{Q} = \emptyset$.

294 ♣♣ Geef verzamelingen $A, B \subset \mathbb{Q}$ zódat $A \cap B = \emptyset$ en zódat A en B beide dicht zijn in $\mathbb{Q}$.

295 ♣♣ Twee isomorfe lineaire ordeningen zijn ofwel beide separabel, ofwel geen van beide.

296 ♣ Bewijs: als $(A, <)$ en $(B, \prec)$ disjuncte, separabele, eindpuntloze lineaire ordeningen zijn, dan is $(A, <) + (B, \prec)$ óók separabel.

10.4.3 Karakterisering van $\mathbb{R}$

10.15 Stelling. (Cantor) *Een niet-lege lineaire ordening $(A, \prec)$ heeft type λ — d.i.: is isomorf met $(\mathbb{R}, <)$ — d.e.s.d.a. $(A, \prec)$*

1. *eindpuntloos,*
2. *ordeningsvolledig, en*
3. *separabel is.*

Bewijs. Dat ieder isomorf van $(\mathbb{R}, <)$ aan de gestelde condities voldoet volgt o.m. uit Voorbeeld 10.14, Opgaven 289 en 295. Voor de rest is er de volgende *Schets*. Laat D een aftelbare verzameling zijn, dicht in de eindpunt-loze lineaire ordening $(A, \prec)$. Dan heeft $(D, \prec)$ geen eindpunten en is zelf dicht geordend (Opgave 292). Dus (Stelling 10.3) $(D, \prec)$ is isomorf met $(\mathbb{Q}, <)$. Laat h een isomorfisme zijn tussen deze ordeningen. Het gezochte isomorfisme H tussen $(A, \prec)$ en $(\mathbb{R}, <)$ voegt aan een element $a \in A$ toe de *sup* van $\{h(b) \mid b \in D \wedge b \prec a\}$ in $\mathbb{R}$. Het is niet moeilijk om te zien dat dit een inbedding van $(A, \prec)$ in $(\mathbb{R}, <)$ is. Dat dit een surjectie is volgt uit de sup-eigenschap voor $(A, \prec)$. ⊣

Opgaven

297 ♣ Werk de details uit van het bewijs van Stelling 10.15.
Toon i.h.b. aan, dat H surjectief is.
Ga na, dat $h = H|D$.

298 ♣ Een niet-lege lineaire ordening $(A, \prec)$ is isomorf met $(\{r \in \mathbb{R} \mid 0 \leqslant r \leqslant 1\}, <)$ —i.e., heeft type $1 + \lambda + 1$— d.e.s.d.a.

1. *iedere* verzameling $X \subset A$ heeft een *sup* in A, en
2. $(A, \prec)$ is separabel.

Bewijs dit.

299 ♣ (Vgl. Opgave 277, blz. 139; zie ook Opgave 290.) Bewijs, dat $\lambda + 1 + \lambda = \lambda$, en dat $\lambda + \lambda \neq \lambda$.

300 ♣ (Vgl. Opgave 282 blz. 140.) Geldt $\lambda \cdot \lambda = \lambda$?

Hier volgt een bewijs, van de overaftelbaarheid van $\mathbb{R}$ dat geen gebruik maakt van decimaal-ontwikkelingen maar van zijn ordenings-eigenschappen. Een nog weer enigszins ander bewijs dat gebruik maakt van reële getallen-als-sneden is verstopt in de aanwijzing bij Opgave 301.

10.16 Gevolg. $\mathbb{N} \prec \mathbb{R}$.

Bewijs. Dat $\mathbb{N} \preceq \mathbb{R}$ is duidelijk. Onderstel, dat $\mathbb{N} \sim \mathbb{R}$, d.w.z.: dat $\mathbb{R}$ aftelbaar is. Dan is $(\mathbb{R}, <)$ een niet-lege aftelbare, dichte lineaire ordening zonder eindpunten. Volgens Stelling 10.3 geldt dan $(\mathbb{R}, <) \cong (\mathbb{Q}, <)$, d.w.z.: $\lambda = \eta$. Dus (Opgaven 277 en 299): $\eta = \eta + \eta = \lambda + \lambda \neq \lambda$; tegenspraak. ⊣

301 ♣ Bewijs: $\mathbb{R} - \mathbb{Q}$ is dicht in $\mathbb{R}$. D.w.z.: tussen iedere twee *rationale* getallen ligt een irrationaal getal.
Aanwijzing. Een makkelijk bewijs gebruikt een kardinaliteits-argument: ieder open interval van $\mathbb{R}$ heeft ordetype λ en is dus i.h.b. overaftelbaar. Dan kan het niet uitsluitend rationale getallen bevatten.
Een andere manier: onderstel, dat $p < q$ rationale getallen zijn. Fixeer een aftelling $p_0, p_1, p_2, \ldots$ van alle rationale getallen in het interval (p, q). Construeer een rij rationale getallen r_0, r_1, $r_2, \ldots$ in het interval (p, q) zódat $p < r_0 < r_2 < r_4 < \cdots > r_5 > r_3 > r_1 > q$, en zódat voor alle i: $p_i < r_{2i}$ of $r_{2i+1} < p_i$. Bekijk het paar (L, R) met $L := \{r \in \mathbb{Q} \mid \exists i(r < r_{2i})\}$ en $R := \{r \in \mathbb{Q} \mid \exists i(r_{2i+1} < r)\}$. (L, R) kan geen gat zijn, dus is er een getal r dat zowel groter is dan alle elementen van L als kleiner dan ieder element van R. Uit de constructie volgt, dat r niet rationaal kan zijn.

Precieze oplossingen voor de volgende twee opgaven eisen het keuze-axioma.

302 ♣ Laat $(A, <)$ een separabele lineaire ordening zijn. Bewijs: iedere collectie onderling disjuncte intervallen $(a, b) = \{x \in A \mid a < x \wedge x < b\}$ van $(A, <)$ $(a < b)$ is *aftelbaar.*

***Suslin Probleem/Hypothese (Suslin 1920).** Het *Suslin-probleem* is de vraag, of Stelling 10.15 doorgaat als conditie 3 (separabiliteit) wordt vervangen door z'n gevolg in Opgave 302, dat iedere collectie paarsgewijs disjuncte intervallen aftelbaar is. De *Suslin Hypothese* (SH) zegt, dat dat zo is. De gewone axiomas van de verzamelingentheorie geven hierover geen uitsluitsel.

303 ♣ Laat $(A, <)$ een separabele lineaire ordening zijn, en $B \subset A$ een dichte deelverzameling. Bewijs, dat de bijbehorende deel-ordening $(B, <)$ óók separabel is.
Waarschuwing. De aftelbare dicht liggende deelverzameling die A volgens het gegeven heeft hoeft geen deel van B te zijn.

304 ♣ (Vgl. Opgave 266, blz. 137.) Onderstel, dat p en q twee reële getallen zijn. Bewijs, dat een automorfisme h van $(\mathbb{R}, <)$ (dat is: een isomorfisme tussen $(\mathbb{R}, <)$ en zichzelf; zie Definitie 9.5, blz. 122) bestaat zódat $h(p) = q$.
Algemener: onderstel, dat $p_1 < \cdots < p_n$ en $q_1 < \cdots < q_n$ twee rijtjes reële getallen zijn. Bewijs, dat een automorfisme h van $(\mathbb{R}, <)$ bestaat zódat $h(p_i) = q_i$ $(i = 1, \ldots, n)$.

De volgende twee opgaven gebruiken ideeën uit het bewijs van Stelling 10.15.

305 ♣♣ Onderstel, dat $\mathcal{A} = (A, <)$ en $\mathcal{B} = (B, \prec)$ ordeningsvolledige lineaire ordeningen zijn, dat $D \subset A$ dicht ligt in $\mathcal{A}$ en $E \subset B$ dicht ligt in $\mathcal{B}$, en dat $(D, <) \cong (E, \prec)$. Bewijs, dat $(A, <) \cong (B, \prec)$.

