

Verzamelingenleer

K. P. Hart

Najaar 2013

Inhoudsopgave

0. Cantor's verzamelingenleer	1
Algebraïsche getallen	1
Intervallen, vlakken,	2
Een bijectie tussen P en $[0, 1]$	3
Topologie en verzamelingenleer	4
Deel 1, [1879]	4
Deel 2, [1880]	4
Deel 3, [1882]	5
Deel 4, [1883a]	6
Deel 5, [1883b]	6
Deel 6, [1884]	7
Het Diagonaalargument	7
\mathbb{Q} is uniek	8
1. Naïeve verzamelingenleer	11
Kardinaalgetallen	11
Vergelijken van Machtigheden	12
Sommen en producten	13
Machtsverheffing	14
Ordetypen	15
Rekenen met ordetypen	16
Welgeordende verzamelingen	18
Ordinaalgetallen	19
Kanonieke representanten	20
Een overaftelbaar ordinaalgetal	21
Ordinaalaritmetiek	22
Optellen	22
Vermenigvuldigen	23
Machtsverheffen	23
De normaalvorm	24
ε -getallen	24
Goodstein-rijen	24
Paradoxen	25
Paradoxen van Burali-Forti en Cantor	25
Paradox van Russell	25
2. Axiomatische verzamelingenleer	27
De taal van de verzamelingenleer	27
Formules	27
Afkortingen	28
Vrije en gebonden variabelen	28

Begrensde kwantoren	29
De Axioma's van Zermelo en Fraenkel	29
Het Keuzeaxioma	30
Opbouw van de verzamelingenleer	30
Drie basale axioma's	30
Nieuwe verzamelingen uit oude	32
Producten, relaties, functies,	33
Ordeningen	35
Ordinaalgetallen	35
De Natuurlijke getallen	36
Inductie en Recursie	38
Kardinaalgetallen	39
Overaftelbare verzamelingen	41
De welordeningsstelling	42
Machten en producten van kardinaalgetallen	44
Regulariteit	45
De Wiskunde in de verzamelingenleer	46
Natuurlijke, gehele en rationale getallen	46
Reële getallen	47
Een paar onafhankelijkheidsresultaten	48
Alleen de lege verzameling	49
Een niet-standaard interpretatie	49
Relativering	49
Het Vervangingsaxioma en het Oneindigheidsaxioma	50
Machtsverzameling	50
Bijlage A. Kettingbreuken	52
Van rij naar getal	52
Van getal naar rij	52
Het is een bijectie	53
Het is een homeomorfisme	54
Verdere opmerkingen	54
Bijlage B. Enige Logica	55
Propositielogica	55
Logisch gevolg en consistentie	55
Afleidingen	56
Eerste-orde Logica	57
Taal	57
Theorieën	57
Afleidingen	58
Structuren	58
Volledigheid en compactheid	58
Bibliografie	61
Index	63

Cantor's verzamelingenleer

Dit hoofdstuk geeft een overzicht van de verzamelingenleer zoals die door Cantor aan het eind van de 19de eeuw ontwikkeld en beoefend werd.

Algebraïsche getallen

Weinig wiskundigen zullen betwisten dat de volgende stelling het begin van de verzamelingenleer betekende.

Wenn eine nach irgendeinem Gesetze gegebenen unendliche Reihe von einander verschiedener reeller Zahlgrößen

$$\omega_1, \omega_2, \dots, \omega_\nu, \dots \tag{4}$$

vorliegt, so läßt sich in jedem vorgegebenen Intervalle ($\alpha \dots \beta$) eine Zahl η (und folglich unendlich viele solcher Zahlen) bestimmen, welche in der Reihe (4) nicht vorkommt; dies sol nun bewiesen werden. G. Cantor [1874]

Wie de titel van Cantor's artikel leest — *Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen* — denkt niet meteen aan verzamelingenleer maar eerder aan algebra of analyse: algebraïsche getallen, dat zijn nulpunten van polynomen met gehele coëfficiënten, wat heeft de verzamelingenleer daar nou mee te maken?

Het antwoord wordt duidelijk als je het artikel leest; je vindt daarin twee stellingen die beide duidelijk een verzameling-achtig karakter hebben. De eerste luidt, in hedendaagse bewoording.

0.1. STELLING. *De verzameling der reële algebraïsche getallen is aftelbaar.*

BEWIJS. Als α een algebraïsch getal is dan is er een polynoom p met gehele coëfficiënten, zó dat $p(\alpha) = 0$. Schrijf dit polynoom als $p(x) = a_0 + a_1x + \dots + a_nx^n$ en noem het natuurlijke getal

$$N = n - 1 + |a_0| + |a_1| + \dots + |a_n|$$

de *hoogte* van p . De kleinste hoogte van een polynoom met x als nulpunt noemen we dan de *hoogte* van het algebraïsche getal x .

Bij elk natuurlijk getal N zijn er maar eindig veel polynomen met hoogte N en dus maar eindig veel algebraïsche getallen met hoogte N . Dit helpt ons een lijst van alle algebraïsche getallen te maken: eerst sorteren we de getallen per hoogte en we gebruiken de ordening van \mathbb{R} om getallen van gelijke hoogte te ordenen. Op deze manier construeren we een rij

$$a_0, a_1, a_2, \dots, a_n, \dots$$

waarin elk algebraïsch getal precies één keer voorkomt. □

De tweede stelling uit het artikel is aan het begin van deze paragraaf geciteerd. Cantor's bewijs gaat als volgt.

BEWIJS. Neem een willekeurig interval (α, β) en noteer met α_1 en β_1 de eerste twee getallen uit de rij (4) in dat interval en zó dat $\alpha_1 < \beta_1$; evenzo zijn α_2 en β_2 de eerste twee getallen uit de rij die in (α_1, β_1) liggen, waarbij $\alpha_2 < \beta_2$. Op dezelfde manier bepalen we de termen α_3 en β_3 , enzovoorts. De getallen $\alpha_1, \alpha_2, \dots$ zijn dus termen van de rij (4) wiens indices een strikt stijgende rij vormen en hetzelfde geldt voor de getallen β_1, β_2, \dots ; verder vormen de getallen $\alpha_1, \alpha_2, \dots$ een stijgende rij en getallen β_1, β_2, \dots een dalende rij. De intervallen $[\alpha, \beta], [\alpha_1, \beta_2], [\alpha_2, \beta_2], \dots$ vormen een dalende rij. We moeten nu twee gevallen onderscheiden.

Of het aantal zo gevonden intervallen is eindig, zeg $[\alpha_n, \beta_n]$ is het laatste. In dat geval zit er in (α_n, β_n) nog maar ten hoogste één term uit de rij (4), er zit dus zeker nog een getal η dat niet in (4) voorkomt, waarmee de stelling in dit geval bewezen is.

Of het aantal intervallen is oneindig groot. Omdat beide rijen monotoon en begrensd zijn bestaan de limieten $\alpha_\infty = \lim \alpha_n$ en $\beta_\infty = \lim \beta_n$. Als $\alpha_\infty = \beta_\infty$ (wat bij de rij der algebraïsche getallen zeker gebeurt) dan is $\eta = \alpha_\infty = \beta_\infty$ als gewenst, hetgeen men eenvoudig uit de definitie van de intervallen afleidt. Als $\alpha_\infty < \beta_\infty$ dan voldoet elk getal η in $(\alpha_\infty, \beta_\infty)$ en ook de getallen α_∞ en β_∞ aan de eisen. \square

Intervallen, vlakken, . . .

In een volgend artikel — *Ein Beitrag zur Mannigfaltigkeitslehre* — onderzocht Cantor de relatie tussen \mathbb{R} en \mathbb{R}^n wat betreft het bestaan van bijecties. Het hoofdresultaat was de volgende stelling.

(A.) Sind x_1, x_2, \dots, x_n voneinander unabhängige, veränderliche reele Größen, von denen jede alle Werte, die ≥ 0 und ≤ 1 sind, annehmen kann, und ist t eine andere Veränderliche mit dem gleichen Spielraum ($0 \leq t \leq 1$), so ist es möglich, die Größe t dem Systeme der n Größen x_1, x_2, \dots, x_n so zuzuordnen, daß zu jedem bestimmten Werte von t ein bestimmtes Wertsystem x_1, x_2, \dots, x_n und umgekehrt zu jedem bestimmten Wertsysteme x_1, x_2, \dots, x_n ein gewisser Wert von t gehört.

G. Cantor [1878]

Het directe gevolg is dat een lijn en een vlak of, meer algemeen, de n -dimensionale ruimte één-één-duidelijk op elkaar afgebeeld kunnen worden. Het bewijs van de hoofdstelling verliep nogal indirect. Eerst bewees Cantor een gelijklopende stelling waarbij alle grootheden alleen *irrationale* waarden in het interval $[0, 1]$ aannemen. Een irrationaal getal e in het interval $[0, 1]$ laat zich namelijk als een kettingbreuk schrijven (zie Bijlage A):

$$e = \frac{1}{\alpha_1 + \frac{1}{\alpha_2 + \frac{1}{\alpha_3 + \frac{1}{\ddots}}}}$$

hierin zijn de α_i natuurlijke getallen (ongelijk aan 0). Uit de theorie van de kettingbreuken volgt dat deze schrijfwijze een bijectie tussen de irrationale getallen enerzijds en de oneindige rijen natuurlijke getallen anderzijds bepaalt. Nu is het eenvoudig een n -tal

irrationale getallen aan één enkel irrationaal getal te koppelen: als

$$\begin{aligned} e_1 &= (\alpha_{1,1}, \alpha_{1,2}, \dots, \alpha_{1,\nu}, \dots) \\ &\dots \\ e_\mu &= (\alpha_{\mu,1}, \alpha_{\mu,2}, \dots, \alpha_{\mu,\nu}, \dots) \\ &\dots \\ e_n &= (\alpha_{n,1}, \alpha_{n,2}, \dots, \alpha_{n,\nu}, \dots) \end{aligned}$$

dan bepaalt dat n -tal een irrationaal getal d als volgt

$$d = (\beta_1, \beta_2, \dots, \beta_\nu, \dots)$$

waarbij

$$\beta_{(\nu-1)n+\mu} = \alpha_{\mu,\nu} \quad (\mu = 1, 2, \dots, n; \nu = 1, 2, 3, \dots) \quad (1)$$

Dit werkt ook omgekeerd: als d gegeven is dan laat formule (1) ons een n -tal irrationale getallen bepalen. Op deze manier hebben we een bijjectie tussen P en P^n gemaakt, waarbij P de verzameling irrationale getallen in $(0, 1)$ voorstelt.

Een bijjectie tussen P en $[0, 1]$

Al wat Cantor toen nog te doen stond was een bijjectie tussen P en $[0, 1]$ te maken. Dat ging in een aantal stappen.

- **1.** De rationale getallen in $[0, 1]$ vormen een aftelbare verzameling Q . *Hint:* Schrijf elk rationaal getal q als breuk m/n met m en n relatief priem en schrijf $N = m + n$. Volg nu het bewijs van de aftelbaarheid van de verzameling der algebraïsche getallen.

Kies een stijgende rij $\langle \varepsilon_\nu \rangle_\nu$ van irrationale getallen in $[0, 1]$ met limiet 1, bijvoorbeeld $\varepsilon_\nu = 1 - \sqrt{2} \times 2^{-\nu}$. Zij verder $G = [0, 1] \setminus (Q \cup \{\varepsilon_\nu : \nu = 1, 2, 3, \dots\})$.

- **2.** Er is een bijjectie tussen P en $F = G \cup Q$.

Rest nog te bewijzen dat er een bijjectie bestaat tussen F en $[0, 1]$.

- **3.** Er bestaat een bijjectie tussen $(0, 1)$ en $[0, 1]$. *Hint:* Klap $(0, \frac{1}{2}]$ om, klap $(\frac{1}{2}, \frac{3}{4}]$ om, klap $(\frac{3}{4}, \frac{7}{8}]$ om, ...
- **4.** Er bestaat een bijjectie tussen $(0, 1)$ en $[0, 1]$.
- **5.** Er bestaat een bijjectie tussen F en $[0, 1]$. *Hint:* Er is een bijjectie tussen $[0, \varepsilon_1]$ en $[0, \varepsilon_1]$, er is een bijjectie tussen $(\varepsilon_1, \varepsilon_2)$ en $(\varepsilon_1, \varepsilon_2]$, er is een bijjectie tussen $(\varepsilon_2, \varepsilon_3)$ en $(\varepsilon_2, \varepsilon_3]$, ...

Cantor merkte op dat een bijjectie tussen $[0, 1]$ en P ook makkelijker aan te geven was.

- **6.** Neem een aftelling $\{q_\nu : \nu \in \mathbb{N}\}$ van Q en definieer $f : [0, 1] \rightarrow P$ door $f(x) = x$ als $x \in G$, en verder $f(\varepsilon_\nu) = \varepsilon_{2\nu}$ en $f(q_\nu) = \varepsilon_{2\nu-1}$ voor alle ν . Toon aan dat f een bijjectie is.

Aan het eind van het artikel staan nog twee opmerkelijke zaken.

Ten eerste bewees Cantor dat er zelfs een bijjectie bestaat tussen $[0, 1]$ en de Hilbertkubus $[0, 1]^\infty$. Dit is duidelijk zodra het volgende is afgeleid.

- **7.** De functie $(m, n) \mapsto m + \frac{1}{2}(m+n-1)(m+n-2)$ definieert een bijjectie van $\mathbb{N} \times \mathbb{N}$ naar \mathbb{N} . NB \mathbb{N} begint bij 1.

Ten tweede maakte Cantor een aantal opmerkingen over het indelen van de oneindige deelverzamelingen van \mathbb{R} in klassen: X en Y behoren tot de zelfde klasse als er een bijectie tussen X en Y bestaat. Daarna schreef Cantor het volgende

Durch ein Induktionsverfahren, auf dessen Darstellung wir hier nicht näher eingehen, wird der Satz nahe gebracht, daß die Anzahl der nach diesem Einteilungsprinzip sich ergebenden Klassen linearer Mannigfaltigkeiten eine endliche und zwar, daß sie gleich *Zwei* ist. G. Cantor [1878]

Hier staat dat Cantor vermoedde, en zelfs dacht te kunnen bewijzen, dat er voor een oneindige deelverzameling X van \mathbb{R} (maar) twee mogelijkheden zijn: er is een bijectie tussen X en \mathbb{N} of er is een bijectie tussen X en \mathbb{R} . Dit is wat nu de Continuum Hypothese heet en sinds 1963 weten we dat Cantor dit nooit had kunnen bewijzen.

Topologie en verzamelingenleer

In een artikel — *Über unendliche lineare Punktmannigfaltigkeiten* — dat in zes delen verscheen zette Cantor zijn resultaten over deelverzamelingen van \mathbb{R} (en in het algemeen de \mathbb{R}^n) uiteen.

Deel 1, [1879]

Hierin vinden we definities van *verdichtingspunt* (Grenzpunkt) en *afgeleide verzamelingen*; deze noties had Cantor al eerder ingevoerd, bij zijn onderzoek aan uniciteitsvragen bij Fourierreeksen.

We noemen x een verdichtingspunt van P als elke omgeving van x oneindig veel punten van P bevat. De afgeleide van een deelverzameling P van \mathbb{R} , genoteerd P' , is de verzameling van alle verdichtingspunten van P . Hoewel P' geen deelverzameling van P hoeft te zijn vormen de hogere afgeleiden wel een dalende rij van verzamelingen:

$$P' \supseteq P'' \supseteq P''' \supseteq \dots \supseteq P^{(\nu)} \supseteq \dots$$

Een verzameling P is van de *eerste soort* als er een natuurlijk getal ν bestaat zó dat $P^{(\nu)}$ een lege afgeleide heeft; anders is P van de *tweede soort*.

Nu is een verzameling P die in een interval $[\alpha, \beta]$ *overal dicht* is, zeker van de tweede soort: het interval $[\alpha, \beta]$ is een deel van elke afgeleide. Cantor beloofde in een later deel op de vraag terug te komen of het omgekeerde ook waar is: bestaat voor een verzameling van de tweede soort een interval waarin deze overal dicht ligt?

- 8. Een punt x is een *verdichtingspunt* van een verzameling P als voor elke $\varepsilon > 0$ een punt $p \in P$ bestaat ongelijk aan x en met $d(p, x) < \varepsilon$.
 - a. Bewijs: P is gesloten dan en slechts dan als $P' \subseteq P$.
 - b. Bewijs: P' is gesloten.

Dit deel eindigt met een definitie van gelijkmatigheid en een uitgebreide versie van het bewijs uit het artikel [1874] dat \mathbb{R} niet aftelbaar is.

Deel 2, [1880]

In dit deel zien we het begin van een theorie van ordinaalgetallen, niet als orde-typen van welgeordende verzamelingen maar meer als een manier om steeds hogere afgeleiden van verzamelingen te kunnen noteren: $P^{(\infty)}$ is de doorsnede van de afgeleiden $P^{(\nu)}$,

$P^{(\infty+1)}$ is de afgeleide van $P^{(\infty)}$, $P^{(\infty+\nu)}$ is de ν -afgeleide van $P^{(\infty)}$, de doorsnede van de zo verkregen afgeleiden is $P^{(2\infty)}$, \dots , de doorsnede van $P^{(\infty)}$, $P^{(2\infty)}$, $P^{(3\infty)}$, \dots wordt met $P^{(\infty^2)}$ genoteerd. Zo voortgaand definieerde Cantor voor elke ‘polynomiale uitdrukking’ $n_0\infty^\nu + n_1\infty^{\nu-1} + \dots + n_\nu$ een bijbehorende afgeleide verzameling. Daar hield Cantor niet op: $P^{(\infty^\infty)}$ is de doorsnede van $P^{(\infty)}$, $P^{(\infty^2)}$, $P^{(\infty^3)}$, \dots enzovoorts, enzovoorts. Cantor liet ook zien dat voor elke index η verzamelingen bestaan waarvoor de η -de afgeleide niet leeg is en de $\eta + 1$ -ste afgeleide wel leeg is.

- 9. De convergente rij $P_1 = \{0\} \cup \{2^{-n} : n \in \mathbb{N}\}$ heeft een afgeleide die uit één punt bestaat.
- 10. Neem in elk interval $[2^{-(n+1)}, 2^{-n}]$ een kopie van P_1 met $2^{-(n+1)}$ als limiet; de zoverkregen verzameling P_2 voldoet aan $P_2'' = \{0\}$.
- 11. Construeer voor elke n een verzameling P_n in $[0, 1]$ met $P_n^{(n)} = \{0\}$.
- 12. Construeer een verzameling P_∞ met $P_\infty^{(\infty)} = \{0\}$.

Deel 3, [1882]

Cantor begon met op te merken dat veel van wat hij in de eerste twee delen gedaan had ook voor deelverzamelingen van \mathbb{R}^n geformuleerd en bewezen kon worden. Hij bewees daarna twee, nog steeds welbekende stellingen.

Satz. In einem n -dimensionale überall ins Unendliche ausgedehnten stetigen raume A sei eine unendliche Anzahl von n -dimensionalen stetigen, von einander getrennten und höchstens an ihren Begrenzungen zusammenstoßenden Teilgebieten (a) definiert; die Mannigfaltigkeit (a) solcher Teilgebiete ist immer abzählbar. G. Cantor [1882]

In wat modernere taal: elke paarsgewijs disjuncte familie niet-lege open deelverzamelingen van \mathbb{R}^n is aftelbaar.

- 13. Bewijs deze stelling.

De tweede stelling is in feite zuiver topologisch: nadat in een gebied (dat is een *samenhangende* open verzameling) A een aftelbare verzameling M gekozen is vervolgt Cantor met

Denkt man sich aus dem Gebiete A die abzählbare Punktmenge (M) entfernt und das alsdan übrig gebliebene Gebiet mit \mathfrak{A} bezeichnet, so besteht der merkwürdiger Satz, daß für $n \geq 2$ das gebiet \mathfrak{A} *nicht aufhört, stetig zusammenhangend* zu sein, daß mit anderen Worten je zwei Punkte N und N' des gebietes \mathfrak{A} immer verbunden werden können durch eine *stetige Linie*, welche mit allen ihren Punkten dem Gebiete \mathfrak{A} angehört, so daß auf ihr kein einziger Punkt der Menge (M) liegt. G. Cantor [1882]

Kortweg: als men uit een samenhangende open verzameling in \mathbb{R}^n , met $n \geq 2$, een aftelbare verzameling weglaat is het resultaat nog steeds wegsamenhangend.

- 14. Bewijs deze stelling voor het geval $A = \mathbb{R}^2$. *Hint:* Neem, gegeven twee punten a en b in het complement, de middelloodlijn van a en b en bekijk voor elk punt c op die middelloodlijn het gebroken lijnstuk $[a, c, b]$; bewijs dat maar aftelbaar veel van die gebroken lijnstukken de verzameling (M) kunnen snijden.

Deel 4, [1883a]

Dit deel bevat een onderzoek naar eigenschappen van de afgeleide verzamelingen die in Deel 2 waren ingevoerd. Cantor noemde een verzameling Q die aan $Q \cap Q' = \emptyset$ voldoet *geïsoleerd*, wij zeggen tegenwoordig (relatief) discreet. In het volgende is elke verzameling begreemd verondersteld.

- ▶ **15.** Een relatief discrete deelverzameling Q van \mathbb{R}^n is aftelbaar. *Hint:* Kies voor $q \in Q$ een $\rho_q > 0$ zó dat $d(q', q) \geq \rho_q$ als $q' \in Q$ en $q' \neq q$. Pas de eerste stelling uit Deel 3 toe op de familie bollen $B(q, \frac{1}{2}\rho_q)$.
- ▶ **16.** Als P' aftelbaar is dan is P aftelbaar. *Hint:* $P \setminus P'$ is relatief discreet.
- ▶ **17.** Als $P^{(\infty)}$ aftelbaar is dan is P aftelbaar. *Hint:* $P' = (P' \setminus P'') \cup (P'' \setminus P''') \cup \dots \cup P^{(\infty)}$.
- ▶ **18.** Als voor een index α de afgeleide $P^{(\alpha)}$ aftelbaar is dan is P aftelbaar.
- ▶ **19.** Neem aan P' is aftelbaar en zij $Q = P \cup P'$. Dan bestaat voor elke $\varepsilon > 0$ een eindige familie intervallen die Q overdekt en waarvan de som der lengten kleiner is dan ε .

Deel 5, [1883b]

Dit is het grootste artikel uit de reeks. Na een korte beschrijving van het voorafgaande gaf Cantor een uitgebreide (filosofische) beschouwing over zijn visie op het oneindige.

Daarna besprak hij twee constructies van de reële getallen uit de rationale getallen, die door Weierstraß en Dedekind en gaf daarna nog een constructie door middel van *Fundamentaalrijen* (Cauchy-rijen). Deze is later door Hausdorff gebruikt om voor elke metrische ruimte een completering te construeren.

Vervolgens nam hij de draad van de verzamelingen en hun afgeleiden weer op. Hij noemde een verzameling *perfect* als deze gelijk is aan zijn afgeleide (dus gesloten en elk punt is verdichtingspunt). Hoewel zo'n verzameling van de tweede soort is en zelfs gelijk aan al zijn afgeleiden hoeft deze nog geen interval te bevatten.

Als ein Beispiel einer perfekten Punktmenge, die in keinem noch so kleinen Intervall überall dicht ist, führe ich den Inbegriff aller reellen Zahlen an, die in der Formel

$$z = \frac{c_1}{3} + \frac{c_2}{3^2} + \dots + \frac{c_\nu}{3^\nu} + \dots$$

enthalten sind, wo die Koeffizienten c_ν nach Belieben die beiden Werte 0 und 2 annehmen haben und die Reihe sowohl aus einer endlichen, wie aus einer unendlichen Anzahl von Gliedern bestehen kann. G. Cantor [1883b]

Dit is de beschrijving van *de* Cantorverzameling.

- ▶ **20.** Toon aan dat de Cantorverzameling inderdaad de geclaimde eigenschappen heeft: perfect en er past geen interval in.

De rest van Deel 5 gaat weer over de ordinaalgetallen, waarbij ∞ vervangen is door ω . De optelling en vermenigvuldiging worden symbolisch, uitgaande van de bovenbeschreven schrijfwijze, gedefinieerd.

Deel 6, [1884]

Dit laatste deel opent met een stelling die meermalen zijn nut in de Analyse bewezen heeft. De stelling betreft een abstracte eigenschap van deelverzamelingen van een \mathbb{R}^n , door Cantor met Υ aangeduid. Die eigenschap moet aan twee eisen voldoen

1. Als P een begrensde deelverzameling van \mathbb{R}^n met eigenschap Υ is en men overdekt P met eindig veel gesloten verzamelingen F_1, F_2, \dots, F_m dan is er een i zó dat $P \cap F_i$ eigenschap Υ heeft.
2. Als P eigenschap Υ heeft en $Q \supseteq P$ dan heeft Q ook eigenschap Υ .

Voorbeelden zijn: ‘is oneindig’ of ‘is overaftelbaar’.

De stelling luidt dan.

0.2. STELLING. *Als P begrensde is en eigenschap Υ heeft dan is er een punt a zó dat voor elke $\varepsilon > 0$ de doorsnede $B(a, \varepsilon) \cap P$ eigenschap Υ heeft,*

- 21. Bewijs de stelling.
- a. Neem aan dat P in een blok $B = \{x \in \mathbb{R}^n : a_i \leq x_i \leq b_i \text{ voor } i \leq n\}$ ligt. Verdeel B in 2^n deelblokken $\{B_i : i \leq 2^n\}$ door elke zijde te halveren. Voor tenminste één van die blokken B_i geldt dat $P \cap B_i$ eigenschap Υ heeft.
 - b. Er is een dalende rij blokken B_1, B_2, B_3, \dots , waarvan de diameters naar 0 convergeren en zó dat voor elke i de doorsnede $P \cap B_i$ eigenschap Υ heeft.
 - c. De doorsnede van de B_i bestaat uit één punt en dat punt is als gewenst.
- 22. a. Elke begrensde oneindige deelverzameling van \mathbb{R}^n heeft een verdichtingspunt.
Hint: Gebruik ‘is oneindig’.
- b. De eenheidskubus $\{x \in \mathbb{R}^n : 0 \leq x_i \leq 1 \text{ voor } i \leq n\}$ is compact. *Hint:* Zij \mathcal{U} een open overdekking; en bekijk de eigenschap ‘geen eindige deelfamilie van \mathcal{U} overdekt’.

