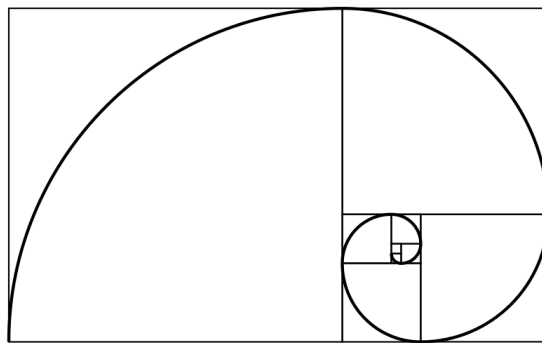


Inleiding in de Wiskunde

S. A. Terwijn



Afdeling Wiskunde
Radboud Universiteit Nijmegen
2014

Institute for Mathematics, Astrophysics, and Particle Physics
Radboud Universiteit Nijmegen
Heyendaalseweg 135
6525 AJ Nijmegen
`terwijn@math.ru.nl`

Méphistophélès:

Vraiment pour un docteur, la demande est frivole!

Je suis l'esprit de vie, et c'est moi qui console.

Je te donnerai tout, le bonheur, le plaisir,

Tout ce que peut rêver le plus ardent désir!

Faust:

Eh bien! pauvre démon, fais-moi voir tes merveilles!

(Uit: Berlioz, La Damnation de Faust, deel II, scène V)

Voorwoord

Deze syllabus behandelt een aantal elementaire onderwerpen die voor een verdere studie van de wiskunde onontbeerlijk zijn, en die dienen als voorkennis voor vrijwel alle andere wiskundevakken. Behandeld worden onderwerpen als formele taal, verzamelingen, functies en relaties, de diverse getallenstelsels, inductie, ordeningen, en kardinaliteit. De behandeling van deze onderwerpen is voornamelijk informeel, dat wil zeggen, niet-axiomatisch, met het idee dat de student eerst een zekere hoeveelheid omgang met de wiskunde moet hebben gehad om een latere strengere behandeling goed te kunnen appreciëren. Zo is bijvoorbeeld de gebruikelijke gang van zaken in de analyse dat de student eerst leert differentiëren en integreren, alvorens geconfronteerd te worden met een axiomatische behandeling van de reële getallen. Een nadere behandeling van de opbouw der wiskunde volgt dan onder andere in het tweedejaarscollege Logica.

Bij het schrijven van deze syllabus hebben we onder andere gebruik gemaakt van de syllabus “Inleiding in de Wiskunde en Verzamelingenleer” van H. C. Doets en A. S. Troelstra [5]. Tevens hebben we enkele voorbeelden ontleend aan de syllabus “Basiswiskunde” van G. van der Geer [7].

Elke hoofdstuk eindigt met een sectie opgaven. Sommige opgaven zijn gemarkeerd met een * om aan te geven dat ze van een hogere moeilijkheidsgraad zijn.

Ik ben dank verschuldigd aan een aantal van mijn collega's voor opmerkingen en aanvullingen bij eerdere versies van deze syllabus. Uiteraard komen de overgebleven tekortkomingen geheel voor rekening van de auteur.

Inhoudsopgave

Voorwoord	1
1 De Taal der Wiskunde	3
1.1 Propositielogica	3
1.2 Kwantoren	6
1.3 Bewijzen	6
2 Verzamelingen	10
2.1 Operaties op verzamelingen	10
2.2 Het cartesisch product	11
2.3 Verzamelingenalgebra	12
3 Functies en Relaties	15
3.1 Relaties	15
3.2 Functies	16
3.3 Equivalentierelaties	17
3.4 Functieverzamelingen	19
3.5 Ordeningen	20
4 Getallen	24
4.1 Getallenstelsels	24
4.2 De gehele getallen	25
4.3 De rationale getallen	26
4.4 De reële getallen	26
4.5 De complexe getallen	27
5 Inductie	30
5.1 Volledige inductie	30
5.2 Binomiaalcoëfficiënten	31
5.3 Formule-inductie	33
5.4 Recursie	34
6 Kardinaliteit	38
6.1 Gelijkmachtigheid	38
6.2 Aftelbare verzamelingen	39
6.3 Overaftelbare verzamelingen	40
6.4 Axiomatische verzamelingenleer	43
Bibliografie	46
Index	46

Hoofdstuk 1

De Taal der Wiskunde

But even if all murderers smile, it must not be inferred that all who smile are murderers. The world is gloomy enough already, and there is no need to employ bad logic to make it worse.