306 ♣♣ Onderstel, dat $(D, <)$ een dichte lineaire ordening is. Bewijs dat een ordeningsvolledige lineaire ordening bestaat waarvan $(D, <)$ een deel-ordening is en waar D dicht in ligt.

10.4.4 Constructie van $\mathbb{R}$

Van Kronecker is de uitspraak: de natuurlijke getallen zijn door God gegeven; de rest is mensenwerk. Hier is wel iets voor te zeggen. Hoe dan ook, bij de verzamelingstheoretische opbouw van de wiskunde hoef je je dan om het bestaan van het ordetype ω niet te bekommeren.

Je kunt rationale getallen opvatten als (onvereenvoudigbare) breuken van gehele getallen, d.w.z. als (gesigneerde) paren van natuurlijke getallen. Dit verzekert de existentie van $\mathbb{Q}$ en daarmee van het ordetype η. (Zie Opgave 315 voor een soortgelijke uitwerking.)

De vraag is vervolgens, hoe je aan de (een) verzameling $\mathbb{R}$ van reële getallen komt. Er zijn verschillende verzamelingstheoretische constructies die een ordening van type λ produceren uitgaande van $(\mathbb{Q}, <)$. Hieronder wordt de constructie met *Dedekind-sneden* besproken die a.h.w. de gaten in $(\mathbb{Q}, <)$ opvult. (Een andere gaat met zgn. *fundamentaalrijen*.) De motivering hiervoor is de observatie van de volgende opgave.

307 ♣ **Opgave.** Definieer de functie $\widehat{\ }: \mathbb{R} \to \wp(\mathbb{Q})$ door: $\widehat{r} := \{q \in \mathbb{Q} \mid q < r\}$. Bewijs, dat $\widehat{\ }$ een isomorfisme is tussen $(\mathbb{R}, \leqslant)$ en $(Ran(\widehat{\ }), \subset)$.
(Vgl. Opgave 238 op blz. 129: die zegt dat $r \mapsto \{r' \in \mathbb{R} \mid r' < r\}$ een isomorfisme is.)

Dus: als je een reëel getal r identificeert met $\widehat{r} := \{q \in \mathbb{Q} \mid q < r\}$, dan transformeert de ordening $\leqslant$ van $\mathbb{R}$ in de inclusie-relatie $\subset$ op de deelcollectie $Ran(\widehat{\ })$ van $\wp(\mathbb{Q})$. De elementen van $Ran(\widehat{\ })$ zijn nu precies de *sneden* in $(\mathbb{Q}, <)$ van de volgende definitie:

10.17 Sneden. Laat $(A, <)$ een lineaire ordening zijn. Een *(links-) snede* in $(A, <)$ is een verzameling $L \subset A$ zódat

1. $L \neq \emptyset$ en $L \neq A$,
2. L is een *initiaal* of *beginstuk* van A, d.w.z.:
   als $a \in L$ en $b < a$, dan geldt ook $b \in L$,
3. L heeft geen grootste element: $\forall a \in L\, \exists b \in L : a < b$.

Opmerking. Als (L, R) een gat is in $(A, <)$ (zie Definitie 10.12, blz. 142), dan is L een snede.
Als L een snede is, dan is $(L, A - L)$ een gat d.e.s.d.a. $A - L$ geen kleinste element heeft.
Als $L \subset A$ een initiaal is van $(A, <)$, dan geldt $(A, <) = (L, <) + (A - L, <)$.

Voorbeelden.
1. $(\mathbb{N}, <)$ en $(\mathbb{Z}, <)$ hebben geen sneden.
2. Iedere snede in $\mathbb{R}$ is van de vorm $L = \{x \in \mathbb{R} \mid x < r\}$, waarbij $r = sup(L)$.
3. In $\mathbb{Q}$ zijn er *twee* typen sneden:

(i) die van de vorm $\widehat{r} := \{x \in \mathbb{Q} \mid x < r\}$ met $r = sup(\widehat{r}) \in \mathbb{Q}$ (de sneden met *sup* in $\mathbb{Q}$). (N.B.: $(\widehat{r}, \mathbb{Q} - \widehat{r})$ is *geen* gat in $(\mathbb{Q}, <)$.)

(ii) de anderen, met *sup* in $\mathbb{R} - \mathbb{Q}$; een voorbeeld is $\{q \in \mathbb{Q} \mid q \leqslant 0\} \cup \{q \in \mathbb{Q} \mid q > 0 \wedge q^2 < 2\}$, met *sup* $\sqrt{2}$. (N.B.: dit zijn de met gaten corresponderende sneden in $(\mathbb{Q}, <)$.)

Laat $\mathfrak{R}$ verder de verzameling van alle sneden in $\mathbb{Q}$ zijn.

De volgende opgaven gaan na dat $(\mathfrak{R}, \subset)$ een (reflexieve) lineaire ordening is die alle karakteristieke eigenschappen van de reële ordening heeft. M.a.w., $(\mathfrak{R}, \subset)$ een een surrogaat voor $(\mathbb{R}, \leqslant)$ (Stelling 10.18).

Opgaven

308 ♣ Bewijs dat de inclusierelatie $\subset$ een *lineaire* ordening is van $\mathfrak{R}$.

309 ♣ Bewijs, dat $(\mathfrak{R}, \subset)$ geen eindpunten heeft.

310 ♣ Bewijs, dat $(\mathfrak{R}, \subset)$ separabel is.
Schets. Laat $L, M \in \mathfrak{R}$, $L \subset M$, $L \neq M$. Bijvoorbeeld, $q' \in M - L$. Omdat M een snede is bestaat $q > q'$ in M. Nu geldt dat $L \subset \widehat{q} = \{x \in \mathbb{Q} \mid x < q\} \subset M$ en $L \neq \widehat{q} \neq M$ ($q' \in \widehat{q} - L$ en $q \in M - \widehat{q}$). Dus: tussen iedere twee sneden ligt er één van de vorm $\widehat{q}$, en daarvan zijn er maar aftelbaar veel.

311 ♣♣ Bewijs, dat $(\mathfrak{R}, \subset)$ de sup-eigenschap heeft.
Aanwijzing. Bewijs dat, als $X \subset \mathfrak{R}$ een collectie sneden is met een bovengrens $L \in \mathfrak{R}$, dan is $\bigcup X$ ($= \bigcup_{M \in X} M$, de vereniging van alle sneden in X, Definitie 3.10 blz. 38), een *snede* die de *sup* is van X.

De voorafgaande opgaven bewijzen de volgende stelling.

10.18 Stelling. $|(\mathfrak{R}, \subset)| = \lambda$.

Bewijs. Volgens de karakterisering van λ, Stelling 10.15, moet je laten zien, dat $(\mathfrak{R}, \subset)$ een lineaire ordening is die geen eindpunten heeft en zowel separabel als ordeningsvolledig is, en dat is de inhoud van Opgaven 308–311. ⊣

312 ♣ Wat gaat er in bovenstaand verhaal mis als je van de sneden in $\mathbb{Q}$ niet eist, dat ze niet-leeg zijn? (Definitie 10.17.1) en als je niet eist, dat ze verschillen van $\mathbb{Q}$? en als je niet eist, dat sneden geen grootste element hebben? (10.17.3.)

313 ♣♣ Laat X een collectie sneden zijn in $\mathbb{Q}$ met een *ondergrens.* Is de *doorsnede* $\bigcap X$ ($= \bigcap_{M \in X} M$) van alle sneden in X noodzakelijk weer een snede? Bewijs, of geef een tegenvoorbeeld.