Het Diagonaalargument

In 1890–91 publiceerde Cantor een artikel — *Über eine elementare Frage der Mannigfaltigkeitslehre* — waarin hij bewees (nogmaals) dat er overaftelbare verzamelingen bestaan. Hij merkte op dat hij dat al eerder gedaan had maar

Es läßt sich aber von jenem Satze ein viel einfacher Beweis liefern, der unabhängig von der Betrachtung der Irrationalzahlen ist.

Sind nämlich m und w irgend zwei einander ausschließende Characteren, so betrachten wir einen Inbegriff M von Elementen

$$E = (x_1, x_2, \dots, x_\nu, \dots),$$

welche von unendlich vielen Koordinaten $x_1, x_2, \dots, x_\nu, \dots$ abhängen. wo jede dieser Koordinaten entweder m oder w ist. M sei die Gesamtheit aller Elemente E .

Zu den Elementen von M gehören beispielsweise die folgende drei:

$$\begin{aligned} E^I &= (m, m, m, m, \dots), \\ E^{II} &= (w, w, w, w, \dots), \\ E^{III} &= (m, w, m, w, \dots). \end{aligned}$$

Ich behaupte nun, daß eine solche Mannigfaltigkeit M nicht die Mächtigkeit der Reihe 1, 2, \dots , ν , \dots hat. G. Cantor [1890]

In het bewijs introduceerde Cantor het beroemde diaonaalargument.

BEWIJS. Laat $E_1, E_2, \dots, E_\nu, \dots$ een of andere rij elementen van M zijn; er bestaat een element E_0 van M dat ongelijk is aan elke E_ν .

Hiertoe schrijven we

$$\begin{aligned} E_1 &= (a_{1,1}, a_{1,2}, \dots, a_{1,\nu}, \dots), \\ E_2 &= (a_{2,1}, a_{2,2}, \dots, a_{2,\nu}, \dots), \\ &\dots \\ E_\mu &= (a_{\mu,1}, a_{\mu,2}, \dots, a_{\mu,\nu}, \dots), \\ &\dots \end{aligned}$$

Hier zijn de $a_{\mu,\nu}$ gelijk aan m of w . We definiëren nu een rij $b_1, b_2, \dots, b_\nu, \dots$, zó dat b_ν gelijk is aan m of w maar *ongelijk* aan $a_{\nu,\nu}$.

Dus als $a_{\nu,\nu} = m$ dan $b_\nu = w$ en als $a_{\nu,\nu} = w$ dan $b_\nu = m$.

Bekijk nu het element $E_0 = (b_1, b_2, b_3, \dots)$ van M , dan ziet men zonder meer dat de gelijkheid $E_0 = E_\mu$ voor geen enkel natuurlijk getal μ opgaat, omdat voor zo'n μ de gelijkheid $b_\nu = a_{\mu,\nu}$ voor alle ν zou gelden, dus in het bijzonder $b_\mu = a_{\mu,\mu}$, wat door de definitie van b_μ uitgesloten is. \square

Cantor was waarschijnlijk trots op dit bewijs.

Dieser Beweis erscheint nicht nur wegen seiner großen Einfachkeit, sondern namentlich auch aus dem Grund bemerkenswert, weil das darin befolgte Prinzip sich ohne weiteres auf den allgemeinen Satz ausdehnen läßt, daß die Mächtigkeiten wohldefinierter Mannigfaltigkeiten kein Maximum haben oder, was dasselbe ist, daß jeder gegebenen Mannigfaltigkeit L ein andere M an die Seite gestellt werden kann, welche von stärkere Mächtigkeit ist als L . G. Cantor [1890]

Als voorbeeld nam Cantor $L = [0, 1]$ met daarbij als M de verzameling functies met domein L en codomein $\{0, 1\}$.

- 23. Maak een injectieve afbeelding van L naar M .
- 24. Bewijs dat er geen surjectieve afbeelding van L naar M bestaat.

Meer algemeen

- 25. Zij X een verzameling en M de verzameling van alle functies van X naar $\{0, 1\}$.
 - a. Er bestaat een injectie van X naar M .
 - b. Er bestaat geen surjectie van X naar M .

ℚ is uniek

In [1895] en [1897] verscheen, in twee delen, het artikel *Beiträge zur Begründung der transfiniten Mengenlehre*, waarin Cantor zijn verzamelingenleer in definitieve vorm uiteenzette. Hierin vinden we de basiseigenschappen van kardinaal- en ordinaalgetallen en hun rekenkunde. Op die rekenkunde komen we later terug. In §9 bewees Cantor een interessante stelling die een voor die tijd nieuwsoortige uitspraak deed.

Hat man eine einfach geordnete Menge M , welche die drei bedingungen erfüllt:

1. $\overline{M} = \aleph_0$,
2. M hat kein dem Range nach niedrigstes und kein höchstes Element,
3. M ist überalldicht

so ist der Ordnungstypus von M gleich η :

$$\overline{M} = \eta.$$

G. Cantor [1895]

Om te beginnen: ‘einfach geordnet’ is wat we nu lineair geordend noemen; verder is \overline{M} Cantor’s notatie voor het kardinaalgetal van M , \aleph_0 is het kardinaalgetal van \mathbb{N} , daarmee is $\overline{M} = \aleph_0$ een korte schrijfwijze voor ‘ M is aftelbaar’; ten slotte: ‘überalldicht’ is wat we dicht geordend noemen: tussen elk tweetal elementen zit en ander element, en η is het ordetype van \mathbb{Q} , met de gewone ordening.

De stelling zegt dus dat, op isomorfie na, \mathbb{Q} de enige aftelbare, dicht geordende, lineair geordende verzameling zonder minimum en maximum is.

BEWIJS. Neem aftellingen $\{q_i : i \in \mathbb{N}\}$ en $\{m_i : i \in \mathbb{N}\}$ van respectievelijk \mathbb{Q} en M . De (gewone) ordening van \mathbb{Q} noteren we $<$, die van M is \prec . We definiëren, recursief, een bijectie $\pi : \mathbb{N} \rightarrow \mathbb{N}$ zó dat $q_i < q_j$ dan en slechts dan als $m_{\pi(i)} \prec m_{\pi(j)}$. De eerste stap ligt voor de hand: $\pi(1) = 1$.

Neem aan dat $\pi(i)$ gevonden is voor $i \leq n$; we definiëren $\pi(n+1)$. Verdeel $\{1, 2, \dots, n\}$ in twee delen: $A = \{i : q_i < q_{n+1}\}$ en $B = \{i : q_{n+1} < q_i\}$. Er zijn drie gevallen: $A = \emptyset$, $B = \emptyset$ en $A \neq \emptyset \neq B$.

In het eerste geval geldt $q_i < q_{n+1}$ voor alle $i \leq n$; omdat M geen maximum heeft kunnen we een j vinden zó dat $m_{\pi(i)} \prec m_j$ voor alle $i \leq n$. We nemen voor $\pi(n+1)$ de minimale j met die eigenschap.

In het tweede geval geldt $q_{n+1} < q_i$ voor alle $i \leq n$; omdat M geen minimum heeft kunnen we een j vinden zó dat $m_j \prec m_{\pi(i)}$ voor alle $i \leq n$. We nemen voor $\pi(n+1)$ de minimale j met die eigenschap.

In het derde geval nemen we $i_1 \in A$ zó dat q_{i_1} maximaal is en $i_2 \in B$ zó dat q_{i_2} minimaal is. Nu nemen we voor $\pi(n+1)$ de minimale j die aan $m_{\pi(i_1)} \prec m_j \prec m_{\pi(i_2)}$ voldoet.

In woorden: $\pi(n+1)$ is de minimale j met de eigenschap dat m_j ten opzichte van $\{m_{\pi(i)} : i \leq n\}$ dezelfde positie inneemt als q_{n+1} ten opzichte van $\{q_i : i \leq n\}$.

Het is duidelijk dat π een *injectieve* afbeelding is met de gewenste eigenschap. Blijft nog te bewijzen dat π surjectief is.

Met inductie naar l bewijzen we dat $\{1, 2, \dots, l\} \subseteq \pi[\mathbb{N}]$. Het geval $l = 1$ is duidelijk: $\pi(1) = 1$. Bij de stap van l naar $l+1$ kiezen we eerst de minimale n zó dat $\{1, 2, \dots, l\} \subseteq \pi[\{1, 2, \dots, n\}]$. Als $l+1$ al in de laatste verzameling zit hoeven we niets te doen; anders bepalen we, als boven, de positie van m_{l+1} ten opzichte van $\{m_{\pi(i)} : i \leq n\}$. Neem dan eerst de minimale $i_l > n$ zó dat q_{i_l} dezelfde positie ten opzichte van $\{q_i : i \leq n\}$ heeft als m_{l+1} ten opzichte van $\{m_{\pi(i)} : i \leq n\}$. Om de gedachten te bepalen nemen we aan dat $m_{l+1} \prec m_{\pi(i)}$ voor $i \leq n$ en nemen we $i_0 \leq n$ zó dat $q_{i_0} = \min\{q_i : i \leq n\}$ (dus ook $m_{\pi(i_0)}$ is minimaal). De keuze van i_l impliceert nu dat $q_{i_l} < q_{i_0}$ en $q_{i_0} < q_i$ als $n < i < i_l$. De posities van q_{i_l} en m_{l+1} ten opzichte van respectievelijk $\{q_i : i < i_l\}$ en $\{m_{\pi(i)} : i < i_l\}$ zijn dus identiek en blijkbaar volgt nu $\pi(i_l) = l+1$. \square

Dit was een van de eerste, zo niet de eerste, structuurstellingen in de Wiskunde: een korte lijst van eigenschappen die een bepaalde structuur karakteriseert.

Het bewijs is later vereenvoudigd tot een heen-en-weerargument ('back-and-forth argument'). Het komt er op neer dat het bewijs van de surjectiviteit in de constructie zelf wordt ondergebracht.

BEWIJS MET BEHULP VAN DE HEEN-EN-WEERMETHODE. Met recursie bouwen we stijgende rijen $\langle A_n : n \in \mathbb{N} \rangle$ en $\langle B_n : n \in \mathbb{N} \rangle$ met bijecties $\pi_n : A_n \rightarrow B_n$ zó dat voor $i, j \in A_n$ geldt: $q_i < q_j$ dan en slechts dan als $m_{\pi(i)} < m_{\pi(j)}$; verder eisen we dat $n \in A_n$ en $n \in B_n$.

We beginnen met $A_1 = B_1 = \{1\}$ en $\pi_1(1) = 1$.

Als A_n, B_n en π_n gevonden zijn maken we A_{n+1}, B_{n+1} en π_{n+1} in twee stappen. Eerst kijken we of $n+1 \in A_n$; zo ja dan zetten we $A'_n = A_n, B'_n = B_n$ en $\pi'_n = \pi_n$, zo nee dan bepalen we de positie van q_{n+1} ten opzichte van $\{q_i : i \in A_n\}$ en pakken we de eerste $j \in \mathbb{N}$ zó dat m_j dezelfde positie inneemt ten opzichte van $\{m_{\pi_n(i)} : i \in A_n\}$. We zetten $A'_n = A_n \cup \{n+1\}$ en $B'_n = B_n \cup \{j\}$, en we breiden π_n uit tot π'_n door $\pi'_n(n+1) = j$.

In de tweede stap draaien we de rollen om: als $n+1 \in B'_n$ dan zijn we klaar: zet $A_{n+1} = A'_n, B_{n+1} = B'_n$ en $\pi_{n+1} = \pi'_n$. In het andere geval nemen we de eerste j in \mathbb{N} zó dat q_j en m_{n+1} gelijke posities hebben ten opzichte van $\{q_i : i \in A'_n\}$ en $\{m_{\pi'_n(i)} : i \in A'_n\}$; dan definiëren we $A_{n+1} = A'_n \cup \{j\}$, $B_{n+1} = B'_n \cup \{n+1\}$ en $\pi_{n+1}(j) = n+1$.

Nu is gelijk duidelijk dat op deze manier een bijectie $\pi : \mathbb{N} \rightarrow \mathbb{N}$ met de gewenste eigenschappen geconstrueerd wordt. \square

In de Analyse kennen we ook een uniciteitsresultaat.

- **26.** Laat K een linear geordend lichaam zijn dat orde-volledig is, dat wil zeggen, elke niet-lege naar boven begrensde verzameling heeft een supremum. Bewijs dat K isomorf is met \mathbb{R} .

Hoofdstuk 1

Naïeve verzamelingenleer

In dit hoofdstuk bekijken we twee dingen die we in Hoofdstuk 0 hebben overgeslagen, namelijk Cantor's rekenkunde voor kardinaal- en ordinaalgetallen.

De resultaten komen voor het grootste deel uit *Beiträge zur Begründung der transfiniten Mengenlehre*; daarin staat ook Cantor's definitie van 'verzameling'.

Unter einer ‚Menge‘ verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten m unserer Anschauung oder unseres Denkens (welche die ‚Elemente‘ von M genannt werden) zu einem Ganzen.

In Zeichen drücken wir dies so aus:

$$M = \{m\}$$

G. Cantor [1895]

Kardinaalgetallen

Elke verzameling heeft een zekere 'Machtigheid' die ook wel haar 'Kardinaalgetal' genoemd wordt.

‚Mächtigkeit‘ oder ‚Cardinalzahl‘ von M nennen wir den Allgemeinbegriff, welcher mit Hülfe unseres activen Denkvermögens dadurch aus der Menge M hervorgeht, daß von der Beschaffenheit ihrer verschiedenen Elemente m und von der Ordnung ihres Gegebenseins abstrahirt wird.

Das Resultat dieses zweifachen Abstractionsacts, die Cardinalzahl oder Mächtigkeit von M , bezeichnen wir mit

$$\overline{M}$$

G. Cantor [1895]

Om kardinaalgetallen te kunnen vergelijken is meer nodig dan deze definitie.

Zwei Mengen M und N nennen wir ‚äquivalent‘ und bezeichnen dies mit

$$M \sim N \text{ oder } N \sim M$$

wenn es möglich ist, dieselben gesetzmässig in eine derartige Beziehung zu einander zu setzen, dass jedem Element der einen von ihnen ein und nur ein Element der andern entspricht.

G. Cantor [1895]

De eerste definitie klinkt, zeker in het Duits, prachtig maar zegt in feite niets; in een verduidelijking schreef Cantor dat bij genoemde abstractie elk element van M overgaat in een ‚Eins‘ en dat het kardinaalgetal \overline{M} een uit dergelijke ‚Einsen‘ bestaande verzameling is. Gelukkig gaf hij meteen een bewijs dat de formuleringen $\overline{\overline{M}} = \overline{N}$ en $M \sim N$ equivalent zijn en in het vervolg van het artikel wordt gelijkheid van kardinaalgetallen altijd teruggevoerd op equivalentie van de desbetreffende verzamelingen.

Bij dit ‘bewijs’ gebruikte Cantor dat \sim een equivalentierelatie is. Om onze bewijzen wat te kunnen stroomlijnen vertalen we Cantor’s definitie van \sim eerst in hedendaagse termen.

1.1. DEFINITIE. We noemen twee verzamelingen *equivalent*, geschreven $M \sim N$ als er een bijectieve afbeelding $f : M \rightarrow N$ bestaat.

- ▶ 1. a. Voor elke verzameling geldt $M \sim M$.
- b. Voor elk drietal verzamelingen M , N en P geldt: als $M \sim P$ en $N \sim P$ dan $M \sim N$.
- c. Voor elk tweetal verzamelingen M en N geldt: als $M \sim N$ dan $N \sim M$. (Voor Cantor was deze opmerking niet nodig omdat zijn formulering de symmetrie al in zich bergt.)

Vanaf nu gebruiken we huidige notatie $|M|$ voor de machtigheid van een verzameling M . Let wel: strikt formeel betekent $|M|$ niets en de gelijkheid $|M| = |N|$ is een afkorting voor “er is een bijectie tussen M en N ”.

Vergelijken van Machtigheden

Gegeven twee verzamelingen M en N , met kardinaalgetallen $\mathfrak{a} = |M|$ en $\mathfrak{b} = |N|$, die aan twee voorwaarden voldoen

1. er is geen deelverzameling van M die equivalent is met N ,
2. er is een deelverzameling N_1 van N , zó dat $N_1 \sim M$.

- ▶ 2. Aan deze voorwaarden blijft voldaan als M en N door equivalente verzamelingen M' en N' vervangen worden.

De twee voorwaarden drukken dus een relatie tussen de kardinaalgetallen \mathfrak{a} en \mathfrak{b} uit.

- ▶ 3. a. De twee verzamelingen M en N zijn niet equivalent, dus $\mathfrak{a} \neq \mathfrak{b}$.
- b. De omgekeerde relatie tussen \mathfrak{a} en \mathfrak{b} geldt niet, dat wil zeggen: als M en N verwisseld worden is niet aan voorwaarden 1 en 2 voldaan.

In het geval dat aan 1 en 2 voldaan is zeggen we dat \mathfrak{a} kleiner is dan \mathfrak{b} of ook dat \mathfrak{b} groter is dan \mathfrak{a} , kortweg

$$\mathfrak{a} < \mathfrak{b} \text{ of } \mathfrak{b} > \mathfrak{a}$$

We schrijven $\mathfrak{a} \leq \mathfrak{b}$ als $\mathfrak{a} < \mathfrak{b}$ of $\mathfrak{a} = \mathfrak{b}$.

- ▶ 4. Bewijs: als $\mathfrak{a} < \mathfrak{b}$ en $\mathfrak{b} < \mathfrak{c}$ dan $\mathfrak{a} < \mathfrak{c}$.
- ▶ 5. Als \mathfrak{a} en \mathfrak{b} kardinaalgetallen zijn dan geldt ten hoogste één van de relaties $\mathfrak{a} = \mathfrak{b}$, $\mathfrak{a} < \mathfrak{b}$ of $\mathfrak{b} < \mathfrak{a}$.

Blijft de vraag of voor elk tweetal kardinaalgetallen \mathfrak{a} en \mathfrak{b} ten minste één van de relaties $\mathfrak{a} = \mathfrak{b}$, $\mathfrak{a} < \mathfrak{b}$ of $\mathfrak{b} < \mathfrak{a}$ geldt. Cantor beweerde van wel maar bewees dit als gevolg van de vergelijkbaarheid van ordinaalgetallen en, zoals we later zullen zien, de universele vergelijkbaarheid van kardinaalgetallen is equivalent met het Keuzeaxioma.

- ▶ 6. Toon aan: als $\mathfrak{a} \leq \mathfrak{b}$ en $\mathfrak{b} \leq \mathfrak{a}$ dan $\mathfrak{a} = \mathfrak{b}$.

Een alternatieve (en tegenwoordig meer gebruikelijke) definitie van ‘kleiner dan of gelijk’ is de volgende: we schrijven $|M| \preceq |N|$ als er een injectieve afbeelding van M naar N bestaat.

- ▶ 7. Ga na: uit $|M| \leq |N|$ volgt $|M| \preceq |N|$.

De omgekeerde implicatie geldt ook maar kost iets meer moeite om te bewijzen. De reden is dat \leq als ‘ $<$ of $=$ ’ is gedefinieerd, waarbij $<$ een sterke conjunctie van twee uitspraken is. Immers, als $|M| \preccurlyeq |N|$ en $|M| \neq |N|$ dan voldoen we, via \preccurlyeq al aan eis 2 van $<$ maar om eis 1 uit \preccurlyeq en \neq af te leiden is echt wat werk nodig.

Een kleine analyse van het probleem leert dat we de volgende stelling nodig hebben; deze stelling wordt aan, onder meer, Cantor, Bernstein en Schroeder toegeschreven; hij is ook in de nagelaten geschriften van Dedekind ([1932]) gevonden.

1.2. STELLING. *Als er injectieve afbeeldingen $f : M \rightarrow N$ en $g : N \rightarrow M$ bestaan dan is er ook een bijectie $b : M \rightarrow N$.*

Voor we deze stelling bewijzen eerst een hulpresultaat.

- 8. Zij M een verzameling en $h : M \rightarrow M$ een afbeelding. Voor elke $A \subseteq M$ bestaat een kleinste verzameling A_0 zó dat $A \subseteq A_0$ en $h[A_0] \subseteq A_0$.
- De familie $\mathcal{A} = \{X : A \subseteq X \subseteq M \text{ en } h[X] \subseteq X\}$ is niet leeg.
 - De verzameling $A_0 = \bigcap \mathcal{A}$ is als gewenst.
 - Geldt $h[A_0] = A_0$?
- 9. Bewijs Stelling 1.2. Schrijf $h = g \circ f$, $N_1 = g[N]$ en $A = M \setminus N_1$.
- Waarom is het voldoende een bijectie tussen M en N_1 te construeren?
Zij A_0 als in de vorige opgave.
 - Toon aan dat de afbeelding $b : M \rightarrow N_1$, gedefinieerd door

$$b(x) = \begin{cases} h(x) & \text{als } x \in A_0 \\ x & \text{als } x \in M \setminus A_0 \end{cases}$$

een bijectie is.

- 10. Bewijs: $|M| \leq |N|$ dan en slechts dan als $|M| \preccurlyeq |N|$.

Hiermee is het controleren van $|M| \leq |N|$ eenvoudiger geworden: we hoeven slechts het bestaan van een injectieve afbeelding van M naar N te verifiëren.

Sommen en producten

Optellen en vermenigvuldigen van kardinaalgetallen gaat als verwacht.

- 11. Toon aan: als $M \sim M'$ en $N \sim N'$, waarbij $M \cap N = \emptyset = M' \cap N'$, dan geldt ook $M \cup N \sim M' \cup N'$,

Uit deze opgave blijkt dat de volgende definitie van de som van twee kardinaalgetallen $\mathfrak{a} = |M|$ en $\mathfrak{b} = |N|$, met $M \cap N = \emptyset$, onafhankelijk is van de keuze van M en N :

$$\mathfrak{a} + \mathfrak{b} = |M \cup N|$$

Twee verzamelingen, M en N , die niet disjunct zijn kunnen disjunct gemaakt worden: $M' = \{\langle m, 1 \rangle : m \in M\}$ en $N' = \{\langle n, 2 \rangle : n \in N\}$ zijn disjunct en er geldt $M \sim M'$ en $N \sim N'$.

- 12. Toon aan: $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$.

In het algemeen, als $\{M_i : i \in I\}$ een familie verzamelingen is kunnen we een disjuncte familie equivalente verzamelingen maken door de index van de verzameling

als extra ‘coördinaat’ in te voeren. Zo krijgen we de volgende definitie van de som van willekeurig veel kardinaalgetallen:

$$\sum_{i \in I} |M_i| = \left| \bigcup_{i \in I} M_i \times \{i\} \right|$$

► **13.** Bewijs: $\sum_{n \in \mathbb{N}} n = \aleph_0$.

Het product van twee kardinaalgetallen heeft een voor de hand liggende definitie. Als $\mathfrak{a} = |M|$ en $\mathfrak{b} = |N|$ dan definiëren we $\mathfrak{a} \cdot \mathfrak{b} = |M \times N|$.

► **14.** Deze definitie is onafhankelijk van de keuze van M en N .

Een product is, net als in het geval van natuurlijke getallen, op te vatten als een som.

► **15.** Laat, voor elke $n \in N$ een verzameling M_n gegeven zijn met $|M_n| = \mathfrak{a}$ en zij $\mathfrak{b} = |N|$. Bewijs: $\mathfrak{a} \cdot \mathfrak{b} = \sum_{n \in N} |M_n|$.

► **16.** Bewijs de volgende rekenregels

- a. $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a}$
- b. $(\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c})$
- c. $\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}$

Machtsverheffing

Machtsverheffen van kardinaalgetallen gaat als volgt. Voor twee verzamelingen M en N , met kardinaalgetallen \mathfrak{a} en \mathfrak{b} , noteren we met ${}^M N$ de verzameling van alle afbeeldingen van M naar N en we definiëren

$$\mathfrak{b}^{\mathfrak{a}} = |{}^M N|$$

De machtsverheffing voldoet aan de verwachte rekenregels.

► **17.** Bewijs de volgende rekenregels door (natuurlijke) bijecties tussen representerende verzamelingen aan te geven.

- a. $\mathfrak{a}^{\mathfrak{b}} \cdot \mathfrak{a}^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b} + \mathfrak{c}}$
- b. $\mathfrak{a}^{\mathfrak{c}} \cdot \mathfrak{b}^{\mathfrak{c}} = (\mathfrak{a} \cdot \mathfrak{b})^{\mathfrak{c}}$
- c. $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b} \cdot \mathfrak{c}}$

Een toepassing van deze rekenkunde is een sneller bewijs van de stelling dat $[0, 1]$, $[0, 1]^2$, \dots , $[0, 1]^n$, \dots hetzelfde kardinaalgetal hebben.

Van nu af duiden we met \aleph_0 het kardinaalgetal van \mathbb{N} aan en reserveren we de letter \mathfrak{c} (van continuum) voor het kardinaalgetal van $[0, 1]$ (en dus ook van \mathbb{R}).

1.3. STELLING. $\mathfrak{c} = 2^{\aleph_0}$.

► **18.** Toon aan dat de verzameling *fin* van *eindige* deelverzamelingen van \mathbb{N} gelijkmachtig is met \mathbb{N} . *Hint:* Definieer $f : \mathbb{N} \rightarrow \text{fin}$ recursief: $f(1) = \emptyset$ en als $n \geq 0$ en $1 \leq k \leq 2^n$ dan $f(2^n + k) = f(k) \cup \{n + 1\}$.

► **19.** Bewijs Stelling 1.3. *Hint:* Definieer $s : {}^{\mathbb{N}}\{0, 1\} \rightarrow [0, 1]$ door $s(x) = \sum_{i=1}^{\infty} x(i) \cdot 2^{-i}$. Dan is s surjectief maar niet injectief; maak van s , met behulp van de afbeelding f uit de vorige opgave een bijectie.

Nu liggen de gewenste gelijkheden voor het oprapen.

► 20. Bewijs de volgende gelijkheden

- a. $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$
- b. Voor elke n geldt $\mathfrak{c}^n = \mathfrak{c}$
- c. $\mathfrak{c} = 3^{\aleph_0} = 4^{\aleph_0} = \dots = n^{\aleph_0} = \dots = \aleph_0^{\aleph_0} = \mathfrak{c}^{\aleph_0}$,

Het diagonaalargument uit Hoofdstuk 0 (pagina 7) bewijst het lastigste onderdeel van de volgende stelling.