B. Russell, *Mortals and Others*, p112.

1.1 Propositielogica

Natuurlijke taal, zoals het Nederlands, bevat vaak dubbelzinnigheden, en leent zich ook niet altijd even goed om wiskunde beknopt in op te schrijven. (De lezer stelle zich een staartdeling voor, in woorden uitgeschreven.) Om spraakverwarring te vermijden, of om dingen beknopt te noteren, gebruiken wiskundigen vaak formele taal. Om te beginnen is er notatie voor wiskundige uitspraken, *propositions* genaamd. Met behulp van de connectieven $\neg$ (“niet”), $\wedge$ (“en”), $\vee$ (“of”), $\rightarrow$ (“impliceert”), $\leftrightarrow$ (“equivalent”) kunnen we gegeven proposities samenvoegen tot nieuwe. Als p en q staan voor proposities, krijgen we op die manier de volgende nieuwe beweringen:

$\neg p$ “niet p ”

$p \wedge q$ “zowel p als q ”

$p \vee q$ “ p of q ”

$p \rightarrow q$ “als p dan q ”

$p \leftrightarrow q$ “ p is equivalent met q ”

We merken nog op dat het “of” in $p \vee q$ staat voor het inclusieve “of”, dat wil zeggen, “ p of q , of beide”. Dit in tegenstelling tot het exclusieve “of p of q ” waarbij p en q niet beide mogen gelden. De equivalentie $p \leftrightarrow q$ betekent dat p en q ofwel beide waar, ofwel beide onwaar zijn. We spreken $p \leftrightarrow q$ ook wel uit als “ p dan en slechts dan als q ”. De formulering “dan en slechts dan als” komt in de wiskunde veelvuldig voor, en wordt vaak afgekort tot “desda”. (In het Engels zegt men “if and only if”, afgekort tot “iff”.) De symbolen $\neg$, $\wedge$, $\vee$, $\rightarrow$, en $\leftrightarrow$ heten de *logische connectieven*, en de symbolen p en q , die dus staan voor willekeurige proposities, heten *propositionele variabelen*. De taal bestaande uit propositionele variabelen, samen met de logische connectieven, heet de *propositielogica*.

In de propositielogica denken we aan de variabelen als wiskundige beweringen die of waar, of onwaar zijn. We gebruiken de notatie 1 voor waar, en 0 voor onwaar. De waarheid van een bewering als $p \wedge q$ hangt af van de waarheid van de beweringen p

en q : $p \wedge q$ is waar dan en slechts dan als zowel p als q waar is. Net zo is $p \vee q$ waar dan en slechts dan als minstens één van p en q waar is. We kunnen dit samenvatten in een tabel, een zogenaamde *waarheidstafel*:

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

De waarheidstafel somt alle mogelijke combinaties waarop p en q waar of onwaar kunnen zijn op, en geeft de bijbehorende waarheidswaarde van de samengestelde proposities $p \wedge q$ en $p \vee q$. We kunnen de waarheidstafel dan ook zien als een precieze *definitie* van de uitdrukkingen $p \wedge q$ en $p \vee q$.

Op analoge wijze hebben we een waarheidstafel voor $\neg p$. Merk op dat deze uitdrukking alleen afhangt van p , dus de waarheidstafel heeft maar twee rijen:

p	$\neg p$
1	0
0	1

Volgens deze waarheidstafel is dus $\neg p$ waar dan en slechts dan als p niet waar is. Tenslotte hebben we de volgende waarheidstafel voor $\rightarrow$ en $\leftrightarrow$:

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

Deze waarheidstafel is dus te lezen als definitie van deze connectieven. We zien dat $p \leftrightarrow q$ waar is dan en slechts dan als de waarheidswaarden van p en q gelijk zijn, en dat $p \rightarrow q$ alleen onwaar is als p waar is en q onwaar. Op dit punt gekomen vraagt de lezer zich misschien af waarom we definiëren dat $p \rightarrow q$ waar is als p onwaar is. Ter motivatie kan het volgende voorbeeld dienen. Het is niet onredelijk om een uitspraak over getallen als

$$\text{als } n < 10 \text{ dan } n < 100$$

als waar te bestempelen. Als we daartoe besluiten moet deze uitspraak echter waar zijn voor *alle* waarden van n . In het bijzonder moeten ook de uitspraken “als $50 < 10$ dan $50 < 100$ ” en “als $200 < 10$ dan $200 < 100$ ” waar zijn, terwijl de premisse in deze gevallen onwaar is. Een verdere moeilijkheid in het geval van de implicatie is dat we in het dagelijks gebruik niet gewend zijn aan uitspraken als “als een bal vierkant is ligt Parijs in Friesland”, waarbij de premisse geen enkel verband houdt met de conclusie. In de propositielogica, en in de definitie van $\rightarrow$ in het bijzonder, is echter het enige dat telt de waarheidswaarde van p en q . Deze implicatie $p \rightarrow q$ wordt ook wel de “materiële” implicatie genoemd, en is equivalent met $\neg p \vee q$ (zie opgave 1.4). Tenslotte merken we nog op dat we een onderscheid maken tussen de symbolen $\rightarrow$ en $\Rightarrow$: Het eerste is een formeel symbool dat we in formules gebruiken; het tweede gebruiken we alleen om een implicatie aan te geven in de *metataal*.

Voor propositionele variabelen gebruiken we vaak de letters p, q, r , en als we meer variabelen nodig hebben gebruiken we ook wel genummerde variabelen $p_1, p_2, p_3, \dots$.

Met behulp van de connectieven kunnen we nu willekeurig lange samenstellingen maken, zoals bijvoorbeeld

$$((p_1 \vee \neg p_2) \rightarrow p_3) \wedge \neg(p_2 \rightarrow p_4). \quad (1)$$

Zulke samenstellingen noemen we *propositionele formules*. Merk op dat we haakjes gebruiken om aan te geven hoe formules zijn opgebouwd; $p \vee q \wedge r$ kan anders zowel $(p \vee q) \wedge r$ als $p \vee (q \wedge r)$ betekenen. Omdat teveel haakjes de leesbaarheid van lange formules kunnen bemoeilijken hebben we de volgende conventies met betrekking tot haakjes:

- $\neg$ bindt sterker dan $\wedge$, $\vee$, en $\rightarrow$. Dus $\neg p \wedge q$ betekent $(\neg p) \wedge q$.
- $\wedge$ en $\vee$ binden sterker dan $\rightarrow$. Dus $p \vee q \rightarrow r$ betekent $(p \vee q) \rightarrow r$.

Met behulp van de waarheidstafels kunnen we in principe van elke propositionele formule de waarheidswaarde uitrekenen, gegeven de waarde van de propositionele variabelen. We zeggen “in principe”, want voor lange formules is deze methode niet erg praktisch, zie opgave 1.2.

Een formule die altijd waar is, ongeacht de waarheidswaarden van zijn variabelen, heet *geldig*, of een *tautologie*. Een formule is een tautologie als in de waarheidstafel in de kolom onder de formule overal een 1 staat.¹ Een voorbeeld van een tautologie is $(p \rightarrow q) \vee (q \rightarrow p)$. Immers, we hebben de volgende waarheidstafel voor deze formule:

p	q	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \vee (q \rightarrow p)$
1	1	1	1	1
1	0	0	1	1
0	1	1	0	1
0	0	1	1	1

We noemen twee propositieformules φ en ψ *equivalent* als geldt dat $\varphi \leftrightarrow \psi$ een tautologie is. Een formule die altijd onwaar is, ongeacht de waarde van zijn variabelen, heet een *contradictie*. Voor een contradictie geldt dat in de waarheidstafel in de kolom onder de formule overal een 0 staat. Een voorbeeld van een contradictie is $p \wedge \neg p$. Formules die noch een tautologie zijn noch een contradictie heten *contingent*. De formule (1) is een voorbeeld van een contingentie, zoals de lezer gemakkelijk nagaat. Merk op dat φ een tautologie is dan en slechts dan als $\neg\varphi$ een contradictie is.