314 ♣ Definieer, voor sneden L en M, gebruikmakend van de optellingsoperatie voor rationale getallen: $L + M := \{p + q \mid p \in L \wedge q \in M\}$. Bewijs dat dit weer een snede is. Beargumenteer, dat dit een adekwate definitie is van optelling. Kun je ook een definitie opstellen van vermenigvuldiging?

De volgende opgave construeert een ordening van type η gebruikmakend van de verzameling $\mathbb{Z}$ van gehele getallen.

315 ♣ Definieer $X := \mathbb{Z} \times \mathbb{N}^+$ $(= \{(n,m) \mid n,m \in \mathbb{Z} \wedge m > 0\})$. Definieer de relatie $\sim$ op X door $(n,m) \sim (p,q) :\equiv nq = mp$.

1. Bewijs, dat $\sim$ een equivalentie is op X. (Het idee hier is, dat de equivalentieklasse van (n,m) voor het rationale getal $\frac{n}{m}$ staat.)
2. Definieer $\prec$ op $X/\sim$ (het quotient van X modulo $\sim$, zie Definitie 4.10 blz. 47) door $|(n,m)| \prec |(p,q)| :\equiv nq < mp$. Ga na, dat deze definitie correct is, d.w.z.: representant-onafhankelijk.
3. Bewijs, dat $(X/\sim, \prec)$ ordetype η heeft.

10.5 *Welordeningen en Ordinaalgetallen

Herinner Definite 6.5 (blz. 69): een relatie $\prec$ op een verzameling A heet *gefundeerd* of *welgefundeerd* als er geen oneindige dalende rij elementen $a_0 \succ a_1 \succ a_2 \succ \cdots$ bestaat in A.

10.19 Welordeningen. Een gefundeerde lineaire ordening heet een *welordening.*

Voorbeelden.
Iedere eindige lineaire ordening is een welordening. $(\mathbb{N}, <)$ is een welordening (Opgave 86 blz. 69).
$(\mathbb{N}, >)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}, <)$ en $(\mathbb{R}, <)$ zijn geen welordeningen.

10.20 Ordinaalgetallen. Het ordetype van een welordening heet een *ordinaalgetal* of kortweg een *ordinaal.*

Opgaven

316 ♣ Bewijs dat een lineaire ordening $(A, <)$ een welordening is d.e.s.d.a. hij voldoet aan het *principe van sterke inductie* (zie 6.3 blz. 67): als voor $X \subset A$ geldt dat $\forall a(\forall a' < a(a' \in X) \Rightarrow a \in X)$, dan geldt $A \subset X$.

317 ♣ Bewijs, dat iedere welordening de sup-eigenschap heeft.

318 ♣ Bewijs:

1. Ieder natuurlijk getal (opgevat als ordetype) is een ordinaal,
2. ω is een ordinaal,
3. als α en β ordinalen zijn, dan is $\alpha + \beta$ er ook één (een geordende som van welordeningen is wéér een welordening),
4. *welgeordende sommen van ordinalen zijn ordinalen (dus producten van ordinalen zijn ordinalen).

De ordinaalgetallen zijn zelf lineair geordend, zelfs welgeordend (zie hierna voor hun natuurlijke welordening). De rij van ordinalen begint als volgt:

$0, 1, 2, \ldots$;
$\omega, \omega+1, \omega+2, \ldots$;
$\omega+\omega = \omega\cdot 2, (\omega\cdot 2)+1, \ldots, \omega\cdot 3, \ldots$;
$\omega\cdot\omega = \omega^2, \ldots, \omega^3, \ldots$;
$\omega^\omega, \ldots, \omega^{\omega^2}, \ldots \omega^{\omega^\omega}, \ldots$

(de notaties ω^ω e.v. suggereren zo ongeveer wat er wordt bedoeld). Dit zijn allemaal ordetypen van *aftelbare* welordeningen.

319 ♣ Iedere aftelbare lineaire ordening kan worden ingebed in $(\mathbb{Q}, <)$ (Opgave 262, blz. 137). Geef een verzameling $X \subset \mathbb{Q}$ van type ω^2. En één van type ω^ω.

320 ♣ Laat $(A, <)$ een welordening zijn en $h : A \to A$ een inbedding (Definitie 10.4 blz. 136). Bewijs, dat $\forall a \in A : a \leqslant h(a)$.

321 ♣ Bewijs: tussen twee welordeningen bestaat hoogstens één isomorfisme.

322 ♣ Bewijs: $(A, <)$ is een welordening d.e.s.d.a. bij ieder initiaal $X \neq A$ van $(A, <)$ (Definitie 10.17 blz. 146) een element $a \in A$ bestaat zódat $X = \{x \in A \mid x < a\}$.

10.21 Stelling. *Voor iedere twee welordeningen $(A, <)$ en $(B, \prec)$ geldt precies één van de volgende drie condities:*

1. $(A, <) \cong (B, \prec)$,
2. *er is een initiaal* $Y \neq B$ *van* $(B, \prec)$ *zódat* $(A, <) \cong (Y, \prec)$,
3. *er is een initiaal* $X \neq A$ *van* $(A, <)$ *zódat* $(X, <) \cong (B, \prec)$.

Deze stelling identificeert een natuurlijke ordening van de ordinalen: het ordinaal van $(A, <)$ is *kleiner* dan dat van $(B, \prec)$ als $(A, <)$ isomorf is met een initiaal $(Y, \prec)$ $(B \neq Y \subset B)$ van $(B, \prec)$.

Bewijs. *Schets:* definieer $h(a) = b$ $(a \in A, b \in B)$ d.e.s.d.a. $(\{x \in A \mid x < a\}, <) \cong (\{y \in B \mid y \prec b\}, \prec)$.
Uit Opgave 321 volgt, dat dit de gezochte correspondentie is. ⊣

***Burali-Forti Paradox.**
Dit is de observatie, dat het ordetype Ω van de ordening van alle ordinalen, omdat dit zelf een ordinaal is, groter moet zijn dan alle ordinalen, i.h.b. groter dan Ω zelf: een tegenspraak, want de ordening is strict; en trouwens, hoe zat het dan met $\Omega + 1$?

De manier waarop gewoonlijk aan de paradox wordt ontsnapt is de volgende: een ordinaal is per definitie het ordetype van een welgeordende *verzameling*. De conclusie moet zijn dat de collectie van alle ordinalen kennelijk geen verzameling is. (Netzomin als de collectie van alle verzamelingen of de Russell-collectie verzamelingen zijn.)

323 ♣ Onderstel dat α een ordinaal is zódat $\alpha \leqslant \lambda$. Bewijs, dat α *aftelbaar* is. D.w.z.: iedere door de gewone ordening welgeordende verzameling van reële getallen is aftelbaar.

324 ♣♣ Geef een bewijs van Stelling 6.16 (blz. 78) door aan een Smullyaanse doos met ballen $n_1, \ldots, n_k$ $(n_1 \geqslant \cdots \geqslant n_k)$ het ordinaal $\omega^{n_1} + \cdots + \omega^{n_k}$ toe te kennen. Kun je zoiets ook doen voor het gevecht tussen Hercules en de Hydra?

325 ♣♣ Zie Subsectie 6.3.4 voor QO en WQO. Onderstel, dat $\leqslant$ QO is op Q

1. Onderstel, dat $\preceq$ een lineaire ordening is van Q zódat $\leqslant \subset \preceq$. Bewijs: als $\leqslant$ WQO is, dan is $\prec$ een welordening.
2. Onderstel dat iedere lineaire ordening $\preceq$ van Q waarvoor $\leqslant \subset \preceq$ een welordening is. Bewijs: $\leqslant$ is WQO op Q.

De volgende stelling zegt, dat bij iedere verzameling een relatie bestaat die de verzameling welordent. Voor sommige verzamelingen spreekt dat vanzelf (bijvoorbeeld, voor $\mathbb{N}$, en voor iedere met $\mathbb{N}$ gelijkmachtige verzameling). Voor andere verzamelingen ($\mathbb{R}$!) is dit bepaald niet vanzelfsprekend. Het bewijs gebruikt het keuze-axioma.