1.4. STELLING. *Voor elk kardinaalgetal \mathfrak{a} geldt $\mathfrak{a} < 2^{\mathfrak{a}}$.*

Ook voor willekeurige families verzamelingen is het product van hun kardinaalgetallen op de voor de hand liggende manier gedefinieerd. Als $\{\mathfrak{a}_i : i \in I\}$ een verzameling kardinaalgetallen is, met representerende verzamelingen M_i , dan definiëren we

$$\prod_{i \in I} \mathfrak{a}_i = \left| \prod_{i \in I} M_i \right|$$

Hierin is $\prod_{i \in I} M_i$ het *Cartesisch product* van de verzamelingen M_i : de verzameling van alle functies $x : I \rightarrow \bigcup_{i \in I} M_i$ die voldoen aan $x(i) \in M_i$ voor alle i .

- 21. Bewijs de volgende algemene formule: $\mathfrak{a}^{\sum_i b_i} = \prod_i \mathfrak{a}^{b_i}$.
- 22. Bewijs: $\prod_{n \in \mathbb{N}} n = \mathfrak{c}$.

Het diagonaalargument kan gebruikt worden om de volgende stelling te bewijzen.

1.5. STELLING (J. König [1905]). *Laat $\{\mathfrak{a}_i : i \in I\}$ en $\{\mathfrak{b}_i : i \in I\}$ twee verzamelingen kardinaalgetallen zijn zó dat $\mathfrak{a}_i < \mathfrak{b}_i$ voor alle i . Dan geldt $\sum_{i \in I} \mathfrak{a}_i < \prod_{i \in I} \mathfrak{b}_i$.*

- 23. Bewijs de stelling van König.
- 24. Bewijs: als $\{A_n : n \in \mathbb{N}\}$ een rij deelverzamelingen van \mathbb{R} is en $|A_n| < \mathfrak{c}$ voor alle n dan geldt $|\bigcup_n A_n| < \mathfrak{c}$.

Tot slot een paar opmerkingen over de monotonie van het machtsverheffen.

- 25. Toon aan: als $|M| \leq |N|$ dan $2^{|M|} \leq 2^{|N|}$.

De exponentiële functie $\mathfrak{a} \mapsto 2^{\mathfrak{a}}$ is dus monotoon-in-de-zwakke-zin: uit $\mathfrak{a} \leq \mathfrak{b}$ volgt $2^{\mathfrak{a}} \leq 2^{\mathfrak{b}}$. De beperking van deze functie tot de eindige kardinaalgetallen is strikt monotoon: als $m < n$ dan $2^m < 2^n$. De vraag dringt zich op of die strikte monotonie ook niet voor oneindige kardinaalgetallen geldt. Het antwoord brengt ons meteen in het gebied van de consistentie en onafhankelijkheid: op grond van de gewone axioma's van de verzamelingenleer, inclusief het Keuzeaxioma, is de strikte monotonie noch te bewijzen noch te weerleggen.

- 26. Bewijs: $2^{\aleph_0} < 2^{\mathfrak{c}}$.

Ordetypen

Zoals elke verzameling een kardinaalgetal heeft, zo heeft elke lineair geordende verzameling een ordetype, in Cantor's woorden:

Jeder geordneten Menge M kommt ein bestimmter ‚Ordnungstypus‘ oder kürzer ein bestimmter ‚Typus‘ zu, den wir mit

$$\overline{M}$$

bezeichnen wollen; hierunter verstehen wir den Allgemeinbegriff, welcher sich aus M ergibt, wenn wir nur von der Beschaffenheit der Elemente m abstrahieren, die Rangordnung unter ihnen aber beibehalten. G. Cantor [1895]

Net als bij machtigheid/kardinaalgetal betekent deze zin niet zoveel maar gelukkig heeft Cantor een equivalente formulering voor “hetzelfde ordetype hebben” waar wel mee te werken is.

We noemen twee lineair geordende verzamelingen $(M, <)$ en $(N, <)$ *isomorf* als er een orde-bewarende bijectie tussen M en N bestaat, dus een bijectie $f : M \rightarrow N$ die voldoet aan: voor elk tweetal elementen x en y van M geldt: als $x < y$ dan $f(x) < f(y)$.

- **27.** Toon aan dat, in bovenstaande situatie, de omgekeerde implicatie ook geldt: als $f(x) < f(y)$ dan $x < y$.

Voor eindige verzamelingen is er geen wezenlijk verschil tussen ordetype en kardinaalgetal.

- **28.** Bewijs: voor elke $n \in \mathbb{N}$ is elk tweetal lineaire ordeningen van $\{1, 2, \dots, n\}$ isomorf.

Als we een natuurlijk getal, n , in de context van ordetypen gebruiken dan bedoelen we daarmee het ordetype van $\{i \in \mathbb{N} : i \leq n\}$.

Het vergelijken van ordetypen is lastiger dan het vergelijken van kardinaalgetallen. De voor de hand liggende definitie — $\overline{M} \leq \overline{N}$ als er een orde-bewarende injectieve afbeelding van M naar N bestaat — heeft een groot nadeel.

- **29.** Toon aan: $\overline{[0, 1]} \leq \overline{(0, 1)}$ en $\overline{(0, 1)} \leq \overline{[0, 1]}$ maar $\overline{[0, 1]} \neq \overline{(0, 1)}$ (de intervallen hebben hun gewone ordening).

We zullen later zien dat een variant op deze definitie een zinvolle vergelijking van ordetypen van *welgeordende* verzamelingen mogelijk maakt.

Rekenen met ordetypen

Ordetypen kunnen bij elkaar opgeteld en met elkaar vermenigvuldigd worden. Hun rekenkunde loopt echter minder glad dan die van de kardinaalgetallen.

Net als bij kardinaalgetallen reserveren we een paar symbolen voor de ordetypen van belangrijke verzamelingen.

- ω is het ordetype van \mathbb{N} met de gewone ordening: $\omega = \overline{\mathbb{N}}$
- η is het ordetype van \mathbb{Q} met de gewone ordening: $\eta = \overline{\mathbb{Q}}$, zie pagina 8
- θ is het ordetype van $[0, 1]$ met de gewone ordening: $\theta = \overline{[0, 1]}$

Vaak willen we een ordetype ‘omkeren’: als $\alpha = \overline{(M, <)}$ dan noteren we $\alpha^* = \overline{(M, >)}$.

- **30.** Ga na:
- a. ω^* is het type van $\{n \in \mathbb{Z} : n \leq 100\}$ met de gewone ordening.
 - b. $\eta^* = \eta$.

De som van twee ordetypen $\alpha = \overline{(M, <_M)}$ en $\beta = \overline{(N, <_N)}$ wordt gedefinieerd door M en N , met behoud van hun gegeven ordeningen, achter elkaar te leggen; formeel schrijven we

$$\alpha + \beta = \overline{(P, <_P)}$$

waarbij $P = (M \times \{0\}) \cup (N \times \{1\})$ en $(p, i) <_P (q, j)$ als

1. $i = 0$ en $j = 1$ of
2. $i = j = 0$ en $p <_M q$ of
3. $i = j = 1$ en $p <_N q$

In woorden: elk element van M komt vóór elk element van N en de elementen van M en N behouden hun gegeven ordening.

► **31.** Bewijs: voor elk drietal ordetypen α , β en γ geldt $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

► **32.** Toon aan

- a. $\omega^* + \omega$ is het ordetype van \mathbb{Z} .
- b. $\eta + 1 + \eta = \eta$

Deze optelling is niet commutatief.

► **33.** a. Toon aan: $1 + \omega = \omega$ en $\omega + 1 \neq \omega$.

- b. Toon aan: $1 + \eta \neq \eta + 1$.

Het product van twee ordetypen $\alpha = \overline{(M, <_M)}$ en $\beta = \overline{(N, <_N)}$ wordt gedefinieerd door β kopiën van α achter elkaar te leggen; in formule

$$\alpha \cdot \beta = \overline{(P, <_P)}$$

waarbij $P = M \times N$ en $(m_1, n_1) <_P (m_2, n_2)$ als

1. $n_1 <_N n_2$ of
2. $n_1 = n_2$ en $m_1 <_M m_2$

Dit is in feite een lexicografische ordening, waarbij de woorden van achter naar voren worden gelezen; in wat meer beeldende termen: in het product $M \times N$ ligt een lager punt altijd voor een hoger punt en elke horizontale lijn is als M geordend.

Sommige rekenregels gelden ook voor ordetypen

► **34.** Toon aan: voor elk drietal ordetypen α , β en γ gelden

- a. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$, en
- b. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

Andere rekenregels gelden juist niet meer

► **35.** Toon aan

- a. $\omega \cdot 2 = \omega + \omega$
- b. $2 \cdot \omega = \omega$
- c. $1 \cdot \omega + 1 \cdot \omega \neq (1 + 1) \cdot \omega$

Dus, de vermenigvuldiging is niet commutatief en slechts aan één kant distributief.

Wel kunnen we, zonder gevaar, eindige machten van ordetypen afspreken: $\alpha^2 = \alpha \cdot \alpha$ en $\alpha^{n+1} = \alpha^n \cdot \alpha$. Het ordetype η is zijn eigen kwadraat.

► **36.** Bewijs: $\eta \cdot \eta = \eta$. *Hint:* Pas de uniciteitsstelling (pagina 8) toe.

Het ordetype η is *universeel* onder de aftelbare ordetypen.

► **37.** Bewijs: elke aftelbare lineair geordende verzameling X is in \mathbb{Q} in te bedden. *Hint:* Bewijs dat $\eta \cdot \bar{X} = \eta$.

Voor θ ligt de zaak wat anders.

► **38.** Bewijs: $\theta \cdot \theta \neq \theta$.

Welgeordende verzamelingen

Een lineair geordende verzameling heet *welgeordend* als elke niet-lege deelverzameling een kleinste element heeft. Het inductieaxioma van Peano zegt in feite niets anders dan dat \mathbb{N} , met de gewone ordening, een welgeordende verzameling is.

- **39.** Definieer \prec op \mathbb{N} door $m \prec n$ als m even is en n oneven of als m en n beide even of beide oneven zijn $m < n$. Toon aan dat \prec een welordering is. Wat is $(\overline{\mathbb{N}}, \prec)$?

De ‘populariteit’ van welgeordende verzamelingen is te danken aan het feit dat ze *transfinite* inductie en recursie mogelijk maken. Hiertoe hebben we de volgende notie en notatie nodig. Een *beginstuk* van een welgeordende verzameling (X, \prec) is een deelverzameling A die voldoet aan: als $x \in A$ en $y \prec x$ dan $y \in A$.

- **40.** Toon aan:
- Elke verzameling van de vorm $\hat{p} = \{x \in X : x \prec p\}$ is een beginstuk.
 - Elk beginstuk dat niet gelijk is aan X is van de vorm \hat{p} .

1.6. STELLING (Inductieprincipe). Zij (X, \prec) een welgeordende verzameling en $A \subseteq X$ zó dat voor elke $x \in X$ geldt: als $\{y : y \prec x\} \subseteq A$ dan $x \in A$. Dan geldt $A = X$.

Het bewijs loopt via contrapositie: als $A \neq X$, neem dan $p = \min(X \setminus A)$, dan geldt $\{y : y \prec p\} \subseteq A$ en $p \notin A$.

Voor een alternatieve formulering van dit principe lopen we wat op de feiten vooruit en noteren we, in een welgeordende verzameling X de directe opvolger van een element x , zo die er is, met $x+1$, dus als x niet het maximum van X is dan $x+1 = \min\{y : x \prec y\}$. Voorts noemen we x een limiet in X als er geen $y \prec x$ is met $x = y+1$.

- **41.** Neem aan $A \subseteq X$ voldoet aan: 1) $\min X \in A$, 2) als $x \in A$ dan $x+1 \in A$, en 3) als x een limiet is en $\hat{x} \subseteq A$ dan ook $x \in A$. Dan geldt $A = X$.
- **42.** Als (X, \prec) welgeordend is en $f : X \rightarrow X$ is strikt stijgend dan geldt voor alle $x \in X$ dat $x \preceq f(x)$. *Hint:* Zij $A = \{x : x \preceq f(x)\}$; bewijs $A = X$.
- **43.** Als (X, \prec) en $(Y, <)$ isomorfe welgeordende verzamelingen zijn dan is er slechts één isomorfisme tussen X en Y . *Hint:* Laat f en g isomorfismen zijn; bewijs $\{x : f(x) = g(x)\} = X$.

Het inductieprincipe maakt bewijzen mogelijk; constructies gebruiken het recursieprincipe.

1.7. STELLING (Recursieprincipe). Zij (X, \prec) een welgeordende verzameling, Y een verzameling en \mathcal{F} de verzameling van alle afbeeldingen die als domein een beginstuk van X hebben en Y als co-domein. Dan bestaat bij elke afbeelding $F : \mathcal{F} \rightarrow Y$ een unieke afbeelding $f : X \rightarrow Y$ die voldoet aan $f(x) = F(f \upharpoonright \hat{x})$ voor alle x .

Het bewijs van het Recursieprincipe is een goede oefening in het werken met welordeningen.

- **44.** Zij \mathcal{G} de deelfamilie van \mathcal{F} die uit alle benaderingen van de gewenste afbeelding bestaat, dat zijn functies g die voldoen aan $g(x) = F(g \upharpoonright \hat{x})$ voor alle x in hun domein.
- \mathcal{G} is niet leeg: in \mathcal{G} zitten de lege functie en $\{\langle \min X, F(\emptyset) \rangle\}$.
 - Als $g, h \in \mathcal{G}$ en $\text{dom } g \subseteq \text{dom } h$ dan $g = h \upharpoonright \text{dom } g$. *Hint:* Inductie.
 - De vereniging $f = \bigcup \mathcal{G}$ is een functie die tot \mathcal{G} behoort.

- d. Het domein van f is gelijk aan X .
- e. Als f en g beide als gewenst zijn dan geldt $f = g$.

We kunnen F ook op een andere manier maken, vergelijk het bewijs van Stelling 1.2 op pagina 13.

- 45. Zij \mathcal{I} de familie van alle deelverzamelingen, I , van $X \times Y$ die voldoet aan: als $f \in \mathcal{F}$ en $f \subseteq I$ en $\text{dom } f = \hat{x}$ dan $\langle x, F(f) \rangle \in I$.
 - a. $X \times Y \in \mathcal{I}$
 - b. Als $\mathcal{I}' \subseteq \mathcal{I}$ dan $\bigcap \mathcal{I}' \in \mathcal{I}$.
 - c. De doorsnede $\bigcap \mathcal{I}$ is de functie die we zoeken.

Het Recursieprincipe formaliseert het idee dat een functie op een welgeordende verzameling kan worden gedefinieerd door zijn beginstukken. We gebruiken het hier om de vergelijkbaarheid van welgeordende verzamelingen aan te tonen.

1.8. STELLING. *Laat $(X, <)$ en $(Y, <)$ twee welgeordende verzamelingen zijn. Dan is X isomorf met een beginstuk van Y of Y is isomorf met een beginstuk van X .*

- 46. Zij \mathcal{F} de verzameling van alle afbeeldingen die een beginstuk van X als domein hebben en Y als co-domein. Definieer $F : \mathcal{F} \rightarrow Y \cup \{Y\}$ door $F(f) = \min(Y \setminus \text{ran } f)$ als $\text{ran } f \neq Y$ en $F(f) = Y$ als f surjectief is. Pas het Recursieprincipe toe op F om een afbeelding $f : X \rightarrow Y \cup \{Y\}$ te verkrijgen die voldoet aan $f(x) = F(f \upharpoonright \hat{x})$ voor alle x .
 - a. Als $x < y$ in X en $f(y) \neq Y$ dan $f(x) < f(y)$.
 - b. Als er een x in X is met $f(x) = Y$ dan is Y isomorf met een beginstuk van X .
 - c. Als $f(x) \neq Y$ voor alle x dan is X isomorf met een beginstuk van Y .

Een alternatieve constructie is de volgende.

- 47. Definieer $f = \{\langle x, y \rangle \in X \times Y : \hat{x} \text{ en } \hat{y} \text{ zijn isomorf}\}$.
 - a. f is een afbeelding
 - b. f^{-1} is een afbeelding
 - c. f is een isomorfisme tussen $\text{dom } f$ en $\text{ran } f$.
 - d. $\text{dom } f$ is een beginstuk van X en $\text{ran } f$ is een beginstuk van Y
 - e. $\text{dom } f = X$ of $\text{ran } f = Y$.

De volgende stelling maakt het vergelijken van ordetypen van welgeordende verzamelingen wat eenvoudiger.

- 48. Laat $(X, <)$ en $(Y, <)$ twee welgeordende verzamelingen zijn. Dan geldt: X is isomorf met een deelverzameling van Y dan en slechts dan als X isomorf is met een beginstuk van Y .

Ordinaalgetallen

Het ordetype van een welgeordende verzameling noemen we een *ordinaalgetal*. Dus ω is een ordinaalgetal, evenals elk natuurlijk getal, maar η en θ zijn dat niet. Het bestaan van meer ordinaalgetallen volgt uit de volgende opgave.

- 49. Als α en β ordinaalgetallen zijn dan zijn ook $\alpha + \beta$ en $\alpha \cdot \beta$ ordinaalgetallen.

Laat $\{(M_i, <_i) : i \in I\}$ een familie lineair geordende verzamelingen zijn en neem aan dat I zelf ook lineair geordend is door $<$. Definieer een ordening $<$ op de verzameling

$$M = \bigcup_{i \in I} M_i \times \{i\}$$

door $(m, i) < (n, j)$ als $i < j$ of $i = j$ en $m \prec_i n$. We noemen $(M, <)$ de *geordende som* van de gegeven familie.

- **50.** a. Toon aan dat $<$ een lineaire ordening is.
 b. Toon aan: als \prec en elke \prec_i welordeningen zijn dan is ook $<$ een welordering.

Laat $\alpha = \overline{M}$ en $\beta = \overline{N}$ twee ordinaalgetallen zijn. We definiëren $\alpha < \beta$ als M isomorf is met een beginstuk van N . Stelling 1.8 impliceert dat elk tweetal ordinaalgetallen vergelijkbaar is.

Kanonieke representanten

Hoewel Cantor's definitie het sterk suggereerden is het in het algemeen niet mogelijk per kardinaalgetal of per ordetype op natuurlijke wijze één vaste representant aan te wijzen. Voor ordinaalgetallen is dat wel mogelijk.

Zij (X, \prec) een welgeordende verzameling. Met \mathcal{I}_X noteren we de verzameling van *echte* beginstukken van X , de beginstukken ongelijk aan X zelf dus.

- **51.** De afbeelding $x \mapsto \hat{x}$ is een isomorfisme tussen (X, \prec) en (\mathcal{I}_X, \subset) .

Dus (\mathcal{I}_X, \subset) is een welgeordende verzameling die isomorf is met X ; wat \mathcal{I}_X op X voor heeft is dat de elementen verzamelingen zijn en dat de ordening de gewone relatie 'deelverzameling van' is. We noemen een welgeordende verzameling (X, \prec) *kanoniek* als deze gelijk is aan (\mathcal{I}_X, \subset) ; dus als $X = \mathcal{I}_X$ en als $x \prec y$ equivalent is met $x \subset y$. Kanonieke welgeordende verzamelingen hebben veel gemeen.

- **52.** Zij (X, \prec) een kanonieke welgeordende verzameling met ten minste drie elementen.
 a. $\min X = \emptyset$
 b. Direct na $\min X$ komt $\{\emptyset\}$.
 c. En meteen daarna komt $\{\emptyset, \{\emptyset\}\}$
- **53.** Zij (X, \prec) een kanonieke welgeordende verzameling.
 a. Voor elke $x \in X$ geldt $x = \hat{x}$
 b. Voor elke $x \in X$ geldt $x + 1 = x \cup \{x\}$ (tenzij $x = \max X$)
 c. Elk element van X is een deelverzameling van X en zelf ook kanoniek
 d. Voor x en y in X zijn equivalent: $x \prec y$, $x \subset y$ en $x \in y$.
 e. X is *transitief*: als $x \in X$ en $y \in x$ dan $y \in X$.
 f. X is welgeordend door \in .

Dat er genoeg kanonieke welgeordende verzamelingen bestaan volgt uit de volgende stelling.

1.9. STELLING. *Elke welgeordende verzameling is isomorf met precies één kanonieke welgeordende verzameling.*

Het 'ten hoogste één' is snel bewezen.

- **54.** Twee isomorfe kanonieke welgeordende verzamelingen zijn gelijk. *Hint:* Toon aan dat het unieke isomorfisme de identieke afbeelding is.

De constructie van de gewenste kanonieke kopie van een welgeordende verzameling gaat met behulp van het Recursieprincipe.

- **55.** Zij (X, \prec) een welgeordende verzameling.

- a. Er bestaat een afbeelding f met domein X die voldoet aan $f(x) = \{f(y) : y \prec x\}$. *Hint:* Recursie, met $F(f) = \{f(x) : x \in \text{dom } f\}$.
- b. De verzameling $(f[X], \in)$ is kanoniek en isomorf met (X, \prec) .

We hebben dus voor elk ordinaalgetal precies één kanonieke welgeordende verzameling met dat type gevonden. We gebruiken dit om ordinaalgetallen te herdefiniëren.

1.10. DEFINITIE. Een *ordinaalgetal* is een transitieve verzameling die welgeordend is door \in .

- **56.** Laat α en β ordinaalgetallen zijn en zij $\gamma = \alpha \cap \beta$.
- γ is een ordinaalgetal
 - $\gamma = \alpha$ of $\gamma = \beta$
 - $\alpha \in \beta$ of $\alpha = \beta$ of $\beta \in \alpha$.
- **57.** a. Als α een ordinaalgetal is dan is ook $\alpha \cup \{\alpha\}$ een ordinaalgetal.
 b. Als α een ordinaalgetal is dan is $\alpha \cup \{\alpha\}$ de directe opvolger van α , dat wil zeggen: er bestaat geen ordinaalgetal γ met $\alpha < \gamma < \alpha \cup \{\alpha\}$.
 c. Als X een verzameling ordinaalgetallen is dan is ook $\bigcup X$ een ordinaalgetal.

We zeggen dat α een *opvolger* is als er een β bestaat zó dat $\alpha = \beta \cup \{\beta\}$; anders noemen we α een *limietgetal*.

- **58.** Zij X een niet-lege verzameling ordinaalgetallen.
- $\min X = \bigcap X$
 - $\sup X = \bigcup X$
- **59.** Zij $\alpha > 0$ een ordinaalgetal; toon aan:
- $\alpha = \sup(\alpha + 1)$
 - α is een limiet dan en slechts dan als $\alpha = \sup \alpha$.

We kunnen de eerste paar ordinaalgetallen eenvoudig opschrijven.

- \emptyset
- $\{\emptyset\}$,
- $\{\emptyset, \{\emptyset\}\}$

Zo voortgaand maken we telkens nieuwe ‘eindige’ ordinaalgetallen: uit α maken we telkens $\alpha \cup \{\alpha\}$. We schrijven $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, ... De definitie van de optelling laat zien dat $\alpha + 1 = \alpha \cup \{\alpha\}$, we houden die notatie in het vervolg aan.

Het ordinaalgetal ω — de kanonieke representant van \mathbb{N} — bestaat uit deze ‘eindige’ ordinaalgetallen’.

- **60.** a. Het ordinaalgetal ω voldoet aan $\emptyset \in \omega$ en aan “als $x \in \omega$ dan $x \cup \{x\} \in \omega$ ”.
 b. Als X een verzameling is die aan bovenstaande eigenschappen voldoet dan $\omega \subseteq X$.

Een overaftelbaar ordinaalgetal

De ordinaalgetallen die we tot nu toe expliciet hebben aangegeven zijn allemaal aftelbaar. Het eerste *overaftelbare* ordinaalgetal krijgen we door alle aftelbare ordinaalgetallen te verenigen, zie Opgave 58. Dit ordinaalgetal noteren we met ω_1 .

We kunnen ω_1 ook zien als ordetype van een expliciete welgeordende verzameling.

- **61.** Zij $W = \{A \in \mathcal{P}(\mathbb{Q}) : A \text{ is welgeordend door de gewone ordening van } \mathbb{Q}\}$ en definieer een relatie \sim op W door $A \sim B$ als $\overline{A} = \overline{B}$.

- a. Toon aan dat \sim een equivalentierelatie is.
 Orden $\Omega = W/\sim$ door $[A] \prec [B]$ als $\overline{A} < \overline{B}$.
 b. Toon aan dat \prec goed-gedefinieerd is en dat $(\Omega, \prec) = \omega_1$.

► **62.** Toon aan: als A een aftelbare deelverzameling van ω_1 is dan is er een $\alpha < \omega_1$ met $A \subseteq \alpha$.

We noemen een functie $f : \omega_1 \rightarrow \omega_1$ *continu* als $f(\sup A) = \sup f[A]$ voor elke deelverzameling van ω_1 met $\sup A < \omega_1$.

► **63.** Bewijs: als $f : \omega_1 \rightarrow \omega_1$ een stijgende, continue en onbegrensde functie is dan bestaat voor elke α een $\beta > \alpha$ met $f(\beta) = \beta$. *Hint:* Maak een stijgende rij $(\alpha_n)_n$ zó dat $f(\alpha_n) < \alpha_{n+1}$ voor alle n .

De volgende stelling staat bekend als het ‘Pressing-Down Lemma’.

1.11. STELLING. *Zij $f : \omega_1 \rightarrow \omega_1$ een functie zó dat $f(\alpha) < \alpha$ als $\alpha > 0$. Dan is er een β zó dat $\{\alpha : f(\alpha) = \beta\}$ overaftelbaar is.*

- **64.** Bewijs deze stelling. Neem aan dat f zó is dat $\{\alpha : f(\alpha) = \gamma\}$ altijd aftelbaar is. Definieer $g : \omega_1 \rightarrow \omega_1$ door $g(\alpha) = \sup\{\beta + 1 : f(\beta) \leq \alpha\}$.
 a. Voor elke α geldt $\alpha < g(\alpha)$.
 Definieer $\alpha_0 = 0$ en, recursief, $\alpha_{n+1} = g(\alpha_n)$.
 b. Toon aan: voor $\beta = \sup_n \alpha_n$ zou moeten gelden $f(\beta) \geq \beta$.

De geordende verzameling ω_1 heeft een natuurlijke topologie: de orde-topologie. Deze heeft de familie van alle open intervallen als basis.