10.22 Welordeningsstelling (Zermelo, 1904). *Iedere verzameling heeft een welordening.*

Bewijs. Laat A de te welordenen verzameling zijn. Onderstel, dat h een keuze-functie is voor de collectie van niet-lege deelverzamelingen van A (zie Definitie 8.21, blz. 112). Het volgende bewijs laat zien hoe deze keuze-functie kan worden getransformeerd tot een welordening van A.
Noteer, voor echte deelverzamelingen B van A, het door h in $A-B$ geselecteerde element met B^s. $B^+ := B \cup \{B^s\}$. Dus, B^+ ontstaat uit B door toevoeging van het door h in $A - B$ geselecteerde element B^s.

Het *idee* van het bewijs is het volgende. Gebruikmakend van h wordt een welordening van (althans, een gedeelte van) A gegenereerd die als volgt begint:
$\emptyset^s$, $\{\emptyset^s\}^s$, $\{\emptyset^s, \{\emptyset^s\}^s\}^s$, $\{\emptyset^s, \{\emptyset^s\}^s, \{\emptyset^s, \{\emptyset^s\}^s\}^s\}^s$, $\ldots$,
$\{\emptyset^s, \{\emptyset^s\}^s, \{\emptyset^s, \{\emptyset^s\}^s\}^s, \ldots\}^s$, $\ldots$

Het eerste doel is het bepalen van de collectie W van alle verzamelingen die beginstuk zijn van deze reeks. De welordening zelf kan dan worden bepaald aan de hand van deze collectie.

Elementen van $\mathcal{K}$ zijn per definitie alle collecties $X \subset \wp(A)$ waarvoor de volgende twee eigenschappen van de (nog te definiëren!) collectie W gelden:

1. $Y \subset X \implies \bigcup Y \in X$ (i.h.b.: $\emptyset = \bigcup \emptyset \in X$),
2. $A \neq B \in X \implies B^+ \in X$.

Merk op, dat $\wp(A) \in \mathcal{K}$. I.h.b. is $\mathcal{K}$ dus niet-leeg. Behalve de gezochte collectie heeft $\mathcal{K}$ nog allerlei elementen (zoals $\wp(A)$) waar je niets aan hebt. De gezochte collectie W is het *kleinste* element van $\mathcal{K}$.
Definieer $W := \bigcap K$. (Zie Definitie 3.10 blz. 38 en de opmerking erna.) De

kunst is nu om te zien dat de zó gedefinieerde collectie W inderdaad de gezochte collectie van het hiervoor beschreven idee is. Dit gebeurt in zes étappes I–VI. De eerste twee zeggen dat, inderdaad, W het kleinste element van $\mathcal{K}$ is.

(I) $W \in \mathcal{K}$.

Bewijs: Check de twee definiërende condities voor $\mathcal{K}$. Opgave.

Dat $W \in \mathcal{K}$ geldt wordt verder geregeld stilzwijgend gebruikt.

(II) $X \in \mathcal{K} \implies W \subset X$.

Dit vanzelfsprekende gevolg van de definitie van W speelt een rol op een aantal cruciale plaatsen. Zie het gebruik van de hulp-collecties X_1 en X_2 in III en van X in IV.

(III) $\subset$ is een lineaire ordening van W.

Bewijs: Dat $\subset$ een (reflexieve) partiële ordening is van W spreekt vanzelf. Lineariteit vormt het *pièce de résistance* van het hele bewijs. Wat aangetoond moet worden is, dat

$$\forall B \in W\, \forall C \in W\, (B \subset C \vee C \subset B). \tag{10.1}$$

Definieer $X_1 := \{B \in W \mid \forall C \in W\, (B \subset C \vee C \subset B)\}$. Het is voldoende om te laten zien, dat $X_1 \in \mathcal{K}$. Dan volgt immers, m.b.v. (II), dat $W \subset X_1$, en dat is juist equivalent met 10.1.

Opdat $X_1 \in \mathcal{K}$ moeten de twee definiërende condities voor $\mathcal{K}$ worden nagelopen.

1. $Y \subset X_1 \implies \bigcup Y \in X_1$.

Onderstel, dat $Y \subset X_1$. Te bewijzen: $\bigcup Y \in X$, ofwel: $\forall C \in W(\bigcup Y \subset C \vee C \subset \bigcup Y)$. Laat dus $C \in W$.

(a) Er is een $B \in Y$ zódat $C \subset B$. In dat geval geldt $C \subset \bigcup Y$.

(b) Er is geen $B \in Y$ zódat $C \subset B$. Dan geldt (wegens $Y \subset X_1$) voor alle $B \in Y$, dat $B \subset C$, en in dat geval heb je dat $\bigcup Y \subset C$.

2. $A \neq B \in X_1 \implies B^+ \in X_1$.

Onderstel, dat $A \neq B \in X_1$. Aangetoond moet worden, dat $B^+ \in X_1$, ofwel

$$\forall C \in W\, (B^+ \subset C \vee C \subset B^+). \tag{10.2}$$

Definieer $X_2 := \{C \in W \mid B^+ \subset C \vee C \subset B^+\}$. Opnieuw is het voldoende om na te gaan, dat $X_2 \in \mathcal{K}$: dan volgt weer dat $W \subset X_2$, hetgeen juist equivalent is met 10.2.

1. $Y \subset X_2 \implies \bigcup Y \in X_2$.

Laat $Y \subset X_2$.

(a) Er is een $C \in Y$ zódat $B^+ \subset C$. In dat geval geldt $B^+ \subset \bigcup Y$.

(b) Er is niet zo'n $C \in Y$. Dan geldt ($Y \subset X_2$) voor alle $C \in Y$ dat $C \subset B^+$, en in dat geval volgt er, dat $\bigcup Y \subset B^+$.

2. $A \neq C \in X_2 \implies C^+ \in X_2$.

Onderstel, dat $A \neq C \in X_2$. Er moet aangetoond worden, dat $C^+ \in X_2$, d.w.z., dat

$$B^+ \subset C^+ \vee C^+ \subset B^+.$$

Nu geldt dat $B \in X_1$, dus i.h.b. $B \subset C^+ \vee C^+ \subset B$. Als $C^+ \subset B$, dan $C^+ \subset B^+$, en je bent klaar. Neem dus maar aan, dat $B \subset C^+$.

Verder geldt dat $C \in X_2$, dus i.h.b. $B^+ \subset C \vee C \subset B^+$. Als $B^+ \subset C$, dan $B^+ \subset C^+$, en je bent weer klaar. Neem dus maar aan, dat $C \subset B^+$.
Tenslotte, omdat $B \in X_1$ geldt er $B \subset C \vee C \subset B$.
In het eerste geval heb je dan, dat $B \subset C \subset B^+$, en dus geldt (B en B^+ schelen maar één element) dat $B = C$ of $C = B^+$, en dus $B^+ = C^+$ of $B^+ \subset C^+$.
In het tweede geval heb je netzo, dat $C \subset B \subset C^+$, dan geldt $C = B$ of $B = C^+$, en dus $C^+ = B^+$ of $C^+ \subset B^+$.

(IV) $\subset$ (eigenlijk: z'n irreflexieve compagnon) is een welordening van W.
Bewijs: Onderstel, dat $\subset$ niet gefundeerd is op W. Dan is er een strict dalende rij $A_0 \supset A_1 \supset A_2 \supset \cdots$ van verzamelingen in W. Definieer $X := \{B \in W \mid \forall n\,(B \subset A_n)\}$. Het is voldoende om na te gaan, dat $X \in \mathcal{K}$: dan volgt immers weer, dat $W \subset X$, en dat is kennelijk onmogelijk (bijvoorbeeld, $A_0 \in W - X$).
1. $Y \subset X \Longrightarrow \bigcup Y \in X$.
Triviaal.
2. $A \neq B \in X \Longrightarrow B^+ \in X$.
Onderstel, dat $A \neq B \in X$, maar $B^+ \notin X$. Bijvoorbeeld, $B^+ \not\subset A_n$. Dan geldt wegens lineariteit van $\subset$ op W, dat $B \subset A_n \subset B^+$. Dus, B en A_n schelen hoogstens één element. Maar dat is absurd: tussen A_n en B liggen nog de onderling verschillende verzamelingen $A_{n+1}, A_{n+2}, \ldots$, en dus schelen A_n en B oneindig veel elementen.

(V) Definieer $f : A \longrightarrow W$ door $f(a) := \bigcup\{B \in W \mid a \notin B\}$. f is een injectie.
Bewijs: Er geldt kennelijk, dat $a \notin f(a)$. Ook geldt dat $a \in f(a)^+$: als $a \notin f(a)^+$, dan volgt $f(a)^+ \in \{B \in W \mid a \notin B\}$, dus $f(a)^+ \subset \bigcup\{B \in W \mid a \notin B\} = f(a)$, een onmogelijkheid. Dus, $a = h(A - f(a))$. Gevolg: als $f(a) = f(b)$, dan geldt $a = h(A - f(a)) = h(A - f(b)) = b$.

(VI) Definieer $\preceq$ op A door $a \preceq b :\equiv f(a) \subset f(b)$. De relatie $\preceq$ (eigenlijk: z'n irreflexieve compagnon $\prec$) is nu een welordening van A.
Bewijs: Lineariteit volgt direct uit het feit dat f een injectie is van A in de lineaire ordening $(W, \subset)$. Gefundeerdheid: iedere oneindige dalende rij $\cdots \prec a_2 \prec a_1 \prec a_0$ in A levert een oneindige, strict dalende rij $\cdots \subset f(a_2) \subset f(a_1) \subset f(a_0)$ in W, in strijd met de gefundeerdheid van $\subset$ op W. $\dashv$

10.6 *Het Lemma van Zorn

Het gebruik van het keuze-axioma in niet-triviale gevallen eist in de regel vertrouwdheid met ordinalen (of ingewikkelde argumentaties à la het bewijs van de Welordeningsstelling 10.22). Bijvoorbeeld, een andere, meer directe, uitwerking van het bewijs-idee van 10.22 bestaat uit het definiëren van een functie van ordinalen naar de verzameling A. Het volgende *Lemma van Zorn* is een equivalent van het keuze-axioma waarmee het gebruik van ordinalen vaak kan worden omzeild, en dat om die reden veel wordt gebruikt.

10.23 Lemma van Zorn. *Laat $(A, \leqslant)$ een niet-lege partiële ordening zijn. Als iedere* keten *in A — dat is: een door $\leqslant$ lineair geordende deelverzameling van A — een bovengrens heeft in A, dan heeft A een maximaal element.*

Bewijs. Zie Opgave 327. ⊣

Opgaven

326 ♣ Geef een bewijs van het keuze-axioma, gebruikmakend van Zorn's Lemma.
Aanwijzing. Laat K een verzameling van niet-lege verzamelingen zijn. Gezocht: een keuzefunctie voor K. Laat $\mathcal{F}$ de verzameling van alle *partiële* keuzefuncties voor K zijn, dat zijn: de functies f met $Dom(f) \subset K$ waarvoor geldt $\forall A \in Dom(f)[f(A) \in A]$. $\mathcal{F}$ wordt partieel geordend door de inclusierelatie $\subset$. Niet iedere vereniging van functies is weer een functie, maar de vereniging $\bigcup L = \bigcup_{f \in L} f$ van een *keten* $L \subset \mathcal{F}$ is dat wél, en is tegelijk bovengrens van die keten. Zorn levert een maximaal element h in $\mathcal{F}$. Maar dan geldt $Dom(h) = K$ (en dus is h een keuzefunctie voor K): was $Dom(h) \neq K$, bijv., $A \in K - Dom(h)$, neem dan een element $x \in A$; en de partiële keuzefunctie $h \cup \{(A, x)\} \in \mathcal{F}$ laat zien, dat h niet maximaal was.

327 ♣ Completeer de volgende schets voor een bewijs van Zorn's Lemma, gebruikmakend van het keuze-axioma.
Onderstel dat $(A, \leqslant)$ een niet-lege partiële ordening is waarin iedere keten een bovengrens heeft. Fixeer een keuze-functie voor de collectie van niet-lege deelverzamelingen van A. Modificeer het bewijs van Stelling 10.22 op de volgende manier. Noteer voor verzamelingen $B \subset A$ waarvoor $\{a \in A \mid \forall b \in B(b < a)\} \neq \emptyset$: $B^+ := B \cup \{h(\{a \in A \mid \forall b \in B(b < a)\})\}$. $\mathcal{K}$ is nu de supercollectie van collecties $X \subset \wp(A)$ met

1. $Y \subset X \Longrightarrow \bigcup Y \in X$,
2. $B \in X \wedge \{a \in A \mid \forall b \in B(b < a)\} \neq \emptyset \Longrightarrow B^+ \in X$.

Check nu onderdelen I, II en III van het bewijs van 10.22.
Bewering: iedere $B \in X$ is een keten.
Bewijs. Definieer $X := \{B \in W \mid \forall b, c \in B(b \leqslant c \vee c \leqslant b)\}$. Het is voldoende om na te gaan, dat $X \in \mathcal{K}$. (Dan volgt $W \subset X$, etc.) Doe dit.
Gevolg. $\bigcup W \in W$ is een keten.
Laat a een bovengrens zijn van $\bigcup W$ in A. Ga na, dat a maximaal is.

328 ♣ Bewijs: bij iedere irreflexieve partiële ordening $(A, <)$ bestaat een verzameling $B \subset A$ die door $<$ wordt welgeordend, en zódat $\{a \in A \mid \forall b \in B(b < a)\} = \emptyset$.

De volgende opgaven eisen allen het gebruik van het Lemma van Zorn.

329 ♣♣ Bewijs: iedere partiële ordening van een verzameling is deel van een lineaire ordening. (Vgl. Opgave 232 blz. 126.)

330 ♣♣ Bewijs de Trichotomie-stelling 8.22, blz. 112.
Aanwijzing. Als verzamelingen A en B geven zijn, beschouw de verzameling van alle injecties f met $Dom(f) \subset A$ en $Ran(f) \subset B$, partieel geordend door $\subset$.

331 ♣♣ Completeer de volgende bewijsschets voor de Welordeningsstelling 10.22.
Laat f een keuze-functie zijn voor $\wp(A) - \{\emptyset\}$, A de te welordenen verzameling. Laat K de verzameling van alle welordeningen $(B, <)$ zijn met 1. $B \subset A$ en 2. als $b \in B$, dan geldt $b = f(A - \{x \in B \mid x < b\})$. Bewijs: (a) van iedere twee welordeningen in K is één een initiaal van de ander; (b) ieder element van A is element van een welordening in K. Hieruit volgt, dat de vereniging van alle welordeningen in K een welordening is van A.

332 ♣ Completeer het volgende bewijs-idee voor de Welordeningsstelling 10.22, gebaseerd op Zorn's Lemma.
Laat A de te welordenen verzameling zijn. Pas Zorn's Lemma toe op de verzameling van alle welordeningen $\mathcal{B} = (B, <)$ met $B \subset A$, partieel geordend door de relatie $\preceq$ gedefinieerd door $\mathcal{B} \preceq \mathcal{C} :\equiv \mathcal{C}$ kan worden geschreven als een geordende som $\mathcal{C} = \mathcal{B} + \mathcal{D}$.

Gemengde Opgaven

333 ♣ Hier volgen drie eigenschappen van de gewone lineaire ordening $(\mathbb{N}, <)$.