- **65.** a. Als $\alpha > 0$ dan is $\{(\beta, \alpha] : \beta < \alpha\}$ een lokale basis in α .
 b. Een punt α is geïsoleerd punt dan en slechts dan als α een opvolger is of 0.
 ► **66.** Bewijs: als $f : \omega_1 \rightarrow \mathbb{R}$ continu is dan bestaat een α zó dat f constant is op het interval $[\alpha, \omega_1)$. *Hint:* Zij $\varepsilon > 0$, kies voor elke $\alpha > 0$ een $\beta_\alpha < \alpha$ zó dat $|f(\gamma) - f(\alpha)| < \varepsilon$ voor $\gamma \in (\beta_\alpha, \alpha]$. Pas Stelling 1.11 toe om een β en een overaftelbare A te vinden. Toon aan dat de diameter van $f[(\beta, \omega_1)]$ ten hoogste 2ε is. Bepaal zo β_n bij 2^{-n} en bekijk $\alpha = \sup_n \beta_n$.

Ordinaalaritmetiek

De rekenkunde van ordinaalgetallen is verrassend rijk en heeft, wellicht onverwachte, toepassingen in de getaltheorie.

Optellen

We weten al dat de optelling associatief is maar niet commutatief, hieruit volgt een asymmetrische relatie met de ordening.

- **67.** Laat α en β ordinaalgetallen zijn met $\beta > 0$.
 a. Toon aan: $\alpha < \alpha + \beta$.
 b. Toon aan: $\beta \leq \alpha + \beta$.

De schrapwetten zijn ook eenzijdig.

- **68.** a. Laat α , β en γ ordinaalgetallen zijn. Toon aan: als $\alpha + \beta = \alpha + \gamma$ dan $\beta = \gamma$.
 b. Geef voorbeelden waaruit blijkt dat de andere schrapwet niet geldt.

Er is ook sprake van continuïteit: als $\langle \alpha_n \rangle_n$ een stijgende rij ordinaalgetallen is dan definiëren we $\lim_n \alpha_n = \bigcup_n \alpha_n$.

- **69.** a. Als α een ordinaalgetal is en $\langle \beta_n \rangle_n$ een rij ordinaalgetallen dan geldt $\lim_n(\alpha + \beta_n) = \alpha + \lim_n \beta_n$.
 b. Bepaal $\lim_n(n + \omega)$.

Vermenigvuldigen

Voor de vermenigvuldiging gelden analoge formules.

- **70.** Laat α en β ordinaalgetallen ongelijk aan 0 zijn.
 a. Toon aan: als $\beta > 1$ dan $\alpha < \alpha \cdot \beta$.
 b. Toon aan: $\beta \leq \alpha \cdot \beta$.

Er is ook een schrapwet.

- **71.** a. Laat α , β en γ ordinaalgetallen zijn met $\alpha > 0$. Toon aan: als $\alpha \cdot \beta = \alpha \cdot \gamma$ dan $\beta = \gamma$.
 b. Geef voorbeelden waaruit blijkt dat de andere schrapwet niet geldt.

Er is ook weer sprake van continuïteit.

- **72.** a. Als α een ordinaalgetal is en $\langle \beta_n \rangle_n$ een rij ordinaalgetallen dan geldt $\lim_n(\alpha \cdot \beta_n) = \alpha \cdot \lim_n \beta_n$.
 b. Bepaal $\lim_n(n \cdot \omega)$.

We kunnen ook delen met rest.

- **73.** Toon aan: bij elk tweetal ordinaalgetallen α en β bestaan unieke γ en ρ zó dat $\alpha = \beta \cdot \gamma + \rho$ en $\rho < \beta$. *Hint:* Zij $A = \{\eta : \text{er is een } \delta \text{ zó dat } \alpha = \beta \cdot \delta + \eta\}$; toon aan dat $A \neq \emptyset$ en neem $\rho = \min A$.

Machtsverheffen

Eindige machten van ordinaalgetallen hebben we al gedefinieerd. Voor willekeurige exponenten gebruiken we een recursieve definitie.

Zij α een ordinaalgetal, we definiëren α^β voor alle β door

- $\alpha^0 = 1$,
- $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$,
- als β een limietgetal is dan $\alpha^\beta = \sup_{\gamma < \beta} \alpha^\gamma$.

Bijvoorbeeld: $2^\omega = \omega$.

- **74.** Bewijs: als α en β aftelbaar zijn dan is ook α^β aftelbaar.

We kunnen α^β als een ordertype zien.

- **75.** Laat α en β ordinaalgetallen zijn en definieer $F(\alpha, \beta) = \{f \in {}^\beta \alpha : \{\xi : f(\xi) \neq 0\} \text{ is eindig}\}$. Definieer een ordening \prec op $F(\alpha, \beta)$ door $f \prec g$ als $f(\xi) < g(\xi)$, waarbij $\xi = \max\{\zeta : f(\zeta) \neq g(\zeta)\}$. Dan is \prec een welordering en α^β is het ordinaalgetal van $(F(\alpha, \beta), \prec)$. We nemen α vast; we bewijzen de bewering met inductie naar β .

- a. $F(\alpha, 0)$ heeft één element.
- b. Als $\gamma < \beta$ dan is $\{f \in F(\alpha, \beta) : (\xi \geq \gamma \rightarrow f(\xi) = 0)\}$ een beginstuk van $F(\alpha, \beta)$ dat isomorf is met $F(\alpha, \gamma)$.
- c. $F(\alpha, \beta + 1)$ is isomorf met $F(\alpha, \beta) \times \alpha$.
- d. Als β een limiet is dan kunnen we, via onderdeel b, $F(\alpha, \beta)$ zien als de vereniging van de $F(\alpha, \gamma)$ met $\gamma < \beta$.
- e. Met inductie volgt nu dat voor elke β het ordinaalgetal van $F(\alpha, \beta)$ gelijk is aan α^β .

De normaalvorm

We schrijven, normaal gesproken, natuurlijke getallen in basis 10; Cantor ontwikkelde een schrijfwijze voor (aftelbare) ordinaalgetallen in basis ω .

- **76.** a. Als $\alpha > 1$ dan geldt voor elke β dat $\beta \leq \alpha^\beta$.
 b. Als $\alpha < \omega^\beta$ dan geldt $\alpha + \omega^\beta = \omega^\beta$.

Voor een ordinaalgetal α definiëren we $\log_\omega^+ \alpha = \min\{\xi : \omega^\xi > \alpha\}$.

- **77.** Zij α een ordinaalgetal ongelijk aan 0 en $\nu = \log_\omega^+ \alpha$.
 a. Het ordinaalgetal ν is een opvolger.
 Schrijf $\nu = \mu + 1$.
 b. Er bestaan een $n \in \omega$ en een ordinaalgetal $\beta < \omega^\mu$ zó dat $\alpha = \omega^\mu \cdot n + \beta$.
 c. Als ξ , m en γ zo zijn dat $\alpha = \omega^\xi \cdot m + \gamma$ en $\gamma < \omega^\xi$ dan geldt $\xi = \mu$, $m = n$ en $\gamma = \beta$.

Neem nu een ordinaalgetal α en ga te werk als in het algoritme van Euclides. Schrijf $\beta_0 = \alpha$ en bepaal α_0 , n_0 en β_1 zó dat $\beta_0 = \omega^{\alpha_0} \cdot n_0 + \beta_1$ en $\beta_1 < \beta_0$. Als $\beta_1 = 0$ stop, anders gaan we verder: bepaal α_1 , n_1 en β_2 zó dat $\beta_1 = \omega^{\alpha_1} \cdot n_1 + \beta_2$ en $\beta_2 < \beta_1$. Herhaal dit tot $\beta_{i+1} = 0$.

- **78.** a. Er bestaat een i zó dat $\beta_{i+1} = 0$.
 b. $\alpha = \omega^{\alpha_0} \cdot n_0 + \dots + \omega^{\alpha_i} \cdot n_i$.

ε -getallen

Cantor noemde de exponent α_0 de graad van α en merkte op dat altijd $\alpha_0 \leq \alpha$. Het lijkt voor de hand te liggen dat $\alpha_0 < \alpha$ maar Cantor vroeg zich af of $\alpha_0 = \alpha$ toch niet mogelijk was. Het antwoord is dat er heel veel van dergelijke α 's zijn.

- **79.** Zij γ een ordinaalgetal en definieer een rij $\langle \gamma_n \rangle_n$ door $\gamma_0 = \gamma$ en $\gamma_{i+1} = \omega^{\gamma_i}$.
 a. De limiet $\alpha = \lim_i \gamma_i$ voldoet aan $\alpha = \omega^\alpha$.
 b. Als γ aftelbaar is dan is $\lim_i \gamma_i$ ook aftelbaar.

Een oplossing van de vergelijking $\xi = \omega^\xi$ heet een ε -getal.

- **80.** Een ordinaalgetal $\alpha > \omega$ is een ε -getal dan en slechts dan als $\beta^\gamma < \alpha$ voor elk tweetal ordinaalgetallen $\beta, \gamma < \alpha$.

Goodstein-rijen

Er is een fraaie toepassing van het bestaan van ε -getallen in de getaltheorie. Om deze te formuleren eerst wat notatie. Neem een vast natuurlijk getal n . Elk getal is op de bekende wijze te schrijven in basis n :

$$a = n^i k_i + n^{i-1} k_{i-1} + \dots + n k_1 + k_0$$

met $0 \leq k_j < n$ voor elke j . Bijvoorbeeld $25 = 2^4 + 2^3 + 1$ of $25 = 3^2 \cdot 2 + 3 \cdot 2 + 1$.

Deze schrijfwijze passen we aan tot er geen getal groter dan de basis meer voorkomt; dat betekent dat we de exponenten ook in basis n schrijven en de exponenten in die exponenten ook, enzovoort. In ons voorbeeld $25 = 2^{2^2} + 2^{2+1} + 1$, de schrijfwijze in basis 3 is al in orde. We zeggen dat 25 *strikt* in basis 2 geschreven is.

Bij elk getal m maken we een rij $\langle m_n \rangle_n$ als volgt: $m_2 = m$, schrijf m_2 strikt in basis 2, vervang elke 2 door een 3 en trek van het resultaat 1 af, dit is m_3 . Dus $25_2 = 25$

en $25_3 = 3^{3^3} + 3^{3+1} + 1 - 1 = 7625597485068$. In de volgende stap schrijven we m_3 strikt in basis 3, vervangen elke 3 door een 4 en trekken 1 van het resultaat of om m_4 te maken. Voor 25 krijgen we $25_4 = 4^{4^4} + 4^{4+1} - 1 \approx 1.340780793 \times 10^{154}$. We gaan zo verder: schrijf m_4 strikt in basis 4, vervang elke 4 door een 5, trek 1 af, het resultaat is m_5 . Dus eerst $25_4 = 4^{4^4} + 4^4 \cdot 3 + 4^3 \cdot 3 + 4^2 \cdot 3 + 4 \cdot 3 + 3$ en dan $25_5 = 5^{5^5} + 5^5 \cdot 3 + 5^3 \cdot 3 + 5^2 \cdot 3 + 5 \cdot 3 + 3 - 1$.

Dus, schrijf m_i strikt in basis i , vervang elke i door $i + 1$ en trek 1 af, het resultaat is m_{i+1} .

De stelling van Goodstein, uit [1944], zegt dat dit proces altijd stopt.

1.12. STELLING (Goodstein). *Voor elke m bestaat een i zó dat $m_i = 0$.*

Het bewijs van de stelling is verrassend eenvoudig, gegeven de normaalvorm van Cantor. We vervangen elk getal m_i door een ordinaalgetal (kleiner dan het eerste ε -getal).

1. Bij m_2 maken we α_2 door elke 2 door ω te vervangen; bij 25_2 hoort dus $\omega^{\omega^\omega} + \omega^{\omega+1} + 1$.
2. Bij m_3 maken we α_3 door elke 3 door ω te vervangen; bij 25_3 hoort dus $\omega^{\omega^\omega} + \omega^{\omega+1}$.
3. Bij m_4 maken we α_4 door elke 4 door ω te vervangen; bij 25_4 hoort dus

$$\omega^{\omega^\omega} + \omega^\omega \cdot 3 + \omega^3 \cdot 3 + \omega^2 \cdot 3 + \omega \cdot 3 + 3$$

i Bij m_i maken we α_i door i te vervangen door ω .

► 81. Bewijs dat de rij $\langle \alpha_i \rangle_i$ strikt dalend is.

1.13. *Opmerking.* De stelling van Goodstein is, met wat moeite, in de taal van de gewone rekenkunde van \mathbb{N} te formuleren. Hij is echter niet met gewone rekenkundige methoden te bewijzen; dit is bewezen door Kirby en Paris in [1982].

Paradoxen

Al vroeg in de ontwikkeling van de verzamelingenleer ontstonden er problemen door de al te ruime definitie (of opvatting) van het begrip verzameling.

Paradoxen van Burali-Forti en Cantor

De eerste gepubliceerde paradox is die van ‘de verzameling W van alle ordinaalgetallen’. Deze is zelf welgeordend en heeft dus een ordetype dat zelf een ordinaalgetal is. Maar dat ordinaalgetal behoort tot zichzelf en is dan kleiner dan zichzelf.

Cantor had zelf ook iets paradoxaals gevonden: de verzameling van alle kardinaalgetallen; deze heeft een kardinaalgetal, zeg \aleph . Dan is \aleph groter dan alle kardinaalgetallen en tegelijk kleiner dan het kardinaalgetal 2^{\aleph} .

Paradox van Russell

De paradoxen van Burali-Forti en Cantor hingen samen met ordinaal- en kardinaalgetallen en hadden nogal wat machinerie nodig om ze te kunnen formuleren. De paradox van Russell was een stuk eenvoudiger (en gebaseerd op het diagonaalargument): bekijk de verzameling $R = \{x : x \notin x\}$.

Met R is iets gekk aan de hand: $R \in R$ dan en slechts dan als $R \notin R$. Deze uitspraak heeft waarheidswaarde nul en komt regelrecht voort uit Cantor's definitie van verzameling.

In het volgende hoofdstuk zullen we zien dat deze paradoxen vermeden kunnen worden, zonder de belangrijke resultaten van dit hoofdstuk op te geven.

Hoofdstuk 2

Axiomatische verzamelingenleer

Zoals we aan het eind van Hoofdstuk 1 gezien hebben kunnen we niet al te onbekommerd met Cantor's 'definitie' (of beter: opvatting) van het begrip verzameling omgaan: niet elke "samenvoeging van dingen tot een geheel" mag het predikaat 'verzameling' dragen. Aan de andere kant, het gebruik van verzamelingen is tot in alle krichten van de wiskunde doorgedrongen. Vrijwel elke definitie van een wiskundig object stipuleert dat het een verzameling is met daarop gedefinieerd een bewerking, relatie, een familie deelverzamelingen ... die aan zekere regels voldoet.

Het was dan ook in het begin van de twintigste eeuw zaak de verzamelingenleer zó te funderen dat de paradoxen niet meer voor konden komen en zó dat alle wiskunde die met gebruik van verzamelingenleer was opgezet behouden zou blijven. In [1908b] gaf Zermelo een axiomatisering van de Verzamelingenleer. De axioma's van Zermelo, met een toevoeging van Fraenkel uit [1922], vormen het meest-gebruikte stelsel. Er zijn andere axiomastelsels in omloop maar die voegen, op het niveau van de verzamelingen, niets wezenlijks aan het stelsel van Zermelo en Fraenkel toe.

De taal van de verzamelingenleer

Voor we de axioma's geven beschrijven we eerst de *taal* waarin de verzamelingenleer geschreven wordt.

Formules

De Verzamelingenleer is *een eerste-orde theorie met gelijkheid*. Wat dat precies betekent wordt in Appendix B uitgelegd. Een wat informelere beschrijving is als volgt.

We werken met een zeer beperkte hoeveelheid symbolen:

- haakjes: (en)
- variabelen: v_1, v_2, v_3, \dots
- logische connectieven: \neg en \wedge
- een kwantor: \exists
- een symbool voor gelijkheid: $=$
- een symbool voor 'element van': \in

Met behulp van deze symbolen kunnen we formules opbouwen

- voor elk tweetal variabelen v_i en v_j zijn $v_i \in v_j$ en $v_i = v_j$ formules,
- als ϕ een formule is dan is $\neg(\phi)$ ook een formule,
- als ϕ en ψ formules zijn dan is ook $(\phi) \wedge (\psi)$ een formule,
- als ϕ een formule en v_i een variabele dan is ook $(\exists v_i)(\phi)$ een formule.

Alleen rijen symbolen die op bovenstaande wijze opgebouwd kunnen worden zijn (welgevormde) formules.

Dit klinkt misschien wat plechtig maar met deze precieze definitie van wat een formule is kunnen we veel van Cantor's definitie redden: zolang we ons tot deze formules beperken komen we een heel eind.

Afkortingen

Als we alles met alléén formules van de voorgegeven vorm zouden beschrijven werd de verzamelingenleer eerder vermoeiend dan interessant. We voeren daarom meteen wat afkortingen in.

- $v_i \neq v_j$ is een afkorting van $\neg(v_i = v_j)$
- $v_i \notin v_j$ is een afkorting van $\neg(v_i \in v_j)$
- $(\phi) \vee (\psi)$ is een afkorting van $\neg((\neg(\phi)) \wedge (\neg(\psi)))$
- $(\phi) \rightarrow (\psi)$ is een afkorting van $(\neg(\phi)) \vee (\psi)$
- $(\phi) \leftrightarrow (\psi)$ is een afkorting van $((\phi) \rightarrow (\psi)) \wedge ((\psi) \rightarrow (\phi))$
- $(\forall v_i)(\phi)$ is een afkorting van $\neg((\exists v_i)(\neg(\phi)))$

Om de leesbaarheid te bevorderen en als de context het toelaat laten we zo veel mogelijk haakjes weg; weinig mensen zullen, bijvoorbeeld, $v_1 \in v_2 \wedge v_2 \in v_3$ anders interpreteren dan als $(v_1 \in v_2) \wedge (v_2 \in v_3)$.

Verder sluiten we aan bij de dagelijkse praktijk en gebruiken we meer letters dan alleen de v_i als variabelen, niet alleen Latijnse maar ook Griekse, Hebreeuwse, Cyrillische ...; de eerste-orde logica laat dit toe: er is logisch gesproken geen verschil tussen

$$(\forall v_1)(\forall v_2)(\exists v_3)((v_1 \in v_3) \wedge (v_2 \in v_3))$$

en

$$(\forall x)(\forall y)(\exists z)((x \in z) \wedge (y \in z)).$$

We gebruiken daarom, als het even kan, gewoon letters zonder indices.

Vrije en gebonden variabelen

Intuïtief gesproken is (een voorkomen van) een variabele *vrij* als je er iets voor kunt invullen en *gebonden* als dat niet kan; of ook wel: een gebonden voorkomende variabele kun je door een andere vervangen, een vrij voorkomende niet. In

$$\int_a^b \sin x \, dx + \int_0^x \cos t \, dt$$

kunnen we voor de a en b getallen invullen, deze variabelen zijn vrij. Voor de x in de eerste integraal kunnen we geen getal invullen maar voor de x in de tweede integraal wel:

$$\int_1^2 \sin x \, dx + \int_0^3 \cos t \, dt$$

is een zinvolle uitdrukking. De t in de tweede integraal komt ook gebonden voor. De dx en dt spelen in de integralen de rol die kwantoren in verzamelingtheoretische formules spelen. De eerste integraal verandert niet als we alle x -en door u vervangen.

Bekijk de volgende formule

$$((\exists v_0)(v_0 \in v_1)) \wedge ((\exists v_1)(v_2 \in v_1)). \quad (1)$$

Het bereik van de kwantor $(\exists v_0)$ is de deel formule $(\exists v_0)(v_0 \in v_1)$ en dat van $(\exists v_1)$ is $(\exists v_1)(v_2 \in v_1)$. In de eerste deel formule komt v_1 vrij voor en in de tweede is v_1 gebonden. Een formule ‘zegt’ iets over zijn vrij voorkomende variabelen; in ons geval “ v_1 is niet leeg en v_2 behoort tot een verzameling”. Bij het vervangen van gebonden en vrije variabelen moeten we oppassen dat die betekenis niet verandert. Het is bijvoorbeeld niet verstandig in de eerste deel formule over te gaan op de gebonden variabele v_1 want $(\exists v_1)(v_1 \in v_1)$ zegt dan “iets is een element van zichzelf”. In het algemeen zullen we dit soort formules en vervangingen vermijden.

Begrensde kwantoren

Vaak zeggen we niet “er is een $x \dots$ ” maar “er is een x in $A \dots$ ” en evenzo met “voor alle”. Voor dit soort gevallen voeren we twee afkortingen in:

$$(\exists x \in A)(\phi) \text{ betekent } (\exists x)((x \in A) \wedge (\phi))$$

en

$$(\forall x \in A)(\phi) \text{ betekent } (\forall x)((x \in A) \rightarrow (\phi)).$$

Dergelijke kwantoren heten *begrensde kwantoren*.

De Axioma's van Zermelo en Fraenkel

Dit axiomastelsel bestaat uit zeven individuele axioma's en twee (oneindige) lijsten van axioma's, of beter gezegd *axiomaschema's*.

AXIOMA 0. ER BESTAAN VERZAMELINGEN. Er bestaat een verzameling:

$$(\exists x)(x = x)$$

AXIOMA 1. EXTENSIONALITEIT. Als twee verzamelingen precies dezelfde elementen hebben dan zijn deze gelijk:

$$(\forall x)(\forall y)((\forall z)(z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

AXIOMA 2. REGULARITEIT. Elke verzameling heeft een \in -minimaal element:

$$(\forall x)((\exists y)(y \in x) \rightarrow (\exists y)(y \in x \wedge \neg(\exists z)(z \in x \wedge z \in y)))$$

AXIOMA 3. HET AFSCHIEDINGSSHEMA. Als ϕ een (welgevormde) formule is met zijn vrije variabelen in de rij x, z, w_1, \dots, w_n (allen ongelijk aan y) dan bestaat bij elke verzameling x een verzameling die bestaat uit precies die elementen van x die aan ϕ voldoen:

$$(\forall x)(\forall w_1) \dots (\forall w_n)(\exists y)(\forall z)(z \in y \leftrightarrow (z \in x \wedge \phi))$$

AXIOMA 4. PAARVORMING. Bij elk tweetal verzamelingen bestaat een verzameling die die twee als elementen heeft:

$$(\forall x)(\forall y)(\exists z)(x \in z \wedge y \in z)$$

AXIOMA 5. VERENIGING. Bij elke verzameling x bestaat een verzameling y waarvan elk element van x een deelverzameling is:

$$(\forall x)(\exists y)(\forall z)(\forall u)((u \in z \wedge z \in x) \rightarrow u \in y)$$

AXIOMA 6. VERVANGINGSSCHEMA. Voor elke formule ϕ met zijn vrije variabelen in de rij x, y, A, w_1, \dots, w_n (allen ongelijk aan B) is de volgende formule een axioma:

$$(\forall A)(\forall w_1) \cdots (\forall w_n)((\forall x \in A)(\exists! y)(\phi) \rightarrow (\exists B)(\forall x \in A)(\exists y \in B)(\phi))$$

AXIOMA 7. ONEINDIGHEID. Er is een niet-lege verzameling die met elk element ook zijn opvolger bevat.

$$(\exists x)(\emptyset \in x \wedge (\forall y \in x)(y \cup \{y\} \in x))$$

AXIOMA 8. MACHTSVERZAMELING. Bij elke verzameling bestaat een verzameling die de deelverzamelingen van de gegeven verzameling als elementen heeft:

$$(\forall x)(\exists y)(\forall z)(z \subseteq x \rightarrow z \in y)$$

De axioma's hierboven werden door Zermelo opgesteld, met uitzondering van het Vervangingsschema, dat werd later door Fraenkel toegevoegd. Tezamen vormen ze de theorie die met ZF wordt aangeduid; voor de oorspronkelijke axioma's van Zermelo gebruikt men wel eens Z.

Het Keuzeaxioma

Het volgende axioma, het keuzeaxioma, heeft, wegens zijn niet-constructieve karakter een aparte plaats.

AXIOMA 9. KEUZEAXIOMA. Elke familie niet-lege verzamelingen heeft een keuzefunctie

$$(\forall x)(\emptyset \notin x \rightarrow (\exists f)((f : x \rightarrow \bigcup x) \wedge (\forall y \in x)(f(y) \in y)))$$

Als aan ZF het keuzeaxioma wordt toegevoegd krijgen we de theorie ZFC.

Opbouw van de verzamelingenleer

We gaan nu aan de hand van de axioma's de verzamelingenleer (opnieuw) opbouwen. We laten alle axioma's nogmaals de revue passeren en geven aan hoe ze gebruikt worden om allerlei welbekende noties in termen van verzamelingen alleen te definiëren.

NB de opgaven kunnen (en moeten) gemaakt worden met behulp van de axioma's die tot dan toe behandeld zijn.

Drie basale axioma's

Omdat we met lege handen beginnen is het volgende axioma echt nodig.

AXIOMA 0. ER BESTAAN VERZAMELINGEN. Er bestaat een verzameling:

$$(\exists x)(x = x)$$

Het eerste echte axioma geeft het verband tussen \in en $=$.

AXIOMA 1. EXTENSIONALITEIT. Als twee verzamelingen precies dezelfde elementen hebben dan zijn deze gelijk:

$$(\forall x)(\forall y)((\forall z)(z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

Dit axioma formaliseert de gebruikelijke gang van zaken bij het bewijzen van gelijkheid van twee verzamelingen A en B : we tonen aan dat uit $x \in A$ altijd $x \in B$ volgt en omgekeerd.

We breiden onze taal meteen uit met een extra symbool: $x \subseteq y$ is een afkorting van

$$(\forall v_1)((v_1 \in x) \rightarrow (v_1 \in y))$$

Overigens geldt het omgekeerde van AXIOMA 1 ook:

$$(\forall x)(\forall y)(x = y \rightarrow (\forall z)(z \in x \leftrightarrow z \in y))$$

het volgt namelijk uit de (logische) axioma's voor gelijkheid.

- 1. Bewijs: $x = y$ dan en slechts dan als $x \subseteq y$ en $y \subseteq x$.

Het volgende axioma, in feite een hele lijst van axioma's — een *axiomaschema*, stelt ons in staat verzamelingen door middel van 'eigenschappen van elementen' te definiëren.