- er is een kleinste element,
- ieder element heeft een directe opvolger,
- er is geen element met voorgangers maar zonder *directe* voorganger.

1. Geef een simpel, concreet voorbeeld van een lineaire ordening met deze drie eigenschappen die niet isomorf is met $(\mathbb{N}, <)$.
2. Wat is het ordetype van jouw ordening?
3. Bepaal alle ordetypen van lineaire ordeningen met de sup-eigenschap en de drie eigenschappen boven.

334 ♣♣ Gegeven is een niet-lege lineaire ordening $(A, <)$ met een ordetype α waarvoor geldt, dat $\alpha + \alpha = \alpha$.
(Een voorbeeld is het ordetype $\alpha := 1 + 2\lambda + 1$: $(1 + 2\lambda + 1) + (1 + 2\lambda + 1) = 1 + 2\lambda + 2 + 2\lambda + 1 = 1 + 2(\lambda + 1 + \lambda) + 1 = 1 + 2\lambda + 1$.)
Bewijs: er is een collectie I van initialen $L \subset A$ met de eigenschap dat zowel $(L, <)$ als $(A - L, <)$ ordetype α hebben, zódat I door $\subset$ wordt geordend in type η.

335 ♣ Definieer de operatie * (die aan eindige lineaire ordeningen eindige lineaire ordeningen toevoegt) als volgt: als A een eindige lineaire ordening is van n elementen, dan ontstaat $A^\star$ uit A door toevoeging van $n + 1$ nieuwe elementen, te weten (i) een nieuw kleinste element m^- kleiner dan het kleinste element m van A; (ii) een nieuw grootste element M^+ groter dan het grootste element M van A, en (iii) tussen iedere twee opvolgende elementen a en b van A een nieuw element $[a, b]$. (Voorbeeld: als A de gewone ordening is op $\{3, 7, 12\}$, dan zou $A^\star$ bijv. kunnen zijn: $\{1, 3, 4, 7, 10, 12, 15\}$: neem $3^- = 1$, $12^+ = 15$, $[3, 7] = 4$ en $[7, 12] = 10$.)

Definieer de oneindige rij van eindige lineaire ordeningen $A_0, A_1, A_2, \ldots$ door: A_0 is een één-elementige ordening, en verder geldt voor alle n: $A_{n+1} = A_n^\star$. (Dus: A_n heeft $1 + 2 + 4 + 8 + \cdots + 2^n = 2^{n+1} - 1$ elementen.) Na afloop van dit proces heb je een (oneindige) lineaire ordening op de vereniging $A_0 \cup A_1 \cup A_2 \cup \cdots$. Welk ordetype heeft deze ordening? Waarom?

336 ♣ Geef een voorbeeld van een verzameling $A \subset \mathbb{Q}$ zódat voor het ordetype α van A (geordend door de ordening van $\mathbb{Q}$) geldt, dat $\omega + \alpha = \alpha$.

337 ♣ Geldt $\eta + 1 + \lambda = \eta + \lambda$? Waarom (niet)?

338 ♣♣ Bewijs:

1. de verzameling van alle lineaire ordeningen van $\mathbb{N}$ is gelijkmachtig met $\mathbb{R}$,
2. de verzameling van alle aftelbaar oneindige lineaire ordetypen is gelijkmachtig met $\mathbb{R}$.

339 ♣♣ Gelden de volgende gelijkheden? Geef een — liefst kort — argument.

1. $\zeta + \zeta = \zeta$,
2. $\rho + \rho = \rho$ (ρ is het ordetype van $\mathbb{R} - \mathbb{Q}$, onder de gewone ordening),
3. $\rho + 1 + \rho = \rho$.

340 ♣♣ Beschouw de (n.b.: lineaire) ordening $\prec$ tussen punten van het gesloten eenheidsvierkant $[0,1] \times [0,1]$ gedefinieerd door

$$(x,y) \prec (a,b) \equiv (x < a \wedge y = b) \vee y < b.$$

(Volgens Definitie 10.10 blz. 140 heeft deze ordening type $(1 + \lambda + 1) \cdot (1 + \lambda + 1)$.)

1. Bewijs dat deze ordening *niet* separabel is.
2. Bewijs dat deze ordening de sup-eigenschap heeft.
   *Algemener, toon aan: als $(A, <)$ de sup-eigenschap heeft en iedere $\mathcal{B}_a$ ($a \in A$) heeft zowel eindpunten als de sup-eigenschap, dan heeft $\sum_{a \in A} \mathcal{B}_a$ óók de sup-eigenschap.
3. Beperk $\prec$ tot $[0,1) \times [0,1)$. (Type: $(1 + \lambda) \cdot (1 + \lambda)$.) Heeft deze beperking de sup-eigenschap?

341 ♣♣ Onderstel dat $(\mathbb{R}, <) = \sum_{a \in A} \mathcal{B}_a$ een condensatie is waarbij de gebruikte ordening $(A, \prec)$ oneindig en dicht is. Bewijs dat tenminste één van de $\mathcal{B}_a$ uit maar één element bestaat. ("Iedere dichte condensatie van $(\mathbb{R}, <)$ bevat een singleton.")

10.24 *Verspreid. Een lineaire ordening waarin $(\mathbb{Q}, <)$ *niet* kan worden ingebed heet *verspreid.*[1]

342 ♣♣ Onderstel, dat de lineaire ordening $(A, \prec)$ en alle lineaire ordeningen $\mathcal{B}_a$ ($a \in A$) verspreid zijn. Bewijs dat $\sum_{a \in A} \mathcal{B}_a$ óók verspreid is.

343 ♣♣ Bewijs dat de volgende twee condities voor een lineaire ordening $\mathcal{B}$ equivalent zijn:

1. $\mathcal{B}$ is verspreid,
2. er is geen condensatie $\mathcal{B} = \sum_{a \in A} \mathcal{B}_a$ van $\mathcal{B}$ waarbij de gebruikte ordening van A dicht en oneindig is.

344 ♣ Er zijn precies *twee* ordetypen van lineaire ordeningen die separabel zijn en waarin *iedere* verzameling een *sup* heeft. Welke zijn dit?

Samenvatting

Belangrijkste begrippen:

- dicht, separabel, sup-eigenschap
- som van ordeningen en typen.

Vragen:

- welke karakteriseringen hebben de ordeningen van $\mathbb{N}$, $\mathbb{Q}$ en $\mathbb{R}$ en hoe bewijs je die?
- hoe construeer je een ordening van type λ uit één van type η?

[1] Eng.: *scattered.*

Literatuur

Het voor de Welordeningsstelling 10.22 gegeven bewijs is een variatie op het tweede bewijs van Zermelo (Neuer Beweis für die Möglichkeit einer Wohlordnung, *Mathematische Annalen* 65 (1908) 107–128; in Zermelo's bewijs worden uit de te welordenen verzameling A netzolang door de keuze-functie geselecteerde elementen verwijderd totdat hij leeg is; in het gegeven bewijs wordt, omgekeerd, A opgebouwd vanuit $\emptyset$ door zulke elementen toe te voegen). Het type definitie van de cruciale collectie W heet een *inductieve definitie*; het opmerkelijke hier is dat W welgeordend blijkt te zijn. De schets in Opgave 331 volgt Zermelo's eerste bewijs. (Beweis, dass jede Menge wohlgeordnet werden kann, *Mathematische Annalen* 59 (1904) 514–516. In dit artikel werd het keuze-axioma voor het eerst expliciet geformuleerd, en de welordeningsstelling is de eerste expliciete toepassing.) Dat hier een welordening opduikt is minder verrassend dan in het tweede bewijs.

Rosenstein [13] beantwoordt alle overblijvende vragen over lineaire ordeningen. Het gebied van de partiële ordeningen is nog omvangrijker, maar één boek hierover met "alles" erin is niet voorhanden.

Literatuur

[1] D. van Dalen. *Formele logica, een informele inleiding.* Oosthoek, Utrecht 1971.

[2] D. van Dalen. *Logic and structure.* Springer, 2e druk, Berlijn 1983.

[3] D. van Dalen, K. Doets en H.C.M. de Swart. *Verzamelingen, naïef, axiomatisch en toegepast.* Oosthoek, Scheltema & Holkema, Utrecht 1975.

[4] K.J. Devlin. *Sets, functions and logic: an introduction to abstract mathematics.* Chapman and Hall, Londen 1992. Gereviseerde editie van de eerste editie uit 1981.

[5] K. Doets. *Basic model theory.* CSLI, Stanford 1996.

[6] P.R. Halmos. *Naive set theory.* Springer, Berlijn 1974. (Nederlandse vertaling: *Intuïtieve Verzamelingenleer.* Aula 372, Het Spectrum 1968.)

[7] J. Henle. *An outline of set theory.* Springer, Berlijn 1986.

[8] K. Kunen. *Set theory, an introduction to independence proofs.* North-Holland, Amsterdam 1983.

[9] A. Levy. *Basic set theory.* Perspectives in mathematical logic. Springer, Berlijn 1979.

[10] G.H. Moore. *Zermelo's axiom of choice, its origins, development, and influence.* Studies in the history of mathematics and physical sciences 8. Springer, Berlijn 1982.

[11] R.P. Nederpelt. *De taal van de wiskunde. Een verkenning van wiskundig taalgebruik en logische redeneerpatronen.* Versluys, Almere 1987.

[12] D. Prawitz. *Natural deduction, a proof-theoretical study.* Almqvist & Wiksell, Stockholm 1965.

[13] J.G. Rosenstein. *Linear orderings.* Academic Press, New York 1982.

[14] R.L. Vaught. *Set theory, an introduction.* Birkhäuser, Boston 1985.

[15] D.J. Velleman. *How to prove it. A structured approach.* Cambridge University Press 1994.

Grieks Alfabet

In de wiskunde bestaat een chronisch gebrek aan symbolen. Een alfabet waarvan de letters gretig aftrek vinden is het Griekse. (En soms wijken we zelfs uit naar Gothisch en Hebreeuws.) Omdat niet iedereen Grieks in z'n pakket heeft gekozen, volgen de meest voorkomende letters hieronder. Schrijf ze!

naam	*kleine letter*	*hoofdletter*
alfa	α	
beta	β	
gamma	γ	Γ
delta	δ	Δ
epsilon	ε	
zeta	ζ	
eta	η	
theta	θ	Θ
iota	ι	
kappa	κ	
lambda	λ	Λ
mu	μ	
nu	ν	
ksi	ξ	Ξ
pi	π	Π
rho	ρ	
sigma	σ	Σ
tau	τ	
upsilon	υ	Υ
phi	φ	Φ
chi	χ	
psi	ψ	Ψ
omega	ω	Ω

Index

abstractie, 31
AC, 112
afbeelding, 51
afleidbaar, 96
afleiding, 89, 91
    van—uit, 96
afleidingsregel, 90
    afgeleid, 96
aftelbaar, 104
aftelling, 104
alef, 111
algebra,
    Boole, 37
    verzamelingen, 33
algebraïsch, 109
antisymmetrisch, 117
argument, 51
asymmetrisch, 117
automorfisme, 122
axioma, 29
    Aussonderung/separatie, 32
    extensionaliteit, 30
    keuze, 112
    machtsverzameling, 37
    somverzameling, 38
axiomatiek, 29
beeld, 51
beeldverzameling, 53
beginstuk, 144
begrip, primitief/gedefinieerd, 29
betrouwbaarheid, 98, 99
bewijs, 15, 89
    uit ongerijmde, 21, 25, 92, 99
bewijsregel, 18
    afgeleid, 19
    deductie, 19
    eliminatie, 18
    generalisatie, 23
    instantiatie, 23
    introductie, 18
bijectie, 55
boom, 76, 84
    binair, 91
    blad, 77
    geordend, 85
    hoogte, 76
    sub-, 76
    top, 77
    wortel, 77
bovengrens, 139
broer, 77
Burali-Forti paradox, 147
Cantor, G., 30, 32, 105, 111, 132, 142
CH, 108
codomein, 52
Cohen, P.J., 108
collectie, 32
complement, 36
component, 47
compositie, 56
conclusie, 18, 91
condensatie, 137
conjunctie, 6
connectief, 2, 6
consistent, 101
continu, 13, 26
    uniform-, 13
continuum, 108
    probleem/hypothese, 108, 113
contrapositie, 8
convex, 138
coördinaat, 41
d.e.s.d.a., 2

Dedekind, R., 107
deductie, natuurlijke, 89
deductieregel, 91
deelverzameling, 33
    echte, 33
definitie, 17, 29
    inductieve, 154
definitiegebied, 51
definitioneel equivalent, 2
definitioneel gelijk aan, 2
dicht in, 141
disjunct, 35
disjunctie, 7
domein, 4, 43, 51
doorsnede, 35, 38
dus, 16
eigenschap, 31, 66
eindig, 70, 71
eindpunt, 125
element, 30
    eerste, 125
    grootste, 125
    kleinste, 125
    laatste, 125
    maximaal, 124
    minimaal, 125
eliminatieregel, 90
equivalent, 10, 12
equivalentie, 8
equivalentieklasse, 46
equivalentierelatie, 45
falsum, 89
formule, 5, 9, 11
functie, 51
    als verdeling, 60
    beperking, 53
    bereik, 51
    domein, 51
    inverse, 58
    karakteristieke, 72
    keuze, 112
    op, 52
    opvolger, 70
    restrictie, 53
    van—naar, 52
    waarde, 51
gat, 140
gefundeerd, 69, 146
geldig, 9, 12
gelijkheid,
    van functies, 52
    van verzamelingen, 30
gelijkmachtig, 70
    hoogstens, 103
getal,
    geheel, 105
    natuurlijk, 4, 65, 111
    rationaal, 30, 105
    reëel, 1, 106
gevolg, logisch, 99
Gödel, K., 108
    volledigheidsstelling, 98, 140
haakjes, 2, 9, 10, 53
Hercules, 78
Hydra, 78
hypothese, 90, 91
    intrekken, 90, 92
identiteitsfunctie, 52, 55
identiteitsrelatie, 44
implicatie, 7
    omkering, 8
inbedding, 134
    tussen bomen, 84
inductie, 65
    basis, 66
    hypothese, 66
    naar n, 66
    naar aantal elementen, 73
    parameter, 66
    stap, 66
    sterke, 67
    vanaf m, 67
    voor eindige verzamelingen, 73
infimum, 140
initiaal, 144
injectie, 55
introductieregel, 90
inverse, 44, 58
    links/rechts, 58, 112
irreflexief, 117
isomorf, 122
isomorfisme, 122