AXIOMA 3. HET AFSCHIEDINGSSCHEMA. Als ϕ een (welgevormde) formule is met zijn vrije variabelen in de rij x, z, w_1, \dots, w_n (allen ongelijk aan y) dan bestaat bij elke verzameling x een verzameling die bestaat uit precies die elementen van x die aan ϕ voldoen:

$$(\forall x)(\forall w_1) \cdots (\forall w_n)(\exists y)(\forall z)(z \in y \leftrightarrow (z \in x \wedge \phi))$$

In de optiek van Cantor was elke entiteit van de vorm $\{z : \phi\}$ een verzameling; de paradox van Russell liet zien, door middel van de formule $z \notin z$, dat dat een stap te ver is. Het Afscheidingsaxioma postuleert dat we wel een verzameling krijgen als we uit een voorgegeven verzameling x de elementen z met eigenschap ϕ afscheiden.

De rol van de (mogelijk) extra vrije variabelen w_1, \dots, w_n is die van parameter: voor elke keuze van w_1, \dots, w_n vormen we een deelverzameling van x . Dat y zelf niet vrij in ϕ mag voorkomen is om te voorkomen dat y in termen van zichzelf wordt gedefinieerd.

- 2. De y in het Afscheidingsaxioma is, bij gegeven x, w_1, \dots, w_n , uniek: als ook u voldoet geldt $u = y$.

De verzameling y uit het Afscheidingsaxioma noteren we als $\{z : (z \in x) \wedge \phi(z)\}$ of als $\{z \in x : \phi(z)\}$.

- 3. a. Toon aan dat er een verzameling bestaat zonder elementen: $(\exists x)(\forall y)(y \notin x)$. *Hint*: Pas het bestaansaxioma toe en dan afscheiding met ' $y \neq y$ ' (dit werkt omdat $(\forall v_1)(v_1 = v_1)$ een *logisch* axioma is).
b. Toon aan dat er precies één verzameling zonder elementen is.

Dankzij deze opgave kunnen we een nieuwe constante invoeren, namelijk \emptyset ; deze constante voldoet per definitie aan $(\forall x)(x \notin \emptyset)$.

- 4. Bewijs: er is geen universele verzameling:

$$\neg(\exists z)(\forall x)(x \in z)$$

Hint: Denk aan $y \notin y$.

Iets minder flauw is het bestaan van doorsnede en verschil.

- 5. a. Toon aan: $(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \leftrightarrow (u \in x \wedge u \in y))$
b. Toon aan: $(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \leftrightarrow (u \in x \wedge u \notin y))$

c. Toon aan: $(\forall x)(x \neq \emptyset \rightarrow (\exists y)(\forall u)(u \in y \leftrightarrow (\forall z)(z \in x \rightarrow u \in z)))$

Het extensionaliteitsaxioma impliceert dat de verzamelingen uit de voorgaande opgave uniek zijn; we noteren ze met, respectievelijk, $x \cap y$, $x \setminus y$ en $\bigcap x$.

De bovenstaande drie axioma's geven nog niet veel verzamelingen. In het 'universum' waarin alleen de lege verzameling bestaat gelden deze axioma's en ook $(\forall y)(y = \emptyset)$.

Nieuwe verzamelingen uit oude

De rest van de axioma's beschrijft hoe we uit oude verzamelingen nieuwe kunnen maken; de lijst lijkt kort maar is sterk genoeg om de niet-paradoxe resultaten van Cantor en zijn navolgers bewijsbaar te maken.

AXIOMA 4. PAARVORMING. Bij elk tweetal verzamelingen bestaat een verzameling die die twee als elementen heeft:

$$(\forall x)(\forall y)(\exists z)(x \in z \wedge y \in z)$$

- 6. Bewijs: bij elk tweetal verzamelingen bestaat precies één verzameling die precies de twee gegeven verzamelingen als element heeft. *Hint*: ten minste één: Paarvorming plus Afscheiding; ten hoogste één: Extensionaliteit.

Op grond van deze opgave voeren we de afkorting $\{x, y\}$ in voor de verzameling die uit precies de verzamelingen x en y bestaat. Verder is $\{x\} = \{x, x\}$, dat hier niets raars gebeurt volgt uit de volgende opgave.

- 7. Bewijs: bij elke verzameling bestaat precies één verzameling die precies de gegeven verzameling als element heeft. *Hint*: De woordelijke versie van Paarvorming is misleidend ('tweetal'); uit de formele versie is op zuiver logische gronden de volgende formule af te leiden:

$$(\forall x)(\forall x)(\exists z)((x \in z) \wedge (x \in z))$$

en deze is logisch equivalent met

$$(\forall x)(\exists z)(x \in z)$$

Pas vervolgens weer Afscheiding toe.

De verzameling $\{x, y\}$ heet wel een *ongeordend paar* omdat $\{x, y\} = \{y, x\}$: de volgorde van de elementen is niet belangrijk. Voor het *geordende paar* $\langle x, y \rangle$ hanteren we de volgende definitie, bedacht door Kuratowski:

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}$$

Iedereen moet de volgende opgave één keer gemaakt hebben:

- 8. Bewijs dat de bovenstaande definitie aan de eis die we aan 'geordend paar' stellen voldoet:

$$\langle a, b \rangle = \langle c, d \rangle \text{ dan en slechts dan als } a = c \text{ en } b = d$$

Met recursie zouden we geordende drietallen, viertallen, ... kunnen definiëren door

$$\langle a, b, c \rangle = \langle \langle a, b \rangle, c \rangle \text{ en } \langle a, b, c, d \rangle = \langle \langle a, b, c \rangle, d \rangle$$

maar we doen dit niet omdat we de notatie $\langle x_1, x_2, \dots, x_n \rangle$ voor rijtjes ter lengte n willen reserveren, zie pagina 37.

- 9. a. Geef een formule die 'z is een geordend paar' uitdrukt.
b. Geef een formule die uitdrukt: "z is een geordend paar en x is de eerste coördinaat van z".

c. Geef een formule die uitdrukt: “ z is een geordend paar en y is de tweede coördinaat van z ”.

► 10. Doe de vorige opgave nog een keer maar gebruik alleen begrensde kwantoren.

Om, onder andere, verzamelingen met meer dan twee elementen te kunnen maken hebben we het volgende axioma.

AXIOMA 5. VERENIGING. Bij elke verzameling x bestaat een verzameling y waarvan elk element van x een deelverzameling is:

$$(\forall x)(\exists y)(\forall z)((z \in x) \rightarrow (z \subseteq y))$$

Hiermee kunnen we de afkorting $\bigcup x$ invoeren.

► 11. Bewijs: bij elke verzameling bestaat precies één verzameling die precies de elementen van de elementen van de gegeven verzameling als element heeft.

In het bijzonder definiëren we $x \cup y = \bigcup\{x, y\}$.

Het volgende axioma is in feite weer een lijst, voor elke formule één. Dit axioma is wat het bewijs van Stelling 1.9 mogelijk maakt. Om de formulering kort te kunnen houden voeren we een afkorting in voor “er is precies één”: de uitdrukking

$$(\exists!x)(\phi(x))$$

staat voor

$$((\exists x)(\phi(x))) \wedge ((\forall x)(\forall y)((\phi(x) \wedge \phi(y)) \rightarrow (x = y)))$$

AXIOMA 6. VERVANGINGSSCHEMA. Voor elke formule ϕ met zijn vrije variabelen in de rij x, y, A, w_1, \dots, w_n (allen ongelijk aan B) is de volgende formule een axioma

$$(\forall A)(\forall w_1) \dots (\forall w_n)((\forall x \in A)(\exists!y)(\phi) \rightarrow (\exists B)(\forall x \in A)(\exists y \in B)(\phi)) \quad (*)$$

2.1. *Opmerking.* De antecedent in (*) zegt, informeel, dat $\phi(x, y)$ op A een ‘functie’ definieert; de consequent garandeert dat die functie een co-domein heeft.

Verder mag B niet vrij in ϕ voorkomen omdat anders B in termen van zichzelf gedefinieerd zou worden.

Met behulp van het Afscheidingsaxioma kunnen we een ‘bereik’ maken.

► 12. Als ϕ en A als in het Vervangingsaxioma zijn dan bestaat — bij gegeven w_1, \dots, w_n — een verzameling B zó dat

$$(\forall y)(y \in B \leftrightarrow (\exists x)(x \in A \wedge \phi))$$

Producten, relaties, functies, ...

Laat A en B twee verzamelingen zijn; we definiëren

$$A \times B = \{\langle x, y \rangle : x \in A \wedge y \in B\}$$

Deze definitie is op twee manieren te rechtvaardigen. De eerste manier gebruikt het Vervangingsaxioma.

- 13. a. Voor elke vaste $x \in A$ geldt $(\forall y \in B)(\exists!z)(z = \langle x, y \rangle)$.
 b. De verzameling $p(x, B) = \{z : (\exists y \in B)(z = \langle x, y \rangle)\}$ bestaat.
 c. Nu geldt $(\forall x \in A)(\exists!z)(z = p(x, B))$
 d. De verzameling $p(A, B) = \{p(x, B) : x \in A\}$ bestaat.
 e. De verzameling $A \times B = \bigcup p(A, B)$ bestaat.

We kunnen $A \times B$ ook via de machtsverzameling definiëren — zie pagina 41. Het heeft zijn voordelen $A \times B$ op twee manieren te kunnen maken. Soms kun je goed gebruik maken van het feit dat een redenering of constructie zich geheel binnen een bepaalde verzameling afspeelt; binnen zo'n verzameling kun je vaak wel aan Vervanging doen maar heb je niet alle machtsverzamelingen tot je beschikking; het omgekeerde kan ook voorkomen: wel voldoende machtsverzamelingen maar niet voldoende Vervanging. In beide gevallen kunnen we dan toch over productverzamelingen beschikken.

Een *relatie* is een verzameling geordende paren; als R een relatie is dan

$$\text{dom } R = \{x : (\exists y)(\langle x, y \rangle \in R)\}$$

en

$$\text{ran } R = \{y : (\exists x)(\langle x, y \rangle \in R)\}$$

Deze definitie is equivalent met die welke door Peano gegeven is:

Perciè potremo definire il simbolo “Relatio” introdotto dai nostri Autori:

$$\text{Relatio} = u \ni [\exists(a; b) \ni [a, b \in \text{Cls} . u \in \text{Cls}'(a; b)]]$$

“Relazione è ogni ente u , che sia $\text{Cls}'(a; b)$, ove a e b sono classi che si possono determinare”.

- 14. Toon aan dat $\text{dom } R$ en $\text{ran } R$ bestaan en dat $R \subseteq \text{dom } R \times \text{ran } R$.

De samenstelling van relaties wordt als volgt gedefinieerd:

$$R \circ S = \{\langle x, z \rangle : (\exists y)(\langle x, y \rangle \in S \wedge \langle y, z \rangle \in R)\}$$

- 15. a. Toon aan dat $R \circ S$ goed-gedefinieerd is. *Hint*: Afscheiding binnen $\text{dom } S \times \text{ran } R$.
b. Toon aan: $(R \circ S) \circ T = R \circ (S \circ T)$.

Een functie is een relatie die aan de gebruikelijk eis voldoet:

$$\text{Funcio} = \text{Relatio} \cap u \ni [y; x \in u . z; x \in u . \supset_{x,y,z} . y = z] \quad \text{Def.}$$

Dus: f is een *functie* (of *afbeelding*) als f een relatie is en

$$(\forall x \in \text{dom } f)(\exists! y \in \text{ran } f)(\langle x, y \rangle \in f)$$

We noteren, als tevoren, de unieke y waarvoor $\langle x, y \rangle \in f$ als $f(x)$. Als $C \subseteq \text{dom } f$ dan $f \upharpoonright C = f \cap (C \times \text{ran } f)$ en $f[C] = \text{ran}(f \upharpoonright C)$

De uitdrukking $f : A \rightarrow B$ betekent: f is een functie, $\text{dom } f = A$ en $\text{ran } f \subseteq B$.

- 16. Toon aan: de samenstelling van twee functies is weer een functie.

Door de domein-onafhankelijke definities van relaties en functies kunnen we sommige eigenschappen net iets anders dan gebruikelijk formuleren.

De *inverse* van een relatie R is $R^{-1} = \{\langle y, x \rangle : \langle x, y \rangle \in R\}$. Een functie f is *injectief* als f^{-1} een functie is. Over *surjectief* en *bijjectief* spreken we alleen in de context van $f : A \rightarrow B$: als $\text{ran } f = B$ noemen we f surjectief en f is bijjectief als hij injectief en surjectief is.

Ordeningen

Laat A een verzameling zijn en R een relatie, waarbij niet gezegd is dat $R \subseteq A \times A$. De relatie R kan op A al dan niet de volgende eigenschappen hebben (we schrijven $x R y$ in plaats van $\langle x, y \rangle \in R$):

reflexiviteit: $(\forall x \in A)(x R x)$

irreflexiviteit: $(\forall x \in A)(\neg(x R x))$

symmetrie: $(\forall x, y \in A)(x R y \rightarrow y R x)$

anti-symmetrie: $(\forall x, y \in A)((x R y \wedge y R x) \rightarrow x = y)$

transitiviteit: $(\forall x, y, z \in A)((x R y \wedge y R z) \rightarrow x R z)$

Door deze formulering hoeven we bij overgang op een deelverzameling B van A niet eerst over de beperking van R tot B te spreken.

De verzameling A wordt door de relatie R *partieel geordend* als R op A reflexief, anti-symmetrisch en transitief is; we zeggen ook wel dat $\langle A, R \rangle$ een *partiële ordening* is.

De verzameling A wordt door de relatie R *totaal* of *lineair geordend* als R op A irreflexief en transitief is en voldoet aan

trichotomie: $(\forall x, y \in A)(x = y \vee x R y \vee y R x)$

we zeggen ook wel dat $\langle A, R \rangle$ een *totale ordening* of een *lineaire ordening* is.

Een *welordening* is een totale ordening $\langle A, R \rangle$ met de eigenschap dat elke niet-lege deelverzameling van A een R -kleinste element heeft:

$$(\forall B)((B \subseteq A \wedge B \neq \emptyset) \rightarrow (\exists x \in B)(\forall y \in B)(x = y \vee x R y))$$

Niet alleen voor welordeningen, maar voor relaties in het algemeen definiëren we nog voorgangersverzamelingen: als R een relatie is en $x \in A$ dan

$$\text{vg}(A, x, R) = \{y \in A : y R x\}.$$

Ordinaalgetallen

De definitie van ordinaalgetal uit Hoofdstuk 1 verandert niet. We verifiëren dat de uitspraken die we over ordinaalgetallen gedaan hebben geldig blijven.

2.2. DEFINITIE. Een verzameling x is *transitief* als elk element van x een deelverzameling van x is.

Bijvoorbeeld \emptyset , $\{\emptyset\}$ en $\{\emptyset, \{\emptyset\}\}$ zijn transitief, maar $\{\{\emptyset\}\}$ is dat niet. Een verzameling x die aan $x = \{x\}$ voldoet is ook transitief.

2.3. DEFINITIE. Een *ordinaalgetal* is een transitieve verzameling die door \in welgeordend wordt.

Iets preciezer, omdat \in geen *verzameling* geordende paren is: een transitieve x is een ordinaalgetal als $\langle x, \in_x \rangle$ een welordening is, waar $\in_x = \{\langle y, z \rangle \in x \times x : y \in z\}$.

Van de vier bovenbeschreven transitieve verzamelingen zijn de eerste drie ook ordinaalgetallen; de vierde is dat niet, omdat onze welordeningen per definitie irreflexief zijn.

We schrijven, als we het over ordinaalgetallen hebben, x in plaats van $\langle x, \in_x \rangle$ en $\text{vg}(x, y)$ in plaats van $\text{vg}(x, y, \in_x)$. De volgende opgave vat nog een keer samen wat we in Hoofdstuk 1 over ordinaalgetallen bewezen hebben

- 17. a. Als x een ordinaalgetal is en $y \in x$ dan is y een ordinaalgetal en $y = \text{vg}(x, y)$.
 b. Isomorfe ordinaalgetallen zijn gelijk.
 c. Als x en y ordinaalgetallen zijn dan geldt precies één van de volgende uitspraken: $x = y$, $x \in y$ of $y \in x$.
 d. Als x , y en z ordinaalgetallen zijn dan volgt uit $x \in y$ en $y \in z$ dat $x \in z$.
 e. Als C een niet-lege verzameling ordinaalgetallen is dan $(\exists x \in C)(\forall y \in C)(x \in y \vee x = y)$.

De paradox van Burali-Forti is nu ook weggewerkt.

2.4. STELLING. $\neg(\exists z)(\forall x)(x \text{ is een ordinaalgetal} \rightarrow x \in z)$.

- 18. Bewijs deze stelling. *Hint*: Met behulp van Afscheiding zou $\text{ON} = \{x : x \text{ is een ordinaalgetal}\}$ een verzameling zijn. Ga na dat ON transitief is en welgeordend door \in ; dus $\text{ON} \in \text{ON}$, tegenspraak.
- 19. Als A een verzameling ordinaalgetallen is en $(\forall x \in A)(\forall y \in x)(y \in A)$ dan is A zelf een ordinaalgetal.

Nu kunnen we Stelling 1.9 echt bewijzen.

2.5. STELLING. Als $\langle A, R \rangle$ een welordering is dan is er een uniek ordinaalgetal C zó dat $\langle A, R \rangle$ isomorf is met C .

- 20. Bewijs deze stelling.
 a. $B = \{a \in A : \langle \text{vg}(A, a, R), R \rangle \text{ is isomorf met een ordinaalgetal}\}$ is welgedefinieerd.
 b. $f = \{\langle a, x \rangle : a \in B, x \text{ is een ordinaalgetal en } \langle \text{vg}(A, a, R), R \rangle \text{ is isomorf met } x\}$ is een functie. *Hint*: Zij $\phi(a, x)$ de formule die uitdrukt dat $\langle \text{vg}(A, a, R), R \rangle$ en het ordinaalgetal x isomorf zijn. Pas nu Vervanging toe op $\phi(a, x) \wedge z = \langle a, x \rangle$.
 c. $C = \text{ran } f$ is een ordinaalgetal
 d. $B = A$ en f is een isomorfisme tussen $\langle A, R \rangle$ en C .

Als in Hoofdstuk 1 gebruiken we Griekse letters voor ordinaalgetallen. We schrijven ook meestal $\alpha < \beta$ in plaats van $\alpha \in \beta$, en $\alpha \leq \beta$ in plaats van $\alpha < \beta \vee \alpha = \beta$, enzovoort.

De definities van som, product en machtsverheffing blijven onveranderd; alsmede de definities van opvolger en limiet. We herinneren ons nog even dat $\alpha + 1 = \alpha \cup \{\alpha\}$.

De Natuurlijke getallen

We definiëren de natuurlijke getallen als speciale ordinaalgetallen.

2.6. DEFINITIE. Een ordinaalgetal α is een natuurlijk getal als

$$(\forall \beta \leq \alpha)(\beta = 0 \vee (\exists \gamma < \beta)(\beta = \gamma + 1)).$$

Dus $0 = \emptyset$ is een natuurlijk getal, en ook $1 = 0 + 1$, $2 = 1 + 1$, $3 = 2 + 1$, ...

- 21. Toon aan: als α een natuurlijk getal is en $\beta < \alpha$ dan is ook β een natuurlijk getal.

Zoals we later zullen zien zijn de axioma's tot nu toe niet sterk genoeg om ons te laten bewijzen dat de natuurlijke getallen een verzameling vormen. Hiervoor is echt een apart axioma nodig.

AXIOMA 7. ONEINDIGHEID. Er is een niet-lege verzameling die met elk element ook zijn opvolger bevat.

$$(\exists x)(\emptyset \in x \wedge (\forall y \in x)(y \cup \{y\} \in x))$$

Zij x een verzameling als in het Oneindigheidsaxioma.

- **22.** Toon aan: elk natuurlijk getal behoort tot x . *Hint:* Zij n een natuurlijk getal dat niet tot x behoort. Dan $n \neq 0$, dus er is een m met $n = m + 1$. Dan $m \in n \setminus x$, dus $n \setminus x \neq \emptyset$. Bekijk nu $n' = \min n \setminus x$.

We kunnen nu de *verzameling* der natuurlijke getallen uit x afscheiden.

2.7. DEFINITIE. De verzameling der natuurlijke getallen noteren we met ω .

Of de elementen van ω de ‘echte’ natuurlijke getallen zijn is meer een kwestie van smaak dan wat anders. Wat telt is dat ω doet wat wij van de natuurlijke getallen willen, namelijk dat ze voldoen aan de axioma’s van Peano (voor deze ene keer schrijven we $S(n)$ in plaats van $n + 1$):

- **23.** Toon aan.
- $0 \in \omega$
 - $(\forall n \in \omega)(S(n) \in \omega \wedge S(n) \neq 0)$
 - $(\forall n, m \in \omega)(n \neq m \rightarrow S(n) \neq S(m))$
 - Inductie: $(\forall X)((X \subseteq \omega \wedge 0 \in X \wedge (\forall n \in X)(S(n) \in X)) \rightarrow X = \omega)$

Deze opgave impliceert dat deze natuurlijke getallen goed genoeg zijn om de elementaire rekenkunde in te bedrijven en dat is alles wat we (in het begin) van ‘de natuurlijke getallen’ willen.

Verder kunnen we nu definiëren wat een eindige verzameling is: een verzameling x is *eindig* als er een $n \in \omega$ bestaat en een bijectieve afbeelding $f : n \rightarrow x$.

- **24.** Bewijs: een verzameling x is eindig dan en slechts dan als er een $n \in \omega$ en een *surjectieve* afbeelding $f : n \rightarrow x$ bestaan.

We kunnen nu verzamelingen van eindige rijtjes definiëren. Voor een natuurlijk getal n en een verzameling A is ${}^n A$ de verzameling van alle afbeeldingen van n naar A . De vraag is hoe deze verzameling gedefinieerd is. Dat gaat met behulp van de volgende formule $\phi(n, y)$

$$(\forall s)(s \in y \leftrightarrow (s : n \rightarrow A))$$

(zie de afkorting op pagina 34).

- **25.** a. Toon aan: $(\exists! y)(\phi(0, y))$. *Hint:* ${}^0 A = \{\emptyset\}$.
- b. Toon aan: als $(\exists! y)(\phi(n, y))$ dan $(\exists! z)(\phi(n + 1, z))$. *Hint:* Tweemaal vervanging. Voor $s \in y$ vast en voor elke $a \in A$ is er één $t : n + 1 \rightarrow A$ met $t(i) = s(i)$ als $i < n$ en $t(n) = a$; dit geeft een unieke verzameling A_s en dus de verzameling $\{A_s : s \in y\}$. Daarna: $z = \bigcup \{A_s : s \in y\}$ voldoet en Extensionaliteit garandeert uniciteit.
- c. Inductie: $(\forall n)(\exists! y)(\phi(n, y))$.

We noteren een element s van ${}^n A$ vaak als $\langle x_0, \dots, x_{n-1} \rangle$, waarbij $x_0 = s(0), \dots, x_{n-1} = s(n-1)$.

Nu kunnen we ook ${}^{<\omega} A$ definiëren, via Vervanging en Vereniging:

$${}^{<\omega} A = \bigcup \{{}^n A : n \in \omega\}$$

- **26.** Zij A een verzameling, dan bestaan voor elke $n \in \omega$ de volgende verzamelingen:
- $[A]^{\leq n}$: de familie deelverzamelingen met ten hoogste n elementen
 - $[A]^n$: de familie deelverzamelingen met precies n elementen

c. $[A]^{<\omega}$: de familie eindige deelverzamelingen

Meer algemeen: als s een functie is met een ordinaalgetal α als domein dan noteren we $s = \langle s_\beta : \beta < \alpha \rangle$. We kunnen dergelijke rijtjes aan elkaar plakken (concateneren): als $\text{dom } s = \alpha$ en $\text{dom } t = \beta$ dan is $s * t$ de functie met domein $\alpha + \beta$ en functiewaarden $(s * t)(\xi) = s(\xi)$ als $\xi < \alpha$ en $(s * t)(\alpha + \xi) = t(\xi)$ als $\xi < \beta$.

Inductie en Recursie

Het Inductieprincipe en het Recursieprincipe zoals geformuleerd in Hoofdstuk 1 zijn lokaal van aard maar we hebben ook globale versies van de principes nodig om ‘voor alle ordinaalgetallen’ stellingen te bewijzen en constructies uit te voeren.

Vaak worden die principes in termen van *klassen* geformuleerd. Dat zullen wij, omdat het goed bij de eerdere versies aansluit, ook doen. Daarom eerst iets over klassen. Een klasse is eigenlijk iets wat aan Cantor’s opvatting van verzameling beantwoordt: elke entiteit van de vorm

$$\{x : \phi(x)\},$$

waarin ϕ nog meer vrije variabelen dan alleen x mag hebben — die kunnen als parameter dienen. Een *echte klasse* is een klasse die geen verzameling is. De volgende twee klassen zijn echte klassen

$$\mathbf{V} = \{x : x = x\}$$

en

$$\mathbf{ON} = \{x : x \text{ is een ordinaalgetal}\},$$

zie Opgave 4 en Stelling 2.4. Formeel gesproken bestaan echte klassen niet maar ze maken het denken over bepaalde zaken wat makkelijker, zoals we zullen zien. We geven klassen met vette letters aan.

2.8. STELLING (Transfinite Inductie over \mathbf{ON}). *Als $\mathbf{C} \subseteq \mathbf{ON}$ en $\mathbf{C} \neq \emptyset$ dan heeft \mathbf{C} een minimum.*

BEWIJS. Zij $\alpha \in \mathbf{C}$ en bekijk de *verzameling* $\alpha \cap \mathbf{C}$. Als deze leeg is is α het gezochte minimum anders is $\min(\alpha \cap \mathbf{C})$ dat (zie Opgave 17). \square

Deze stelling representeert in feite oneindig veel stellingen: voor elke formule één. Immers, als $\mathbf{C}(x, z_1, \dots, z_n)$ een formule is dan zegt de stelling het volgende

$$(\forall z_1) \cdots (\forall z_n) \left(((\forall x)(\mathbf{C} \rightarrow \mathbf{ON}(x)) \wedge (\exists x)(\mathbf{C})) \rightarrow (\exists x)(\mathbf{C} \wedge (\forall y)(\mathbf{C}(y, z_1, \dots, z_n) \rightarrow x \leq y)) \right)$$

Het bewijs van de formele vorm loopt net als het gegeven bewijs; door het gebruik van allerlei formules wordt het een stuk minder leesbaar.

We kunnen deze stelling gebruiken bij transfinite-inductiebewijzen: als we voor alle α de implicatie $((\forall \beta < \alpha)\psi(\beta)) \rightarrow \psi(\alpha)$ bewezen hebben mogen we $(\forall \alpha)\psi(\alpha)$ concluderen.

Evenzo krijgen we een globaal recursieprincipe.

2.9. STELLING (Transfinite Recursie over \mathbf{ON}). *Als $\mathbf{F} : \mathbf{V} \rightarrow \mathbf{V}$ dan is er een unieke $\mathbf{G} : \mathbf{ON} \rightarrow \mathbf{V}$ zó dat $(\forall \alpha)(\mathbf{G}(\alpha) = \mathbf{F}(\mathbf{G} \upharpoonright \alpha))$.*

BEWIJS. Uniciteit volgt met transfinitie inductie: aangenomen dat \mathbf{G}_1 en \mathbf{G}_2 voldoen, bewijst men dat $\mathbf{C} = \mathbf{ON}$, waar $\mathbf{C} = \{\alpha : \mathbf{G}_1(\alpha) = \mathbf{G}_2(\alpha)\}$.

Het bewijs van het bestaan van \mathbf{G} verloopt als in het bewijs van Stelling 1.7: we maken hem als de ‘vereniging’ van benaderingen. Een benadering is een functie g met domein een ordinaalgetal en zó dat $(\forall \alpha \in \text{dom } g)(g(\alpha) = \mathbf{F}(g \upharpoonright \alpha))$. Nu moeten twee dingen bewezen worden:

- Als g en h benaderingen zijn dan geldt $g(\alpha) = h(\alpha)$ voor $\alpha \in \text{dom } g \cap \text{dom } h$.
- Voor elk ordinaalgetal γ is er een benadering met domein γ .

Dan definiëren we $\mathbf{G} = \{\langle \alpha, x \rangle : (\exists g)(g \text{ is een benadering, } \alpha \in \text{dom } g \text{ en } g(\alpha) = x)\}$. \square

De formele versie van de stelling gaat uit van een formule $\mathbf{F}(x, y)$ (met eventueel andere vrije variabelen) en zegt dat men expliciet een formule $\mathbf{G}(v, y)$ kan bouwen, min of meer als in de laatste regel van het bewijs, zó dat het volgende bewezen kan worden

$$(\forall x)(\exists! y) \mathbf{F}(x, y) \rightarrow ((\forall \alpha)(\exists! y) \mathbf{G}(\alpha, y) \wedge (\forall \alpha)(\exists x)(\exists y)(\mathbf{G}(\alpha, y) \wedge \mathbf{F}(x, y) \wedge x = \mathbf{G} \upharpoonright \alpha))$$

Waarbij $x = \mathbf{G} \upharpoonright \alpha$ staat voor

$$x \text{ is een functie } \wedge \text{dom } x = \alpha \wedge (\forall \beta \in \text{dom } x)(\mathbf{G}(\beta, x(\beta)))$$

Uniciteit komt nu neer op equivalentie van formules (wat natuurlijk betekent dat de bijbehorende klassen gelijk zijn): onder analoge voorwaarden voor \mathbf{F} en \mathbf{G}' bewijst men $(\forall \alpha)(\forall y)(\mathbf{G}(\alpha, y) \leftrightarrow \mathbf{G}'(\alpha, y))$.

De volgende opgave rechtvaardigt, uiteindelijk, de werkwijze in Opgave 55 van Hoofdstuk 1.

- 27. a. Zij $\mathbf{F} : \mathbf{V} \rightarrow \mathbf{V}$ en zij $\langle X, < \rangle$ een welordening. Bewijs dat er een functie f bestaat met domein X en zó dat $f(x) = \mathbf{F}(f \upharpoonright \hat{x})$ voor alle $x \in X$.
- b. Toon aan: met $\mathbf{F} = \{\langle x, \text{ran } x \rangle : x \in \mathbf{V}\}$ krijgen we een isomorfisme tussen X en zijn kanonieke representant.

Kardinaalgetallen

In onze opbouw van de verzamelingenleer zijn kardinaalgetallen speciale ordinaalgetallen en hebben, bijgevolg, alleen welordenbare verzamelingen een welbepaald kardinaalgetal.

2.10. DEFINITIE. Laat A en B verzamelingen zijn.

- (1) $A \preceq B$ betekent dat er een injectie van A naar B bestaat,
- (2) $A \approx B$ betekent dat er een bijectie van A naar B bestaat,
- (3) $A \prec B$ betekent $A \preceq B$ en $B \not\preceq A$

In feite definiëren we hiermee klassen geordende paren, ofwel formules waar paren verzamelingen al dan niet aan kunnen voldoen. Hoewel we dit eigenlijk bij iedere definitie in het achterhoofd moeten houden zal dat idee snel vervagen en gaan we weer ‘gewoon’ met verzamelingen om.

Stelling 1.2 blijft geldig: als $A \preceq B$ en $B \preceq A$ dan volgt $A \approx B$.

2.11. DEFINITIE. Als A een welordenbare verzameling is dan is $|A|$ het kleinste ordinaalgetal α met $A \approx \alpha$.

Dus als we $|A|$ schrijven nemen we impliciet aan dat A te welordenen is. Voor welordenbare verzamelingen A en B geldt $A \approx B$ dan en slechts dan als $|A| = |B|$, en natuurlijk ook $A \approx |A|$. Voor welordenbare verzamelingen kiest de operatie $|A|$ een welbepaald element uit de bijbehorende \approx -equivalentieklasse.

Voor elk ordinaalgetal α bestaat $|\alpha|$ en geldt $|\alpha| \leq \alpha$.

2.12. DEFINITIE. Een ordinaalgetal α is een kardinaalgetal als $\alpha = |\alpha|$.

Een equivalente uitspraak is $(\forall \beta < \alpha)(\beta \not\approx \alpha)$.

► 28. Toon aan: als $|\alpha| \leq \beta \leq \alpha$ dan $|\beta| = |\alpha|$.

- 29. Laat $n \in \omega$, toon aan
- $n \not\approx n + 1$. *Hint*: Inductie.
 - $(\forall \alpha)(\alpha \approx n \rightarrow \alpha = n)$

Hiermee hebben we onze eerste kardinaalgetallen te pakken.

2.13. STELLING. ω is een kardinaalgetal en elke $n \in \omega$ is een kardinaalgetal.

2.14. DEFINITIE. Een verzameling A is

eindig: als $|A| < \omega$,

oneindig: als hij niet eindig is,

aftelbaar: als $|A| \leq \omega$,

overaftelbaar: als hij niet aftelbaar is.

- 30. Bewijs: elk oneindig kardinaalgetal is een limiet-ordinaalgetal. *Hint*: als $\alpha \geq \omega$ dan $\alpha \approx \alpha + 1$.
- 31. Toon aan: A is aftelbaar dan en slechts dan als er een surjectieve afbeelding $f : \omega \rightarrow A$ bestaat.

De letters κ , λ en μ duiden meestal oneindige kardinaalgetallen aan. Het optellen en vermenigvuldigen van kardinaalgetallen gaat nagenoeg hetzelfde als in Hoofdstuk 1; de betekenis van de formules is nu anders.

2.15. DEFINITIE. Laat κ en λ kardinaalgetallen zijn.

- $\kappa \oplus \lambda = |\kappa \times \{0\} \cup \lambda \times \{1\}|$
- $\kappa \otimes \lambda = |\kappa \times \lambda|$

De tweede definitie is gerechtvaardigd omdat de lexicografische orde op $\kappa \times \lambda$ een welorde is.

- 32. Toon aan
- $|\kappa + \lambda| = |\lambda + \kappa| = \kappa \oplus \lambda$
 - $|\kappa \cdot \lambda| = |\lambda \cdot \kappa| = \kappa \otimes \lambda$
 - Voor $n, m \in \omega$ geldt $n \oplus m = n + m$ en $n \otimes m = n \cdot m$.
- 33. a. Toon aan: $\kappa \oplus \kappa = \kappa$.
- b. Toon aan: $\kappa \oplus \lambda = \max\{\kappa, \lambda\}$.

Omdat de kardinaalgetallen een deelklasse van **ON** vormen kunnen we ook voor kardinaalgetallen van transfinitie inductie gebruik maken.

2.16. STELLING. Als κ een oneindig kardinaalgetal is dan $\kappa \otimes \kappa = \kappa$.

Het bewijs van deze stelling maakt gebruik van een speciale welordening van $\kappa \times \kappa$, in feite van een klasse die $\mathbf{ON} \times \mathbf{ON}$ welordent. Definieer $\langle \alpha, \beta \rangle \triangleleft \langle \gamma, \delta \rangle$ als

- $\max\{\alpha, \beta\} < \max\{\gamma, \delta\}$, of
- $\max\{\alpha, \beta\} = \max\{\gamma, \delta\}$ en $\beta < \delta$, of
- $\max\{\alpha, \beta\} = \max\{\gamma, \delta\}$ en $\beta = \delta$ en $\alpha < \gamma$.

- 34. Toon aan: het type van $\langle \{\langle \beta, \gamma \rangle : \max\{\beta, \gamma\} = \alpha \rangle, \triangleleft \rangle$ is $\alpha + \alpha + 1$. *Hint*: teken een plaatje.
- 35. Toon aan: $\alpha \times \alpha = \{ \langle \beta, \gamma \rangle : \langle \beta, \gamma \rangle \triangleleft \langle \alpha, 0 \rangle \}$.
- 36. Toon aan: het type van $\langle \omega \times \omega, \triangleleft \rangle$ is ω .
- 37. Toon aan: $|\alpha \times \alpha| = |\alpha|$ voor elk oneindig ordinaalgetal α . *Hint*: Toon aan: als α een kardinaalgetal is dan is het type van $\langle \alpha \times \alpha, \triangleleft \rangle$ gelijk aan α .
- 38. Bewijs dat elk kardinaalgetal een ε -getal is.

Overaftelbare verzamelingen

De axioma's tot nu toe laten vooralsnog toe dat *elke* verzameling aftelbaar is; het bestaan van niet-aftelbare (*overaftelbare*) verzamelingen vergt een nieuw axioma.

AXIOMA 8. MACHTSVERZAMELING. Bij elke verzameling bestaat een verzameling die de deelverzamelingen van de gegeven verzameling als elementen heeft:

$$(\forall x)(\exists y)(\forall z)(z \subseteq x \rightarrow z \in y)$$

We kunnen hier, met behulp van het Afscheidingsaxioma, weer een afkorting bij maken: de *machtsverzameling van x* , genoteerd $\mathcal{P}(x)$, bestaat uit precies alle deelverzamelingen van x .

- 39. Bij elke verzameling bestaat precies één verzameling die uit precies alle deelverzamelingen van de gegeven verzameling bestaat.

Voor we verder gaan lossen we nog een belofte in en geven aan hoe $A \times B$ met behulp van dit axioma gemaakt kan worden.

- 40. Laat A en B verzamelingen zijn.
- a. Als $x \in A$ en $y \in B$ dan $\{x\}, \{x, y\} \in \mathcal{P}(A \cup B)$.
 - b. Als $x \in A$ en $y \in B$ dan $\langle x, y \rangle \in \mathcal{P}(\mathcal{P}(A \cup B))$.
 - c. $A \times B = \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) : (\exists x \in A)(\exists y \in B)(z = \langle x, y \rangle)\}$

Het diagonaalargument blijft, natuurlijk, geldig.

2.17. STELLING. Zij A een verzameling dan $A \prec \mathcal{P}(A)$.

De afbeelding $x \mapsto \{x\}$ laat zien dat $A \preceq \mathcal{P}(A)$ en met behulp van het diagonaalargument volgt dat $A \not\approx \mathcal{P}(A)$.

We hebben nu tenminste één overaftelbare verzameling te pakken: $\mathcal{P}(\omega)$. Wat we (nog) niet hebben is zijn kardinaalgetal omdat we (nog) niet weten of $\mathcal{P}(\omega)$ te welordenen is.

Om steeds grotere welgeordende verzamelingen te maken gebruiken we de methode van pagina 21 en het Vervangingsaxioma.

Zij X een verzameling en bekijk

$$W(X) = \{ \langle A, R \rangle : A \in \mathcal{P}(X), R \in \mathcal{P}(X \times X) \text{ en } R \text{ welordent } A \}$$

Dit is een welgedefinieerde verzameling en dankzij Stelling 2.5 kunnen we Vervanging toepassen om de functie $\{ \langle x, \alpha \rangle : x \in W(X), \alpha \text{ een ordinaalgetal en } \alpha \text{ is het type van } x \}$ te maken en daarmee de waardenverzameling $\aleph(X)$.

- 41. a. Toon aan: $\aleph(X)$ is het kleinste ordinaalgetal α dat *niet* voldoet aan $\alpha \preceq X$.
 b. Toon aan: $\aleph(X)$ is een kardinaalgetal.
 c. Toon aan: als α een ordinaalgetal is dan $|\alpha| < \aleph(\alpha)$ en $\aleph(\alpha)$ is het kleinste kardinaalgetal groter dan α .
 d. Toon aan: er bestaan willekeurig grote kardinaalgetallen.

De ‘functie’ $X \mapsto \aleph(X)$ heet wel Hartogs’ Aleph.

- 42. a. Toon aan: $\aleph(X) < \aleph(\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(X)))))$
 b. Bewijs: $\aleph(X) < \aleph(\mathcal{P}(\mathcal{P}(\mathcal{P}(X))))$
 c. Er is geen rij $\langle X_n : n \in \omega \rangle$ van verzamelingen die voldoet aan $(\forall n)(\mathcal{P}(X_{n+1}) \preceq X_n)$.

Met behulp van de \aleph -functie en transfinitie recursie definiëren we de ‘rij’ van alle oneindige kardinaalgetallen $\langle \omega_\alpha : \alpha \in \mathbf{ON} \rangle$ als volgt:

- $\omega_0 = \omega$,
- $\omega_{\alpha+1} = \aleph(\omega_\alpha)$,
- $\omega_\alpha = \bigcup_{\beta < \alpha} \omega_\beta$, als α een limiet is.

Voor elk ordinaalgetal α schrijven we, hoewel niet strikt nodig, ook $\aleph_\alpha = \omega_\alpha$; de \aleph_α wordt meestal in kardinaal-context gebruikt en ω_α in ordinaal-context.

De welordeningsstelling

Tot nu toe hebben we het uitstekend zonder het Keuzeaxioma kunnen stellen. Om echter machten van kardinaalgetallen te kunnen definiëren moeten we weten dat bepaalde verzamelingen te welordenen zijn en dat kunnen we alleen met behulp van het Keuzeaxioma bewijzen.

AXIOMA 9. KEUZEAXIOMA. Elke familie niet-lege verzamelingen heeft een keuzefunctie

$$(\forall x)(\emptyset \notin x \rightarrow (\exists f)((f : x \rightarrow \bigcup x) \wedge (\forall y \in x)(f(y) \in y)))$$

De welordeningsstelling van een verzameling hangt van een specifiek geval van het Keuzeaxioma af.

2.18. STELLING (Lokale Welordeningsstelling). Voor een verzameling X zijn equivalent:

- (a) X kan welgeordend worden
 (b) Er is een functie $C : \mathcal{P}(X) \setminus \{\emptyset\} \rightarrow X$ zó dat $(\forall Y \subseteq X)(Y \neq \emptyset \rightarrow C(Y) \in Y)$

- 43. Bewijs deze stelling.
 a. Toon aan: (a) impliceert (b)
 b. Toon aan: (b) impliceert (a). *Hint*: Pas het Recursieprincipe (Stelling 1.7) toe met $\aleph(X)$ op de plaats van X , met X op de plaats van Y en een geschikte functie F .

De volgende opgave bevat Zermelo’s eerste bewijs, uit [1904], van de Welordeningsstelling; het is in feite het bewijs uit de vorige opgave maar met de toepassing van het

Recursieprincipe expliciet gemaakt en met vermindering van het gebruik van ordinaalgetallen.

- 44. Noem een welordering $\langle M, \prec \rangle$ een C -verzameling als $M \subseteq X$ en als voor elke $x \in M$ geldt dat $x = C(A)$, waarbij $A = X \setminus \{y \in M : y \prec x\}$.
- Toon aan: er zijn C -verzamelingen
 - Toon aan: Als $\langle M, \prec \rangle$ en $\langle N, < \rangle$ beide C -verzamelingen zijn dan is M een beginstuk van N of omgekeerd en de ordeningen stemmen op de kleinere verzameling overeen.
 - Toon aan: De vereniging Y van alle C -verzamelingen is weer een C -verzameling.
 - Toon aan: $Y = X$.

Wat later, in [1908a], gaf Zermelo nog een bewijs van de Welordeningsstelling; hier zijn de recursie en eventueel impliciet gebruik van ordinaalgetallen helemaal weggewerkt.

- 45. Een deelverzameling \mathcal{A} van $\mathcal{P}(X)$ heet een C -keten als $X \in \mathcal{A}$, als voor elke $A \in \mathcal{A} \setminus \{\emptyset\}$ geldt dat $A' = A \setminus \{C(A)\} \in \mathcal{A}$ en als $\bigcap \mathcal{A}' \in \mathcal{A}$ voor elke $\mathcal{A}' \subseteq \mathcal{A}$.
- Toon aan: $\mathcal{P}(X)$ is een C -keten.
 - Toon aan: als \mathfrak{A} een familie C -ketens is dan is ook $\bigcap \mathfrak{A}$ een C -keten.
- Zij \mathcal{W} de doorsnede van de familie van alle C -ketens. Noem $A \in \mathcal{W}$ *vergelijkbaar* als voor elke $U \in \mathcal{W}$ geldt dat $U \subseteq A$ of $A \subseteq U$.
- Toon aan: X is vergelijkbaar.
 - Toon aan: als A vergelijkbaar is dan is A' het ook. *Hint:* Toon aan dat $\{U \in \mathcal{W} : U \subseteq A' \text{ of } A \subseteq U\}$ een C -keten is.
 - Toon aan: als $\mathcal{W}' \subseteq \mathcal{W}$ uit vergelijkbare elementen bestaat dan is $\bigcap \mathcal{W}'$ ook vergelijkbaar.
 - Toon aan: elk element van \mathcal{W} is vergelijkbaar.
 - Zij $Y \subseteq X$ willekeurig. Toon aan: er is een uniek element W_Y van \mathcal{W} dat voldoet aan $Y \subseteq W_Y$ en $C(W_Y) \in Y$. *Hint:* $W = \bigcap \{A \in \mathcal{W} : Y \subseteq A\}$.

In het bijzonder hoort dus bij elk element x van X een unieke $W_x \in \mathcal{W}$ met $x \in W_x$ en $x = C(W_x)$. Definieer $x \prec y$ als $y \in W_x'$.

- Bewijs dat \prec een welordering van X is.

Stelling 2.18 impliceert dat het Keuzeaxioma equivalent is met de (Globale) Welordeningsstelling, die zegt dat elke verzameling welgeordend kan worden. Hier betekent 'equivalent' dat de formule

$$\text{Keuzeaxioma} \leftrightarrow \text{Welordeningsstelling}$$

uitgaande van de axioma's van Zermelo en Fraenkel bewezen kan worden.

We formuleren nog twee uitspraken die, in deze zin, equivalent zijn met het Keuzeaxioma. Beide staan bekend als maximaliteitsprincipes: ze garanderen het bestaan van maximale elementen in bepaalde collecties. In het algemeen, als R een relatie is en A een verzameling dan heet $a \in A$ *maximaal* (ten opzichte van R) als $(\forall b \in A)(a R b \rightarrow b = a)$.

HET LEMMA VAN ZORN. Zij $\langle P, \leq \rangle$ een partiële ordening met de eigenschap dat elke *lineair* geordende deelverzameling van P een bovengrens heeft. Dan heeft P maximale elementen (ten opzichte van \leq).

HET LEMMA VAN TEICHMÜLLER EN TUKEY. Zij \mathcal{F} een familie deelverzamelingen van een verzameling X met de eigenschap dat $F \in \mathcal{F}$ dan en slechts dan als *elke eindige* deelverzameling van F tot \mathcal{F} behoort. Dan bevat \mathcal{F} maximale elementen (ten opzichte van \subseteq).

- 46. Bewijs dat deze twee uitspraken inderdaad equivalent zijn met het Keuzeaxioma.

Enige gevolgen van het Keuzeaxioma in de Wiskunde zijn

1. De stelling van Tychonoff: elk product van compacte ruimten is compact.
2. Elke vectorruimte heeft een basis.
3. Elke commutatieve ring met 1 heeft maximale idealen.
4. De stelling van Hahn-Banach.
5. Er bestaan niet-meetbare deelverzamelingen van \mathbb{R} .

De stelling van Tychonoff voor T_1 -ruimten is equivalent met het Keuzeaxioma; de versie voor Hausdorff ruimten is strikt zwakker, maar niet uit de axioma's van Zermelo en Fraenkel te bewijzen. Gevolg 2 is ook equivalent met het Keuzeaxioma, mits geen beperking aan het grondlichaam wordt opgelegd. De laatste drie zijn strikt zwakker dan het Keuzeaxioma maar onbewijsbaar in de theorie van Zermelo en Fraenkel; 3 en 4 impliceren elk 5 en Solovay heeft laten zien dat 5 niet bewijsbaar is.

We nemen van nu af het Keuzeaxioma aan. Af en toe, als het belangrijk is, zullen we expliciet opmerken of het Keuzeaxioma echt nodig is of vermeden kan worden.

Machten en producten van kardinaalgetallen

Machtsverheffen en vermenigvuldigen van (willekeurig veel) kardinaalgetallen gaan via verzamelingen functies.

2.19. DEFINITIE. Als κ en λ kardinaalgetallen zijn dan $\kappa^\lambda = |\lambda^\kappa|$.

- 47. Toon aan: de verzameling ${}^\lambda\kappa$ bestaat. *Hint:* ${}^\lambda\kappa \subseteq \mathcal{P}(\kappa \times \lambda)$.

Op dezelfde manier kan het bestaan van willekeurige productverzamelingen worden aangetoond. Als X een familie verzamelingen is dan

$$\prod X = \{f \in \mathcal{P}(X \times \bigcup X) : (f : X \rightarrow \bigcup X) \wedge (\forall x \in X)(x \neq \emptyset \rightarrow f(x) \in x)\}$$

Het product van een familie kardinaalgetallen is dan het kardinaalgetal van de bijbehorende productverzameling; de definitie van de som van zo'n familie geven we meteen mee.

2.20. DEFINITIE. Zij $\{\kappa_i : i \in I\}$ een verzameling kardinaalgetallen. Dan

- $\otimes_{i \in I} \kappa_i = \left| \prod_{i \in I} \kappa_i \right|$
- $\oplus_{i \in I} \kappa_i = \left| \bigcup_{i \in I} (\kappa_i \times \{i\}) \right|$

Voor de definitie van de som is het Keuzeaxioma ook nodig: we moeten weten dat de vereniging welgeordend kan worden.

De stelling van König, Stelling 1.5, is in deze context ook geldig; het bewijs kan nu zonder het Keuzeaxioma geleverd worden, om de flauwe reden dat we alleen met welgeordende verzamelingen werken.

De oude rekenregels voor vermenigvuldiging en machtsverheffen behoeven geen nieuw bewijs: ze waren en blijven gebaseerd op het bestaan van bijjecties.

- 48. Bewijs: als $\lambda \geq \omega$ en $2 \leq \kappa \leq \lambda$ dan $\kappa^\lambda = 2^\lambda$.

Als X een verzameling is en κ een kardinaalgetal dan definiëren we

- $[X]^\kappa = \{A \in \mathcal{P}(X) : |A| = \kappa\}$;

- $[X]^{<\kappa} = \{A \in \mathcal{P}(X) : |A| < \kappa\}$; en
- $[X]^{\leq\kappa} = \{A \in \mathcal{P}(X) : |A| \leq \kappa\}$.

► 49. Laat $\lambda \leq \kappa$. Bedenk en bewijs formules voor het kardinaalgetal van $[\kappa]^{<\lambda}$, $[\kappa]^{\leq\lambda}$ en $[\kappa]^\lambda$.

Regulariteit

Als laatste bespreken we de gevolgen van het Regulariteitsaxioma.

AXIOMA 2. REGULARITEIT. Elke verzameling heeft een \in -minimaal element:

$$(\forall x)((\exists y)(y \in x) \rightarrow (\exists y)(y \in x \wedge \neg(\exists z)(z \in x \wedge z \in y)))$$

Dit axioma is van een wat andere soort dan de andere: in plaats van gereedschap voor het maken van nieuwe verzamelingen aan te reiken legt het ons een beperking op.

- 50. a. Toon aan: er is geen verzameling x met $x = \{x\}$.
 b. Toon aan: er is geen rij $\langle x_n : n \in \omega \rangle$ van verzamelingen die voldoet aan $x_{n+1} \in x_n$ voor alle n .

Dankzij het Regulariteitsaxioma kunnen de klasse \mathbf{V} van alle verzamelingen stelselmatig opbouwen. Met behulp van transfinitie recursie definiëren we een rij $\langle V_\alpha : \alpha \in \mathbf{ON} \rangle$ (eigenlijk een klasse dus) als volgt.

- $V_0 = \emptyset$,
- $V_{\alpha+1} = \mathcal{P}(V_\alpha)$, en
- $V_\alpha = \bigcup_{\beta < \alpha} V_\beta$ als α een limiet is.

- 51. Toon aan: voor elke α geldt
 a. V_α is transitief
 b. $(\forall \beta \leq \alpha)(V_\beta \subseteq V_\alpha)$

2.21. STELLING. *Het Regulariteitsaxioma is equivalent met de gelijkheid $\mathbf{V} = \bigcup_{\alpha \in \mathbf{ON}} V_\alpha$.*

Voor het bewijs van deze stelling moeten we eerst wat voorwerk doen. We schrijven, voorlopig, $\mathbf{U} = \bigcup_{\alpha \in \mathbf{ON}} V_\alpha$ en definiëren de rang van een $x \in \mathbf{U}$ als

$$\text{rang}(x) = \min\{\alpha : x \in V_{\alpha+1}\}.$$

De rangfunctie heeft een aantal nuttige eigenschappen.

- 52. a. Toon aan: voor elke α geldt $V_\alpha = \{x \in \mathbf{U} : \text{rang}(x) < \alpha\}$.
 b. Toon aan: als $y \in x \in \mathbf{U}$ dan $y \in \mathbf{U}$ en $\text{rang}(y) < \text{rang}(x)$.
 c. Toon aan: als $x \in \mathbf{U}$ dan $\text{rang}(x) = \sup\{\text{rang}(y) + 1 : y \in x\}$.
- 53. Toon aan: voor elke α geldt
 a. $\alpha \in \mathbf{U}$ en $\text{rang}(\alpha) = \alpha$;
 b. $\alpha = V_\alpha \cap \mathbf{ON}$.