kardinaalgetal, 110
keuzefunctie, 112
kind, 77
klasse, 32
knoop, 77
König's lemma, 77
kombinatoriek, 73
Kronecker, 144
Kruskal, J., Stelling, 84
kwantor, 2, 11
    beperkte, 13
lambda-notatie, 53
lemma, 29
logica,
    eerste-orde, 140
    hogere-orde, 140
    kwantor, 11
    propositie, 9
    tweede-orde, 140
machtsverzameling, 37, 62
model, 4
modus ponens, 19, 91
negatie, 6
ondergrens, 140
oneindig, 71
    aftelbaar, 104
onwaar, 6
opvolger, 126
    directe, 126
ordening, 119
    dicht, 132
    irreflexief, 119
    lineaire, 125
    plaatje, 120
    quasi, 82
    rationale, 132
    reële, 142
    reflexief, 119
    wel-quasi, 82
ordeningsvolledig, 139
ordetype, 128
    reële, 144
ordinaalgetal, 146
origineel, 51
ouder, 77
overaftelbaar, 105
paar,
    geordend, 41
    ongeordend, 33
pad, 76
    lengte, 76
    van, naar, door, 76
permutatie, 55
principe,
    comprehensie, 30, 32
    minimaliteits, 68
    pigeon-hole, 74, 107
product, 42
    van ordeningen, 138
    van ordetypen, 138
    van verzamelingen, 41, 62
propositie, 29
propositieletter, 9
quotient, 47
Ramsey, F.P., 75
reflexief, 45, 117
relatie, 43
    beperking, 134
    bereik, 43
    binaire, 44
    domein, 43
    equivalentie, 45
    inverse, 121, 124
    tussen, 43
    van—naar, 43
representant, 46
    -onafhankelijk, 62
rigide, 129
Russell, B.A.W., paradox, 32
separabel, 141
singleton, 33
Smullyan R.; balspel, 78
snede, 144
som,
    van kardinalen, 111
    van ordeningen, 135, 137
    van ordetypen, 136, 137
somverzameling, 38
stamboom, 77
stelling, 29
struktuur, 4
subboom, 76

subformule, 10
submodel, 134
sup-eigenschap, 139, 140
supremum, 139
surjectie, 55
Suslin hypothese, 143
Suslin probleem, 143
symmetrisch, 45, 117
teken,
    identiteit, 2
    logisch, 2
    niet-logisch, 4
tellen, 70
top-down, 84
transcendent, 109
transitief, 45, 117
trichotomie, 112, 151
triviaal, 8, 34, 38, 43, 45, 68, 118
universum, 4
variabele, 2
    gebonden/vrij, 2, 3, 5, 31, 53
    propositie, 9
verdeling, 47, 60, 74
vereniging, 35, 38
verschil, 35
verspreid, 153
verum, 89
vervulbaar, 101
vervult, 98
verzameling, 29
    lege, 33
    notatie, 31
    onderliggende, 44
volledig origineel, 53
volledigheid, 98, 100, 101
voorganger, 126
    directe, 126
voorwaarde, voldoende/nodige, 8
waar, 6
waardering, 98
waarheidstafel, 6, 9
waarheidswaarde, 6
welgefundeerd, 69, 146
welordening, 146
Welordeningsstelling, 148
wet,
    contrapositie, 10
    DeMorgan, 10, 36
    van Peirce, 95
willekeurig ding, 23, 66
Zermelo, E., 32, 148
ZF, 29
zin, 11
Zorn's lemma, 112, 150

Notatie

$\dashv$ – einde bewijs
$\mathbb{N} = \{0, 1, 2, \ldots\}$ – vz. natuurlijke getallen
$\mathbb{Z}$ – vz. der gehele getallen
$\mathbb{Q}$ – vz. der rationale getallen
$\mathbb{R}$ – vz. der reële getallen
$:\equiv$ – per definitie equivalent met, 2
$:=$ – per definitie gelijk aan, 2
$\rightarrow$, $\Rightarrow$ – implicatie, 2, 8
$\wedge$ – conjunctie, 2, 6
$\vee$ – disjunctie, 2, 7
$\neg$ – negatie, 2, 6
$\leftrightarrow$, $\Leftrightarrow$ – equivalentie, 2, 8
$\equiv$ – logisch equivalent met, 10
$\forall$ – universele kwantor, 2
$\exists$ – existentiële kwantor, 2
$=$ – gelijkheid, 2
W, O – waarheidswaarden, 6
$\models\!\!\Longrightarrow$ – direct gevolg van, 19
$\models\!\!\Longrightarrow\!\!\!\!\Rightarrow$ – gevolg van, 20
MP, $\rightarrow$E – modus ponens, 20, 24, 91
D, $\rightarrow$I – deductieregel, 20, 24, 92
$\wedge$E/I – el./intr. regel $\wedge$, 20, 24, 92
$\leftrightarrow$E/I – el./intr. regel $\leftrightarrow$, 21, 24
$\neg$E/I – el./intr. regel $\neg$, 21, 24
BO – bewijs uit ongerijmde, 21, 24, 92
$\vee$ E/I – el./intr. regel $\vee$, 22, 24
$\forall$E/I – el./intr. regel $\forall$, 23, 24
$\exists$E/I – el./intr. regel $\exists$, 23, 24
$\in$, $\notin$ – (geen) element van, 30
$\{a_1, \ldots, a_n\}$ – vz. van $a_1, \ldots, a_n$, 31
$\{x \mid E\}$ – vz. van x-en met E, 31
$\{x \in A \mid E\}$ – vz. van $x \in A$ met E, 31
$\{a\}$ – vz. met element a, 33
$\emptyset$ – lege verzameling, 33
$\subset$, $\supset$ – deel van, omvat, 33
$\cap$, $\cup$ – doorsnede, vereniging 35
$-$ – verschil, 35
A^c – complement, 36
$\wp(X)$ – machtsverzameling van X, 37
$\bigcup_i A_i$, $\bigcap_i A_i$ – vereniging/doorsnede, 38
(a, b) – geordend paar, 41
$A \times B$ – product, 42
A^2 – $A \times A$, 42
xRy, $R(x, y)$, $(x, y) \in R$ – 43
$Dom(R)$ – domein van R, 43
$Ran(R)$ – beeld van R, 43
Δ_A – identiteitsrelatie op A, 44
R^* – inverse van R, 44
$mod(n)$ – modulo n, 46
$|\, a \,|_R$ – eq. klasse van a modulo R, 46
A/R – quotient van A mod R, 47
$Dom(f)$ – domein van f, 51
$Ran(f)$ – beeld van f, 51
$f(x)$ – beeld van x onder f, 51
$x \mapsto y$ – y beeld van x, 51
$f : X \rightarrow Y$ – f functie van X naar Y, 52
1_X – identiteitsfunctie op X, 52
$f|A$ – beperking van f tot A, 53
$f[A]$ – beeld van A onder f, 53
$f^{-1}[B]$ – origineel van B onder f, 53
$\xrightarrow{\text{op}}$ – surjectie, 55
$\xrightarrow{1-1}$ – injectie, 55
$g \circ f$, gf – compositie van f en g, 56
f^{-1} – inverse van f, 58

$\prod_i X_i$ – product der X_i, 62
X^I – verzameling van functies : $I \to X$, 62
$\sim$ – gelijkmachtig met, 70
$\bot$, $\top$ – falsum/verum, 89
$\vdash$ – afleidbaar (uit), 96
$\gamma \models \varphi$ – γ vervult φ, 98
$\Gamma \models \varphi$ – φ volgt logisch uit Γ, 99
$\models \varphi$ – φ logisch geldig, 99
$\preceq$ – machtigheid hoogstens gelijk aan, 103
$\prec$ – machtigheid kleiner dan, 105
$|A|$ – kardinaalgetal van A, 111
$\aleph_0$ – kardinaal van $\mathbb{N}$, 111
$+$ – (kardinale) som, 111
$\times$ – (kardinaal) product, 111
$\aleph_\xi$ – ξ-de alef, 111
$\cong$ – isomorf, 122
$|(A, <)|$ – ordetype van $(A, <)$, 128
ω – ordetype van $(\mathbb{N}, <)$, 128
ζ – ordetype van $(\mathbb{Z}, <)$, 128
η – ordetype van $(\mathbb{Q}, <)$, 128
λ – ordetype van $(\mathbb{R}, <)$, 128
α^* – inverse van α, 128
$\mathcal{A} + \mathcal{B}$ – som ordeningen, 135
$\alpha + \beta$ – som typen, 136
$\sum_{a \in A} \mathcal{B}_a$ – gegen. som, 137
$\mathcal{A} \times \mathcal{B}$ – product ordeningen, 138
$\alpha \cdot \beta$ – product typen, 138
sup, *inf* – supremum/infimum, 139/40