Het bewijs van Stelling 2.21 is nu niet moeilijk meer. We hebben nog wel een nieuw begrip nodig.

De *transitieve afsluiting* van een verzameling is de kleinste transitieve verzameling waarvan de gegeven verzameling een deelverzameling is. eze maken we als volgt:

- $\bigcup^0 X = X$;
- $\bigcup^{n+1} X = \bigcup(\bigcup^n X)$; en

- $\text{trcl } X = \bigcup \{ \bigcup^n X : n \in \omega \}$.
- 54. Toon aan:
 - a. $X \subseteq \text{trcl } X$.
 - b. $\text{trcl } X$ is transitief.
 - c. Als Y transitief is en $X \subseteq Y$ dan $\text{trcl } X \subseteq Y$.
 - d. Als X transitief is dan $X = \text{trcl } X$.
 - e. $\text{trcl } X = X \cup \bigcup \{ \text{trcl } x : x \in X \}$.
- 55. Toon aan: voor elke x geldt $x \in \mathbf{U}$ dan en slechts dan als $x \subseteq \mathbf{U}$.
- 56. Toon aan: als $x \in \mathbf{U}$ dan is er een $y \in x$ zó dat $y \cap x = \emptyset$. *Hint*: neem y van minimale rang.
- 57. Bewijs: voor elke x geldt $x \in \mathbf{U}$. *Hint*: als $x \notin \mathbf{U}$ neem dan een minimale $y \in \text{trcl } x \setminus \mathbf{U}$.

Het Regulariteitsaxioma is er, voor ons, vooral om ons het leven wat makkelijker te maken. De gelijkheid $\mathbf{V} = \mathbf{U}$ stelt ons in staat veel dingen over verzamelingen met transfinitie inductie te bewijzen of met transfinitie recursie te construeren. Verzamelingen als in Opgave 50 zitten daarbij gewoon in de weg; het Regulariteitsaxioma is een manier om die links te laten liggen. Waar we wel op moeten letten is dat we niet een kind of twee met het badwater weggooien. Dat laatste is, dankzij het Keuzeaxioma, gelukkig niet het geval: elke structuur die we tegenkomen — groep, ring, topologische ruimte, ... — heeft een onderliggende verzameling; door deze te welordenen kunnen we er een (isomorfe) kopie van maken met een ordinaalgetal als onderliggende verzameling. Dit betekent dat we de Wiskunde net zo goed binnen \mathbf{U} kunnen bedrijven en dat is wat het Regulariteitsaxioma formaliseert.

De Wiskunde in de verzamelingenleer

We laten zien hoe een paar bekende verzamelingen binnen \mathbf{V} terug te vinden zijn.

Natuurlijke, gehele en rationale getallen

We hebben in ω al een structuur gevonden die zich als de verzameling der natuurlijke getallen gedraagt. We spreken dus af $\mathbb{N} = \omega$.

De gehele getallen kunnen op een natuurlijke manier uit \mathbb{N} gemaakt worden. Definieer een relatie \sim op \mathbb{N}^2 door

$$\langle k, l \rangle \sim \langle m, n \rangle \text{ als } k + n = m + l$$

Dit is een equivalentierelatie, waarbij de klasse van $\langle k, l \rangle$, genoteerd $[\langle k, l \rangle]$, het verschil $k - l$ representeert. De gehele getallen zijn, per definitie, de equivalentieclassen onder deze relatie; we noteren die verzameling met \mathbb{Z} .

- 58. a. Toon aan: \sim is een equivalentierelatie.
- b. Toon aan: $[\langle k, l \rangle] + [\langle m, n \rangle] = [\langle k + m, l + n \rangle]$ is een goedgedefinieerde binaire operatie op \mathbb{Z} .
- c. Toon aan: $[\langle k, l \rangle] \times [\langle m, n \rangle] = [\langle km + ln, kn + lm \rangle]$ is een goedgedefinieerde binaire operatie op \mathbb{Z} .
- d. Toon aan: $\langle \mathbb{Z}, +, \times \rangle$ is een integriteitsgebied (bij Algebra 1 ook wel domein genoemd).
- e. Toon aan: $[\langle k, l \rangle] < [\langle m, n \rangle]$ als $k + n < m + l$ definieert een lineaire ordening op \mathbb{Z} .

f. Toon aan: $n \mapsto \langle n, 0 \rangle$ identificeert \mathbb{N} met de niet-negatieve gehele getallen.

Om de rang van \mathbb{Z} te bepalen eerst wat voorbereidend werk.

- 59. Druk de rang van $\{x, y\}$, $\langle x, y \rangle$, $\bigcup x$, $x \times y$ en $\mathcal{P}(x)$ uit in die van x en y .
- 60. Bepaal de rang van \mathbb{Z} .

In de algebra wordt \mathbb{Q} gedefinieerd als het quotiëntenlichaam van \mathbb{Z} . Definieer een equivalentierelatie \approx op $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ door

$$\langle k, l \rangle \approx \langle m, n \rangle \text{ als } k \cdot n = m \cdot l$$

Dit is een equivalentierelatie en de klasse van $\langle k, l \rangle$, weer genoteerd als $[\langle k, l \rangle]$, representeert het quotiënt k/l . de verzameling equivalentieclassen noteren we met \mathbb{Q} .

- 61. a. Toon aan: \approx is een equivalentierelatie.
- b. Toon aan: $[\langle k, l \rangle] + [\langle m, n \rangle] = [\langle k \cdot n + l \cdot m, l \cdot n \rangle]$ is een goedgedefinieerde binaire operatie op \mathbb{Q} .
- c. Toon aan: $[\langle k, l \rangle] \cdot [\langle m, n \rangle] = [\langle k \cdot m, l \cdot n \rangle]$ is een goedgedefinieerde binaire operatie op \mathbb{Q} .
- d. Toon aan: $\langle \mathbb{Q}, +, \cdot \rangle$ is een lichaam.
- e. Toon aan: $[\langle k, l \rangle] < [\langle m, n \rangle]$ als $(kn - ml)ln > 0$ definieert een lineaire ordening op \mathbb{Q} .
- f. Toon aan: voor elke $q \in \mathbb{Q}$ bestaat een $n \in \mathbb{N}$ zó dat $q < [\langle n, 1 \rangle]$.
- 62. Bepaal de rang van \mathbb{Q} .

Reële getallen

De reële rechte \mathbb{R} maken we door middel van Dedekind-snedes. Een deelverzameling D van \mathbb{Q} is een *Dedekind-snedes* als D een echt beginstuk van \mathbb{Q} zonder maximum is.

- 63. Ga na dat $\{q \in \mathbb{Q} : q < 3\}$ en $\{q \in \mathbb{Q} : q < 0 \text{ of } q^2 < 5\}$ Dedekind-snedes zijn.

De reële rechte is de verzameling van alle Dedekind-snedes:

$$\mathbb{R} = \{A \in \mathcal{P}(\mathbb{Q}) : (\forall x, y \in \mathbb{Q})((y < x \wedge x \in A) \rightarrow y \in A) \wedge (\forall x \in A)(\exists y \in A)(x < y)\}$$

Elk rationaal getal q bepaalt een snede: $\{x \in \mathbb{Q} : x < q\}$.

Definieer de som van twee snedes s en t door

$$s + t = \{x + y : x \in s \wedge y \in t\}$$

- 64. a. Bewijs dat de optelling goedgedefinieerd is: $s + t$ is weer een snede.
- b. Bewijs dat $\langle \mathbb{R}, + \rangle$ een Abelse groep is.

De ordening van \mathbb{R} is de gewone inclusie: $s < t$ betekent $s \subset t$. Noem s positief als $0 < s$, dat wil zeggen, als $0 \in s$.

- 65. a. Toon aan: voor elke s geldt $0 < -s$, $0 = s$ of $0 < s$.
- b. Toon aan: als $0 < s$ en $0 < t$ dan $0 < s + t$.
- c. Toon aan: $s < t$ dan en slechts dan als $0 < t - s$.

Als altijd: $s \leq t$ betekent 's < t of s = t'. Verder schrijven we $> = <^{-1}$ en $\geq = \leq^{-1}$.

Vermenigvuldiging is wat lastiger te definiëren; de definitie ligt voor de hand maar omdat producten van negatieve getallen positief kunnen worden moeten we een paar gevallen onderscheiden. Eerst voor niet-negatieve snedes: als $0 \leq s, t$ dan

$$s \cdot t = \{q \in \mathbb{Q} : q < 0\} \cup \{p \cdot q : 0 \leq p < s, 0 \leq q < t\}$$

- 66. a. Bewijs dat $s \cdot t$ weer een niet-negatieve snede is.
 b. Bewijs dat \cdot aan de gebruikelijke regels voldoet: associativiteit, commutativiteit, distributiviteit over $+$, neutraal element en het bestaan van inversen voor positieve sneden.

Breid de vermenigvuldiging uit over heel \mathbb{R} :

- als $s, t < 0$ dan $s \cdot t = (-s) \cdot (-t)$;
- als $s \geq 0$ en $t < 0$ dan $s \cdot t = -(s \cdot (-t))$.

- 67. a. Bewijs dat \mathbb{R} met deze optelling, vermenigvuldiging en ordening een volledig geordend lichaam is.
 b. Bepaal de rang van \mathbb{R} .

Een alternatieve constructie van \mathbb{R} is die door Cantor, gebaseerd op werk van Weierstraß en gestroomlijnd door Hausdorff.

Een rij $\langle q_n \rangle_n$ rationale getallen heet een *fundamenteaalrij* (en natuurlijk ook een Cauchy-rij) als het volgende geldt

$$(\forall a > 0)(\exists N \in \mathbb{N})(\forall m, n \geq N)(|q_m - q_n| < a)$$

hierbij is $|q| = \max\{-q, q\}$ de *absolute waarde* van het rationale getal q .

- 68. a. Toon aan: elke fundamenteaalrij is begrensd, er is een M zó dat $|q_n| \leq M$ voor alle n .
 b. Toon aan: als $\langle p_n \rangle_n$ en $\langle q_n \rangle_n$ fundamenteaalrijen zijn dan zijn $\langle p_n + q_n \rangle_n$ en $\langle p_n \cdot q_n \rangle_n$ het ook.

Noem twee fundamenteaalrijen $\mathbf{p} = \langle p_n \rangle_n$ en $\mathbf{q} = \langle q_n \rangle_n$ equivalent als

$$(\forall a > 0)(\exists N \in \mathbb{N})(\forall m \geq N)(|p_m - q_m| < a)$$

(dus als $\lim_n (p_n - q_n) = 0$). We schrijven $\mathbf{p} \sim \mathbf{q}$.

- 69. Toon aan: als $\mathbf{p} \sim \mathbf{p}'$ en $\mathbf{q} \sim \mathbf{q}'$ dan $\mathbf{p} + \mathbf{q} \sim \mathbf{p}' + \mathbf{q}'$ en $\mathbf{p} \cdot \mathbf{q} \sim \mathbf{p}' \cdot \mathbf{q}'$.

Cantor's definitie van \mathbb{R} is als de verzameling van alle \sim -equivalentieklassen van fundamenteaalrijen. Definieer optelling, vermenigvuldiging en ordening van klassen als volgt

- $[\mathbf{p}] + [\mathbf{q}] = [\mathbf{p} + \mathbf{q}]$,
- $[\mathbf{p}] \cdot [\mathbf{q}] = [\mathbf{p} \cdot \mathbf{q}]$,
- $[\mathbf{p}] < [\mathbf{q}]$ als er een $a > 0$ en $N \in \mathbb{N}$ bestaan zó dat $p_n + a < q_n$ voor $n \geq N$.

- 70. a. Bewijs dat ook deze versie van \mathbb{R} een volledig geordend lichaam is.
 b. Bepaal de rang van deze versie van \mathbb{R} .

Een paar onafhankelijkheidsresultaten

Laten zien dat een formule niet bewijsbaar is, uitgaande van andere formules, gaat met gebruik van de volledigheidstelling van Gödel.

Om aan te geven hoe zoiets in zijn werk gaat bekijken we de formule $(\forall x)(\forall y)(x * y = y * x)$ uit de taal van de groepen. Is deze af te leiden uit de drie basisaxioma's van de groepentheorie, dat wil zeggen, bestaat er een eindige rij van formules waarin elke formule een axioma is of volgt uit voorgaande formules door middel van afleidingsregels en zó dat de laatste formule $(\forall x)(\forall y)(x * y = y * x)$ is? Het nalopen van alle formele

bewijzen is geen optie want die vormen een oneindige verzameling. De makkelijke helft van de volledigheidstelling zegt dat het voldoende is een structuur te maken waarin de groepsaxioma's wel gelden (een groep dus) maar de gegeven formule niet. De moeilijke helft zegt dat dit ook nodig is: als er geen afleiding is kan men een structuur bouwen waarin de groepsaxioma's wel gelden en de formule in kwestie niet.

De groep S_3 doet wat wij willen, de groepsoperatie voldoet aan de groepsaxioma's en voor de elementen $x = (1\ 2)$ en $y = (2\ 3)$ geldt $x \circ y \neq y \circ x$.

Voor de verzamelingenleer geldt hetzelfde; als je van een formule wilt vaststellen dat deze uitgaande van andere niet bewijsbaar is moet je een structuur maken waarin $=$ en \in geïnterpreteerd worden, waarin de uitgangspunten wel gelden en waarin de onderhavige formule niet geldt.

Alleen de lege verzameling

We hebben al een structuur gezien waarin sommige axioma's wel gelden en andere niet: $\{\emptyset\}$, met $=$ als gelijkheid en \in zonder interpretatie. Hierin gelden axioma's 0, 1, 2 en 3 maar is geen x te vinden die voldoet aan $(\exists y)(y \in x)$.

Een niet-standaard interpretatie

Neem als 'universum' de verzameling \mathbb{Z} , interpreteer $=$ als gelijkheid en interpreteer \in met $<$. Dan geldt Axioma 0: het gehele getal 0 voldoet aan $x = x$. Ook geldt Axioma 1: als n en m voldoen aan $(\forall x)(x < n \leftrightarrow x < m)$ dan volgt $n = m$. Er is geen 'lege verzameling' want er geldt $(\forall n)(\exists m)(m < n)$. Dus Axioma 3 geldt niet.

- **71.** Ga na dat in deze structuur Axioma 2 ook niet geldt.

Relativering

In de bovenstaande voorbeelden bekeken we maar een paar axioma's en was duidelijk wat de formules binnen de structuren inhielden.

Voor de volgende voorbeelden is het van belang wat nauwkeuriger te weten hoe een formule binnen een structuur geïnterpreteerd wordt. We bekijken vooral verzamelingen waarin we $=$ en \in als 'is gelijk aan' en 'is element van' interpreteren. Zij M zo'n verzameling. We definiëren voor elke formule φ zijn *relativering* φ^M tot M als volgt.

- $(x \in y)^M$ is $x \in y$ en $(x = y)^M$ is $x = y$;
- $(\neg(\varphi))^M$ is $\neg(\varphi^M)$;
- $((\varphi) \wedge (\psi))^M$ is $(\varphi^M) \wedge (\psi^M)$; en
- $((\exists x)(\varphi))^M$ is $(\exists x \in M)(\varphi^M)$.

Met andere woorden: elke kwantor wordt begrensd door M .

Meestal, maar niet altijd, is M transitief; in dat geval is het extensionaliteitsaxioma automatisch waar in M .

- **72.** Laat M transitief zijn en $x \in M$.
- a. Toon aan: $(\exists y)(y \in x)$ dan en slechts dan als $(\exists y \in M)(y \in x)$
 - b. Bewijs: voor elke formule φ zonder kwantoren geldt $(\exists y \in x)(\varphi^M)$ dan en slechts dan als $((\exists y \in x)(\varphi))^M$.
- **73.** Zij M transitief. Bewijs: $((\forall x)(\forall y)((\forall z)(z \in x \leftrightarrow z \in y) \rightarrow x = y))^M$.

Ook regulariteit geldt in M :

- **74.** Zij M transitief. Bewijs: $((\forall x)((\exists y)(y \in x) \rightarrow (\exists y)(y \in x \wedge \neg(\exists z)(z \in x \wedge z \in y))))^M$

Het Vervangingsaxioma en het Oneindigheidsaxioma

Met behulp van de verzamelingen V_α kunnen we laten zien dat de Vervangings- en Oneindigheidsaxioma's ieder niet uit de rest der axioma's is af te leiden. De V_α , voor limietgetallen α , voldoen namelijk aan bijna alle axioma's. Zij dus, voorlopig, α een limietgetal.

- **75.** Toon aan: in V_α gelden de volgende axioma's:
- Axioma 0.
 - Axioma 1.
 - Axioma 2.
 - Axioma 3. *Hint:* De af te scheiden verzameling bestaat; laat zien dat deze tot V_α behoort.
 - Axioma 4. *Hint:* Opgave 59
 - Axioma 5. *Hint:* Opgave 59
 - Axioma 8. *Hint:* Opgave 59
 - Axioma 9. *Hint:* Opgave 59

Het Oneindigheidsaxioma is het makkelijkst onafhankelijk te praten. We nemen namelijk V_ω als universum.

- **76.** a. Toon aan: voor alle $n \in \omega$ geldt $|V_n| < \omega$.
b. Toon aan: $|V_\omega| = \omega$.
- **77.** Het Vervangingsschema geldt in V_ω . *Hint:* Na relativering wordt over V_ω gekwantificeerd; dus $A \in V_\omega$ en bij elke $x \in A$ zit de bijbehorende y ook in V_ω . Neem een geschikte V_m als de gezochte B .
- **78.** Het Oneindigheidsaxioma geldt niet in V_ω . *Hint:* ω is uniek en $\omega \notin V_\omega$.

Voor de onafhankelijkheid van het Vervangingsschema werken we in $V_{\omega+\omega}$.

- **79.** Het Oneindigheidsaxioma geldt in $V_{\omega+\omega}$.
Er is tenminste één formule waarvoor Vervanging in $V_{\omega+\omega}$ niet opgaat.
- **80.** Definieer \prec op ω door $m \prec n$ als 1) m even is en n oneven, of 2) $n + m$ even is en $m < n$.
- Toon aan: $\langle \omega, \prec \rangle$ is een welordening.
 - Toon aan: voor elke $n \in \omega$ is er één ordinaalgetal γ in $V_{\omega+\omega}$ zó dat $\text{vg}(\omega, n, \prec)$ isomorf is met γ .
 - Toon aan: er is geen ordinaalgetal β in $V_{\omega+\omega}$ zó dat $\langle \omega, \prec \rangle$ isomorf is met β .

Machtsverzameling

Om de onafhankelijkheid van het Machtsverzamelingsaxioma aan te tonen voeren voor elk kardinaalgetal κ de verzameling $H(\kappa)$ in

$$H(\kappa) = \{x : |\text{trcl } x| < \kappa\}$$

De verzameling van alle verzamelingen die 'erfelijk' kardinaliteit kleiner dan κ hebben. Twee speciale gevallen: $H(\aleph_0)$ is de verzameling van erfelijk eindige verzamelingen en $H(\aleph_1)$ is de verzameling van erfelijk aftelbare verzamelingen.

Binnen de $H(\kappa)$ gelden veel van onze axioma's.

- **81.** Zij κ een oneindig kardinaalgetal. Toon aan:
- $H(\kappa) \subseteq V_\kappa$.
 - $H(\kappa)$ is transitief.
 - $H(\kappa) \cap \mathbf{ON} = \kappa$.
 - Als $x \in H(\kappa)$ dan $\bigcup x \in H(\kappa)$.
 - Als $x, y \in H(\kappa)$ dan $\{x, y\} \in H(\kappa)$.
 - Als $x \in H(\kappa)$ en $y \subseteq x$ dan $y \in H(\kappa)$.
 - Voor elke x geldt $x \in H(\aleph_1)$ dan en slechts dan als $x \subseteq H(\aleph_1)$ en $|x| < \aleph_1$.
Hint: Opgave 54 en het Keuzeaxioma.

Met behulp van de laatste twee onderdelen volgt dat in $H(\aleph_1)$ de Afscheidings- en Vervangingsaxioma's gelden; het Oneindigheidsaxioma geldt omdat $\omega \in H(\aleph_1)$. Het Keuzeaxioma geldt ook binnen $H(\aleph_1)$: als $x \in H(\aleph_1)$ dan ook behoort $x \times \bigcup x$ tot $H(\aleph_1)$ en daarmee ook elke keuzefunctie voor x .

- **82.** Bewijs: in $H(\aleph_1)$ geldt dat elke verzameling aftelbaar is.

In $H(\aleph_1)$ geldt het machtsverzamelingsaxioma dus niet; merk op dat $\mathcal{P}(\omega) \subseteq H(\aleph_1)$, de machtsverzameling van ω is dus, wat $H(\aleph_1)$ betreft, een klasse die geen verzameling is.

- **83.** Bewijs: $H(\aleph_0) = V_\omega$.

Bijlage A

Kettingbreuken

Tussen de irrationale getallen en de rijen natuurlijke getallen (ongelijk aan 0) is een fraaie bijectie te maken.

Van rij naar getal

Gegeven een rij (a_1, a_2, a_3, \dots) maken we een irrationaal getal a , als volgt:

$$a = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots}}}} \quad (\dagger)$$

Dit moeten we als volgt lezen: we maken een rij rationale getallen

$$\frac{1}{a_1}, \frac{1}{a_1 + \frac{1}{a_2}}, \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}}, \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4}}}}, \dots \quad (\ddagger)$$

Deze rij convergeert naar een irrationaal getal in het interval $(0, 1)$.

Van getal naar rij

Omgekeerd, gegeven een getal a in het interval $(0, 1)$ maken we een rij (a_1, a_2, a_3, \dots) van natuurlijke getallen door het algoritme van Euclides op 1 en a toe te passen:

$$\begin{aligned} 1 &= a_1 \cdot a + r_1 \\ a &= a_2 \cdot r_1 + r_2 \\ r_1 &= a_3 \cdot r_2 + r_3 \\ &\dots \\ r_{i-1} &= a_{i+1} \cdot r_i + r_{i+1} \\ &\dots \end{aligned}$$

Hierbij zorgen we er telkens voor dat $0 \leq r_{i+1} < r_i$, net als bij gewoon delen met rest.

Bijvoorbeeld, als $a = \frac{1}{2}\sqrt{2}$ vinden we achtereenvolgens: $1 = 1 \cdot \frac{1}{2}\sqrt{2} + (1 - \frac{1}{2}\sqrt{2})$, $\frac{1}{2}\sqrt{2} = 2 \cdot (1 - \frac{1}{2}\sqrt{2}) + (\frac{3}{2}\sqrt{2} - 2)$, $1 - \frac{1}{2}\sqrt{2} = 2 \cdot (\frac{3}{2}\sqrt{2} - 2) + (5 - \frac{7}{2}\sqrt{2})$, $\frac{3}{2}\sqrt{2} - 2 = 2 \cdot (5 - \frac{7}{2}\sqrt{2}) + (\frac{17}{2}\sqrt{2} - 12)$, ...

► 1. Dit proces stopt na eindig veel stappen dan en slechts dan als a een *rationaal* getal is.

Dus elk irrationaal getal bepaalt een oneindige rij natuurlijke getallen. Rest nog te bewijzen dat de twee hierboven beschreven processen elkaars inversen zijn.

Het is een bijectie

We hanteren de gebruikelijke schrijfwijze voor kettingbreuken: het rechterlid van (†) noteren we $[a_1, a_2, a_3, \dots]$ en de termen van de rij (‡) als $[a_1]$, $[a_1, a_2]$, $[a_1, a_2, a_3]$, $[a_1, a_2, a_3, a_4]$, \dots

Voor de tellers en noemers van de partiële kettingbreuken bestaat een mooie recursieformule: Zet eerst $p_{-1} = 1$, $q_{-1} = 0$, $p_0 = 0$ en $q_0 = 1$ en definieer p_n en q_n voor $n \geq 1$ als volgt:

$$\begin{aligned} p_n &= a_n \cdot p_{n-1} + p_{n-2} \\ q_n &= a_n \cdot q_{n-1} + q_{n-2} \end{aligned} \quad (*)$$

- **2.** a. Toon aan: $[a_1] = \frac{p_1}{q_1}$
 b. Toon aan: $[a_1, a_2] = \frac{p_2}{q_2}$
 c. Toon aan: $[a_1, a_2, a_3] = \frac{p_3}{q_3}$
- **3.** Bewijs: voor alle $n \in \mathbb{N}$ geldt $[a_1, a_2, \dots, a_n] = \frac{p_n}{q_n}$. *Hint:* Inductie; bewijs eerst dat (ook voor reële $x > 0$) $[a_1, a_2, \dots, a_{n-1}, x] = \frac{x \cdot p_{n-1} + p_{n-2}}{x \cdot q_{n-1} + q_{n-2}}$ en vul dan een geschikte waarde voor x in.
- **4.** a. Bewijs: $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$.
 b. Toon aan: $\text{ggd}(p_n, q_n) = 1$.
- **5.** a. Toon aan: $q_n \geq F_n$, waarbij F_n het n de Fibonacci-getal is.
 b. Toon aan:

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$$

c. Toon aan:

$$[a_1, a_2, \dots, a_n] = \sum_{k=1}^n \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

- d. Toon aan: $\lim_{n \rightarrow \infty} [a_1, a_2, \dots, a_n]$ bestaat. *Hint:* De reeks in het vorige onderdeel is absoluut convergent.
 e. Bewijs: als de rijen (a_1, a_2, a_3, \dots) en (b_1, b_2, b_3, \dots) verschillen dan verschillen de limieten ook. *Hint:* Neem de eerste index n met $a_n \neq b_n$ en schat de sommen van de staarten van de reeksen af.

De afbeelding $(a_1, a_2, a_3, \dots) \mapsto a$ is dus injectief. Voor de surjectiviteit nemen we aan dat $a \in (0, 1)$ irrationaal is en dat de rij (a_1, a_2, a_3, \dots) het resultaat is van het toepassen van het algoritme van Euclides op 1 en a .

- **6.** a. Bewijs: $[a_1, a_2, \dots, a_n] > a$ als n oneven is.
 b. Bewijs: $[a_1, a_2, \dots, a_n] < a$ als n even is.
 c. Bewijs: $a = \lim_{n \rightarrow \infty} [a_1, a_2, \dots, a_n]$.

Het is een homeomorfisme

De hierboven gevonden afbeelding heeft nog meer mooie eigenschappen. We noemen er een. De beide verzamelingen dragen elk een natuurlijke topologie: $\mathbb{N}^{\mathbb{N}}$ heeft de producttopologie, waarbij \mathbb{N} de discrete topologie draagt en de irrationale getallen in $(0, 1)$ beschouwen we als deelruimte van \mathbb{R} met de gewone topologie.

- 7. Bewijs: de afbeelding $(a_1, a_2, a_3, \dots) \mapsto a$ is een homeomorfisme.

Verdere opmerkingen

Er is nog veel meer over kettingbreuken te vertellen; twee eenvoudige dingen staan hieronder.

Als van een getal de decimale ontwikkeling vanaf zekere index periodiek is dan is dat getal rationaal; voor kettingbreuken kun je periodiciteit ook karakteriseren.

- 8. De rij $(a_1, a_2, a_3, \dots, a_n, \dots)$ is op den duur periodiek dan en slechts dan als het getal a een oplossing is van een kwadratische vergelijking met gehele coëfficiënten. *Hint*: Probeer eerst eens een eenvoudig geval: $(1, 1, 1, 1, \dots)$ bijvoorbeeld.

De partiële kettingbreuken, de *convergenten* van de kettingbreuk, geven, in zekere zin, optimale benaderingen van a .

- 9. Toon aan: $|a - \frac{p_n}{q_n}| < q_n^{-2}$ (de notatie als in (*)).

Enige Logica

De mathematische logica is, zeer kort gezegd, de wiskunde van het redeneren en het bewijzen. Deze appendix geeft slechts een korte inleiding. Voor een uitgebreide behandeling wordt verwezen naar het college *Logica* aan de TU Delft en het bij die cursus gebruikte boek [2010] van Mendelson.

Propositielogica

De Propositielogica vertelt ons hoe we met ‘niet’, ‘en’, ‘of’, ‘impliceert’ en ‘dan en slechts dan’ kunnen rekenen. Dat rekenen gebeurt aan de hand van de volgende tabellen.

p	$\neg p$
1	0
0	1

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Deze tabellen geven aan wat de waarheidswaarde (0 is ‘onwaar’, 1 is ‘waar’) van een samengestelde bewering is als van de deelbewering de waarheidswaarde al is vastgesteld. De kolommen spreken redelijk voor zich: $\neg p$ is waar dan en slechts dan als p onwaar is; $p \wedge q$ is waar alléén als p en q beide waar zijn enzovoorts. Op deze manier kan van steeds ingewikkelder samenstellingen de mogelijke waarheidswaarden bepaald worden, afhankelijk van de waarheidswaarde van de ‘atomaire’ beweringen p, q, \dots

Belangrijk zijn de *tautologieën*, dat zijn samenstellingen/formules die altijd waarheidswaarde 1 hebben.

- 1. Ga na dat de volgende beweringen tautologieën zijn
- $p \rightarrow (q \rightarrow p)$
 - $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$
 - $(\neg q \rightarrow \neg p) \rightarrow ((\neg q \rightarrow p) \rightarrow q)$

Merk op dat indien we in bovenstaande opgave voor p, q en r willekeurige formules invullen we weer tautologieën krijgen.

Logisch gevolg en consistentie

Een redenering heeft meestal de volgende vorm: uit uitspraken F_1, \dots, F_n, \dots volgt uitspraak G . Als we naar de tabel voor \rightarrow kijken komt dit neer op: telkens als F_1, \dots, F_n, \dots waarheidswaarde 1 hebben heeft ook G waarheidswaarde 1. We voeren de notatie $\mathcal{F} \models G$ in om dit af te korten en we zeggen ook wel dat G een *logisch gevolg* van \mathcal{F} is.

De uitspraak $\mathcal{F} \models G$ heeft natuurlijk alleen inhoud als er waarheidstoekenningen zijn die alle $F \in \mathcal{F}$ waarheidswaarde 1 geven (de kolom van \rightarrow laat zien dat uit iets dat toch nooit waar is alles volgt). We noemen \mathcal{F} *consistent* als er ten minste één waarheidstoekenning is die alle $F \in \mathcal{F}$ waar maakt.

- 2. Ga na dat \mathcal{F} consistent is dan en slechts dan als $\mathcal{F} \not\models (p \wedge \neg p)$.

Een niet-triviale stelling over dit begrip is de volgende.

B.1. STELLING (Compactheidsstelling). *Een verzameling formules is consistent dan en slechts dan als elke eindige deelverzameling consistent is.*

BEWIJS. Eén richting is duidelijk. Voor de lastige richting nemen we aan dat elke eindige deelverzameling van een verzameling \mathcal{F} van formules consistent is. Zij P de verzameling van alle atomaire proposities en bekijk de verzameling $W = \{0, 1\}^P$ van alle waarheidstoekenningen; deze draagt, wegens de Stelling van Tychonoff, een compacte topologie: de producttopologie, waarbij we $\{0, 1\}$ discreet veronderstellen.

Voor elke $F \in \mathcal{F}$ schrijven we $W_F = \{x \in W : x \text{ maakt } F \text{ waar}\}$. Het complement van W_F is open: als $x \notin W_F$ en y neemt op de eindig veel atomaire proposities uit F dezelfde waarden aan als x dan is F onder de toekenning y ook onwaar. Dus elke W_F is gesloten.

Dat elke eindige deelverzameling van \mathcal{F} consistent is betekent dat de familie $\{W_F : F \in \mathcal{F}\}$ de eindige doorsnede eigenschap heeft. Wegens de compactheid van W volgt nu dat $\bigcap \{W_F : F \in \mathcal{F}\}$ niet leeg is; elke x in die doorsnede is als gewenst. \square

- 3. Toon aan dat het omgekeerde uit het bovenstaande bewijs ook geldt: de Compactheidsstelling impliceert de Stelling van Tychonoff.

De compactheidsstelling wordt ook wel als volgt geformuleerd.

B.2. STELLING. *Er geldt $\mathcal{F} \models G$ dan en slechts dan als er een eindige deelverzameling \mathcal{F}' van \mathcal{F} is met $\mathcal{F}' \models G$.*

- 4. Bewijs dat dit inderdaad een herformulering van de Compactheidsstelling is. *Hint: $\mathcal{F} \models G$ is equivalent met " $\mathcal{F} \cup \{\neg G\}$ is niet consistent".*

Afleidingen

Een formule kan ook op een andere manier als gevolg van een verzameling formules gezien worden.

Een *afleiding* van een formule G uit een verzameling formules \mathcal{F} is een rij formules F_1, F_2, \dots, F_n waarbij $F_n = G$ en elke F_k een formule is zó dat

- deze in \mathcal{F} zit, of
- deze een tautologie is, of
- er twee eerdere formules F_i en F_j zijn met F_i gelijk aan $F_j \rightarrow F_k$

De laatste regel is een afleidingsregel, *Modus Ponens* geheten, die iets uit de rede-nerpraktijk formaliseert: als we F_j en $F_j \rightarrow F_k$ hebben bewezen mogen we ook F_k concluderen.

Het bestaan van een afleiding van G uit \mathcal{F} wordt als volgt uitgedrukt: $\mathcal{F} \vdash G$.

In het boek van Mendelson wordt, in eerste instantie, het tweede punt in de definitie van afleiding afgezwakt tot: F_k is een versie van één van de uitdrukkingen uit Opgave 1. Daarna wordt bewezen dat elke tautologie afleidbaar is.

De volledigheidstelling uit de Logica zegt dat ‘logisch gevolg van’ en ‘afleidbaar uit’ equivalent zijn.

B.3. STELLING (Volledigheidstelling). *Er geldt $\mathcal{F} \vdash G$ dan en slechts dan als $\mathcal{F} \models G$.*

Merk op dat de Compactheidsstelling hier een eenvoudig gevolg van is: Uit de definitie van afleiding volgt immers meteen dat $\mathcal{F} \vdash G$ dan en slechts dan als $\mathcal{F}' \vdash G$ voor een eindige deelverzameling \mathcal{F}' van \mathcal{F} . Dit geeft aan dat het bewijs van de Volledigheidstelling niet geheel triviaal is.

Eerste-orde Logica

In de verzamelingenleer werken we ook met kwantoren en de relaties = en \in . De eerste-orde logica breidt de propositielogica uit met juist dat gereedschap.

Taal

De taal van een eerste-orde theorie bestaat uit haakjes, de kwantoren, de logische connectieven, variabelen, relatiesymbolen (van in principe willekeurige ariteit), constanten en functiesymbolen (ook van willekeurig veel variabelen). Hiermee worden op de gangbare manier formules uit gemaakt.

- De taal van de verzamelingenleer heeft \in en = als relatiesymbolen.
- De taal van de groepentheorie heeft een binair functiesymbool f en = als relatiesymbool.

Theorieën

Een theorie heeft in het algemeen drie soorten axioma's.

Logische axioma's. Om te beginnen zijn er de zuiver logische axioma's; dit zijn alle mogelijke *generalisaties* van formules van de volgende vorm:

- Tautologieën.
- $(\forall x)(\varphi(x)) \rightarrow \varphi(t)$ als t voor x ingevuld kan worden
- $(\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)(\psi))$ mits x niet vrij voorkomt in φ

Een generalisatie van een formule ϕ is een formule van de vorm $(\forall x)(\phi)$; in bovenstaande lijst mag willekeurig vaak een universele kwantor voor geplaatst worden. Dit weerspiegelt het idee dat een formule die voor een ‘willekeurige’ x waar is ook voor alle x waar is.

Axioma's voor gelijkheid. Als de taal het symbool = bevat gebruiken we de generalisaties van de volgende twee formules om het (gewenste) gedrag van = te formaliseren.

- $x = x$
- $x = y \rightarrow (\psi \rightarrow \psi')$ waar ψ' uit ψ ontstaat door 0 of meer x -en door y -en te vervangen

Specifieke axioma's. Dit zijn de uitgangspunten van de theorie die men op wil bouwen. Zo is de theorie van de groepen een eerste-orde theorie met gelijkheid, met een binair functiesymbool f en met als specifieke axioma's de generalisaties van

- $f(x, f(y, z)) = f(f(x, y), z)$
- $(\exists e)((\forall x)(f(x, e) = f(e, x)) \wedge (\forall x)(\exists y)(f(x, y) = e \wedge f(y, x) = e))$

Dit is een eindige lijst; de lijst van axioma's van ZFC is, dankzij Afscheiding en Vervanging, oneindig lang.

Afleidingen

Een afleiding in de eerste-orde logica is gedefinieerd als in de propositielogica met, natuurlijk, als uitbreiding dat in de rij nu ook de nieuwe logische axioma's, de axioma's voor gelijkheid (eventueel) en de specifieke axioma's gebruikt kunnen worden. Verder is er nog een extra afleidingsregel: als φ afgeleid is kunnen we ook $(\forall x_i)(\varphi)$ afleiden (voor elke variabele x_i), wat weerspiegelt dat iets dat voor een 'willekeurige' x bewezen is in feite voor *alle* x bewezen is.

De *stellingen* van de theorie zijn de formules die in een (correcte) afleiding voorkomen. Van de resultaten in Hoofdstuk 2 kan, met veel moeite, aangetoond worden dat het inderdaad stellingen van de theorie ZFC zijn.

De notatie $\mathcal{F} \vdash G$ houdt zijn betekenis; die van $\mathcal{F} \models G$ moet aangepast worden.

Structuren

Een *structuur* voor een taal bestaat uit een verzameling X met daarbij voor elk relatiesymbool een relatie op X (van de juiste ariteit), voor elke constante een aangewezen element van X en voor elk (n -air) functiesymbool een functie van X^n naar X . Als het symbool $=$ in de taal voorkomt kiezen we daarbij altijd de gelijkheidsrelatie op X .

Een structuur voor de taal van de groepen bestaat dus uit een verzameling G en een functie $f : G^2 \rightarrow G$. Als die G en f ook nog aan de groepsaxioma's voldoen noemen we de structuur een model voor de groepentheorie, een groep dus.

Volledigheid en compactheid

Ook de eerste-orde logica kent een volledigheidstelling.

Hierbij wordt $\mathcal{F} \models G$ als volgt gedefinieerd: "in elke structuur waarin de formules uit \mathcal{F} waar zijn is G ook waar".

B.4. STELLING (Volledigheidstelling). *Er geldt $\mathcal{F} \vdash G$ dan en slechts dan als $\mathcal{F} \models G$.*

In het geval van de groepentheorie zegt dit: iets is af te leiden uit de axioma's van de groepentheorie dan en slechts dan als het waar is in *elke* groep. Dit is niet het intrappen van een open deur; als je van een formule weet dat hij in elke groep geldig is kan dat zijn doordat je het alleen maar gezien hebt. Wat de stelling zegt is dat er dan, noodzakelijk, een afleiding van die formule uit de groepsaxioma's moet bestaan.

Wat de stelling ook zegt is dat om te laten zien dat G *niet* uit \mathcal{F} afgeleid kan worden het voldoende is één structuur aan te geven waarin de formules uit \mathcal{F} wel gelden maar G niet.

De groep S_3 is een structuur waarin de groepsaxioma's gelden, als we f interpreteren door $f(x, y) = x \circ y$, maar de formule $(\forall x)(\forall y)(f(x, y) = f(y, x))$ niet; deze is dus niet uit de groepsaxioma's af te leiden.

Dezelfde uitspraken gelden dus ook voor de theorie ZFC; het probleem daarbij is dat we wegens Gödel's *Onvolledigheidsstellingen* niet binnen ZFC kunnen bewijzen dat ZFC modellen heeft. Hoe we dan toch kunnen bewijzen dat noch de Continuum Hypothese noch zijn negatie uit ZFC af te leiden is, bijvoorbeeld, te lezen in het boek van Kunen [1980].

Bibliografie

- CANTOR, G.
- [1874] Über eine eigenschaft des inbegriffes aller reellen algebraischen zahlen. *Crelles Journal für Mathematik*, **77**, 258–262. Cantor's bewijs dat \mathbb{R} overaftelbaar is. Ook in CANTOR [1980, p. 115–118].
 - [1878] Ein Beitrag zur Mannigfaltigkeitslehre. *Crelles Journal für Mathematik*, **84**, 242–258. Cantor's bewijs dat \mathbb{R} en \mathbb{R}^n gelijkmachtig zijn. Ook in CANTOR [1980, p. 119–133].
 - [1879] Über unendliche lineare Punktmannigfaltigkeiten. Nr. 1. *Mathematische Annalen*, **15**, 1–7. Ook in CANTOR [1980, p. 165–209].
 - [1880] Über unendliche lineare Punktmannigfaltigkeiten. Nr. 2. *Mathematische Annalen*, **17**, 355–358. Ook in CANTOR [1980, p. 165–209].
 - [1882] Über unendliche lineare Punktmannigfaltigkeiten. Nr. 3. *Mathematische Annalen*, **20**, 113–121. Ook in CANTOR [1980, p. 165–209].
 - [1883a] Über unendliche lineare Punktmannigfaltigkeiten. Nr. 4. *Mathematische Annalen*, **21**, 51–58. Ook in CANTOR [1980, p. 165–209].
 - [1883b] Über unendliche lineare Punktmannigfaltigkeiten. Nr. 5. *Mathematische Annalen*, **21**, 545–586. Ook in CANTOR [1980, p. 165–209].
 - [1884] Über unendliche lineare Punktmannigfaltigkeiten. Nr. 6. *Mathematische Annalen*, **23**, 453–488. Ook in CANTOR [1980, p. 165–209].
 - [1890] Über eine elementare Frage der Mannigfaltigkeitslehre. *Jahresbericht der Deutschen Mathematischen Vereinigung*, **I**, 75–78. Het diagonaalargument. Ook in CANTOR [1980, p. 278–281].
 - [1895] Beiträge zur Begründung der transfiniten Mengenlehre (Erster Artikel). *Mathematische Annalen*, **46**, 481–512. Ook in CANTOR [1980, p. 282–311].
 - [1897] Beiträge zur Begründung der transfiniten Mengenlehre (Zweiter Artikel). *Mathematische Annalen*, **49**, 207–246. Ook in CANTOR [1980, p. 312–351].
 - [1980] *Gesammelte Abhandlungen mathematischen und philosophischen Inhalts*. Springer-Verlag, Berlin. Herdruk van de uitgave uit 1932, geredigeerd door Ernst Zermelo.
- DAUBEN, J. W.
- [1979] *Georg Cantor. His mathematics and philosophy of the infinite*. Harvard University Press, Cambridge, Mass.
- DEDEKIND, R.
- [1932] Ähnliche (deutliche) Abbildung and ähnliche Systeme, 1887.7.11. In *Gesammelte mathematische Werke (Dritter Band)*, R. Fricke, E. Noether, and Ö. Ore, editors, p. 447–449. Vieweg, Braunschweig.
- FRAENKEL, A. A.
- [1922] Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre. *Mathematische Annalen*, **86**, 230–237.
- GOODSTEIN, R. L.
- [1944] On the restricted ordinal theorem. *The Journal of Symbolic Logic*, **9**, 33–41.
- HARTOGS, F.
- [1915] Über das Problem der Wohlordnung. *Mathematische Annalen*, **76**, 438–443.

JECH, T.

- [2003] *Set theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin. The third millennium edition, revised and expanded.

KIRBY, L. and J. PARIS.

- [1982] Accessible independence results for Peano arithmetic. *The Bulletin of the London Mathematical Society*, **14**(4), 285–293.

KÖNIG, J.

- [1905] Zum Kontinuumproblem. *Mathematische Annalen*, **60**, 177–180.

KUNEN, K.

- [1980] *Set theory. An introduction to independence proofs*, Studies in Logic and the Foundations of Mathematics 102. Studies in Logic and the Foundations of Mathematics. North-Holland Publishing Co., Amsterdam.

MENDELSON, E.

- [2010] *Introduction to mathematical logic*. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, fifth edition.

ZERMELO, E.

- [1904] Beweis, daß jede Menge wohlgeordnet werden kann. *Mathematische Annalen*, **59**, 514–516.
- [1908a] Neuer Beweis für die Möglichkeit einer Wohlordnung. *Mathematische Annalen*, **65**, 107–128.
- [1908b] Untersuchungen über die Grundlagen der Mengenlehre I. *Mathematische Annalen*, **65**, 261–281.

ZORN, M.

- [1935] A remark on method in transfinite algebra. *Bulletin of the American Mathematical Society*, **41**, 667–670.

Index

- \aleph_0 , 14, 42
- \aleph_α , 42
- $\aleph(X)$, Hartogs' aleph, 42
- \forall , 28
- \vdash , 56
- \circ , 34
- \mathfrak{c} , continuum, 14
- \subseteq , 31
- \leftrightarrow , 28
- \bigcap , 32
- \cap , 31
- \in , 27
- \wedge , 27
- $M \sim N$, 12
- \exists , 27
- $\exists!$, 33
- η , ordetype van \mathbb{Q} , 16
- $=$, 27
- $H(\kappa)$, 50
- \rightarrow , 28
- $|M|$, machtigheid, 12
- \overline{M} , 11
- \emptyset , 31
- \models , 55, 58
- \setminus , 31
- \mathbb{N} , 46
- \neg , 27
- \notin , 28
- \neq , 28
- \vee , 28
- ω , 6, 16, 37
- ω_0 , 42
- ω_1 , 21
- ω_α , 42
- ON**, 38
- P , de irrationale getallen, 3
- $\mathcal{P}(x)$, 41
- \mathbb{Q} , 47
- \mathbb{R} , 47
- θ , ordetype van $[0, 1]$, 16
- $\text{trcl } X$, 46
- V**, 38
- V_α , 45
- \bigcup , 33
- \cup , 33
- \triangleleft , welorde van **ON** \times **ON**, 41
- \mathbb{Z} , 46
- afbeelding, 34
- afgeleide verzameling, 4
- afleiding, 56
- afleidingsregel, 56
- aftelbare verzameling, 40
- algebraïsch getal, 1
- anti-symmetrische relatie, 35
- axioma
 - afscheiding, 29, 31
 - bestaan, 29, 30
 - extensionaliteit, 29, 30
 - Keuzeaxioma, 30, 42
 - machtsverzameling, 30, 41
 - oneindigheid, 30, 36
 - paarvorming, 29, 32
 - regulariteit, 29, 45
 - vereniging, 29, 33
 - vervanging, 30, 33
- axioma's van Peano, 37
- back-and-forth argument, 10
- beginstuk, 18
- begrensde kwantor, 29
- bereik van een relatie, 34
- bijjectieve functie, 34
- \mathfrak{c} , continuum, 14
- G. Cantor
 - beschrijving van de Cantorverzameling, 6
 - definitie van equivalentie, 11
 - definitie van kardinaalgetal, 11
 - definitie van machtigheid, 11
 - definitie van ordetype, 16
 - definitie van verzameling, 11
 - diagonaalargument, 7
 - formulering van Continuum Hypothese, 4
 - gelijkmachtigheid van \mathbb{R} en \mathbb{R}^n , 2
 - overaftelbaarheid van \mathbb{R} , 1
 - \mathbb{Q} is uniek, 9
- Cantor-normaalvorm voor ordinaalgetallen, 24
- Cantorverzameling, 6
- Cartesisch product, 15
- Cauchy-rij, 48
- consistent, 56
- Continuum Hypothese, 4
- Dedekind-snede, 47
- diagonaalargument, 7, 15
- domein van een relatie, 34

- doorsnede
 - familie, 32
 - twee verzamelingen, 31
- eindige verzameling, 37, 40
- ε -getal, 24
- equivalente verzamelingen, 12
- formule, 27, 28
 - generalisatie, 57
 - relativering, 49
- functie, 34
 - bijjectief, 34
 - injectief, 34
 - surjectief, 34
- fundamenteelrij, 48
- gebied, 5
- gebonden variabele, 28
- generalisatie van een formule, 57
- geordend paar, 32
- geordende som, 20
- getal
 - algebraïsch, 1
 - irrationaal, 2
- Goodstein-rij, 24–25
- heen-en-weerargument, 10
- hoogte van een polynoom, 1
- Inductieprincipe, 18, 38
- injectieve functie, 34
- inverse relatie, 34
- irrationaal getal, 2
- irreflexieve relatie, 35
- isomorfie van lineair geordende verzamelingen, 16
- kanonieke welgeordende verzameling, 20
- kardinaalgetal
 - definitie, 39
- kardinaalgetal van een verzameling, 11
- kardinaalgetallen
 - machtsverheffen, 14
 - optellen, 13, 40
 - vergelijken, 12
 - vermenigvuldigen, 14, 40
- kettingbreak, 2, 52–54
- Keuzeaxioma, 30, 42
- klasse, 38
- kwantor
 - \forall , 28
 - \exists , 27
 - $\exists!$, 33
 - begrensd, 29
- limietgetal, 21
- lineaire ordening, 16, 35
- logisch gevolg, 55
- machtigheid van een verzameling, 11
- machtsverheffing van kardinaalgetallen, 14
- machtsverheffing van ordinaalgetallen, 23
- machtsverzameling, 41
- Modus Ponens, 56
- natuurlijk getal, 36
- normaalvorm voor ordinaalgetallen, 24
- oneindige verzameling, 40
- ongeordend paar, 32
- optelling van kardinaalgetallen, 13, 40
- optelling van ordetypen, 16
- optelling van ordinaalgetallen, 22
- opvolger, 21
- ordetype, 15
 - omgekeerde, 16
- ordetypen
 - optellen, 16
 - vergelijken, 16
 - vermenigvuldigen, 17
- ordinaalgetal, 4
 - à la Cantor, 19
 - definitie, 21, 35
 - limietgetal, 21
 - opvolger, 21
 - overaftelbaar, 21
- ordinaalgetallen
 - machtsverheffen, 23
 - optellen, 22
 - vermenigvuldigen, 23
- overaftelbare verzameling, 40
- paar
 - geordend, 32
 - ongeordend, 32
- paradox
 - Burali-Forti, 25
 - Cantor, 25
 - Russell, 25
- partiële ordening, 35
- Peano
 - axioma's van, 37
 - definitie van functie, 34
 - definitie van relatie, 34
- perfecte verzameling, 6
- Pressing-Down Lemma, 22
- productverzameling, 33
- Recursieprincipe, 18, 20, 38

- reflexieve relatie, 35
- relatie, 34
 - anti-symmetrisch, 35
 - bereik, 34
 - domein, 34
 - inverse, 34
 - irreflexief, 35
 - reflexief, 35
 - samenstelling, 34
 - symmetrisch, 35
 - transitief, 35
- relativering van een formule, 49
- samenstelling van relaties, 34
- snede van Dedekind, 47
- stelling, 58
 - Cantor-Bernstein, 13
 - Goodstein, 25
 - Inductieprincipe, 18, 38
 - van König, 15
 - Pressing-Down Lemma, 22
 - Recursieprincipe, 18, 38
 - Schroeder-Bernstein, 13
 - Lemma van Teichmüller en Tukey, 43
 - Welordeningsstelling, 42
 - Lemma van Zorn, 43
- surjectieve functie, 34
- symmetrische relatie, 35
- tautologie, 55
- totale ordening, 35
- transitieve afsluiting, 45
- transitieve relatie, 35
- transitieve verzameling, 20, 21, 35
- uniciteit van \mathbb{Q} , 9
- variabele, 27
 - gebonden, 28
 - vrij, 28
- verdichtingspunt, 4
- vereniging
 - familie, 33
 - twee verzamelingen, 33
- vergelijken van kardinaalgetallen, 12
- vergelijken van ordetypen, 16
- vermenigvuldiging van kardinaalgetallen, 14, 40
- vermenigvuldiging van ordetypen, 17
- vermenigvuldiging van ordinaalgetallen, 23
- verschil, 31
- verzameling
 - afgeleide, 4
 - aftelbaar, 40
 - Cantorverzameling, 6
 - van de eerste soort, 4
 - eindig, 37, 40
 - kardinaalgetal, 11
 - lineair geordend, 16, 35
 - machtigheid, 11
 - machtsverzameling, 41
 - oneindig, 40
 - overaftelbaar, 40
 - overal dicht, 4
 - partieel geordend, 35
 - perfect, 6
 - product-, 33
 - samenhangend, 5
 - totaal geordend, 35
 - transitief, 20, 21, 35
 - van de tweede soort, 4
 - welgeordend, 18, 35
- verzamelingen
 - Cartesisch product, 15
 - equivalent, 12
 - vrije variabele, 28
- welgeordende verzameling, 18
 - beginstuk, 18
 - kanoniek, 20
- welgevormde formule, 28
- welordening, 18, 35
- Z, 30
- ZF, 30
- ZFC, 30