We merken verder nog op dat $\vee$ en $\wedge$ *associatief* zijn, dat wil zeggen dat geldt dat de volgende formules tautologieën zijn (zie opgave 1.5):

$$p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r, \quad (2)$$

$$p \wedge (q \wedge r) \leftrightarrow (p \wedge q) \wedge r. \quad (3)$$

Dit betekent dat we $p \vee q \vee r$ mogen schrijven in plaats van $p \vee (q \vee r)$, en ook $p \wedge q \wedge r$ in plaats van $p \wedge (q \wedge r)$, zonder dat hierbij verwarring kan ontstaan.

¹Zoals gezegd is deze methode om tautologieën te herkennen voor formules met veel variabelen niet erg praktisch, maar dat wil niet zeggen dat er geen betere methoden zouden kunnen bestaan. De vraag of er een efficiënte methode bestaat om te bepalen of een formule geldig is is equivalent met één van de grote open problemen uit de wiskunde, namelijk het P-versus-NP-probleem.

1.2 Kwantoren

Naast de logische connectieven gebruiken we de afkortingen $\exists x$ voor “er bestaat een x ” en $\forall x$ voor “voor alle x ”. Het symbool $\exists$ heet de *existentiële kwantor*, en $\forall$ heet de *universele kwantor*. Met deze kwantoren kunnen we formules opschrijven van de vorm $\exists x\varphi(x)$ (“er bestaat een x zodat $\varphi(x)$ ”) en $\forall x\varphi(x)$ (“voor alle x geldt $\varphi(x)$ ”). Met behulp van opeenvolgende kwantoren kunnen we ingewikkelder uitspraken formuleren. Zo betekent $\forall x\exists y\varphi(x, y)$ dat er voor alle x een y bestaat zodat $\varphi(x, y)$ geldt. Formules met kwantoren heten *predikaatlogische formules*. Voor een preciezere definitie van de predikaatlogica verwijzen we naar het college Logica.²

Met behulp van de logische connectieven kunnen we weer samenstellingen maken van predikaatlogische formules. Zo betekent bijvoorbeeld

$$(\forall x\varphi(x)) \rightarrow (\exists y\psi(y)) \quad (4)$$

dat als voor alle x de uitspraak $\varphi(x)$ geldt, dat er dan een y bestaat zodat $\psi(y)$. Om overmatig gebruik van haakjes te vermijden gebruiken we de volgende conventie:

- $\forall$ en $\exists$ binden sterker dan de logische connectieven. We kunnen dus (4) ook schrijven als $\forall x\varphi(x) \rightarrow \exists y\psi(y)$

We merken verder nog op dat, op grond van de betekenis van $\exists$ en $\forall$, het volgende geldt:

- $\neg\exists x\varphi(x)$ is equivalent met $\forall x\neg\varphi(x)$,
- $\neg\forall x\varphi(x)$ is equivalent met $\exists x\neg\varphi(x)$.

Als een bewering $\varphi(x)$ niet geldt voor een zekere x , dan bewijst x dat de universele bewering $\forall x\varphi(x)$ onwaar is. We noemen x dan een *tegenvoorbeeld* voor deze bewering. Zo is $x = 7$ een tegenvoorbeeld voor de bewering dat alle getallen deelbaar zijn door 3.

Het moge duidelijk zijn dat we in de definities van de propositielogica en de predikaatlogica bepaalde keuzes hebben gemaakt. Met name de aanname dat elke propositie hetzij waar, hetzij onwaar is is verstrekkend, en ook aanvechtbaar. Voor de meeste delen van de moderne wiskunde is deze tweewaardige logica, meestal aangeduid als *klassieke logica*, echter de meest passende. Het ligt geenszins in de bedoeling om hier de indruk te wekken dat de klassieke logica de enig mogelijke keuze is. Er bestaan wel degelijk ook logica's die andere vormen van wiskundig of formeel redeneren beschrijven, en die in andere contexten, zoals de filosofie, taalkunde, of informatica, passender kunnen zijn. Deze alternatieven, zoals bijvoorbeeld intuïtionistische logica (toegesneden op de constructieve wiskunde) en de in de informatica veel gebruikte modale- en temporele logica, vallen buiten het bereik van deze inleiding. We merken tot slot alleen nog op dat voor het begrip van de genoemde alternatieven allereerst een goed begrip van de klassieke logica noodzakelijk is, zodat de klassieke logica in zekere zin een ijkpunt is voor alle andere vormen van redeneren.

1.3 Bewijzen

Naar alle redelijkheid zou wiskunde in het Nederlands “mathematiek” of iets dergelijks moeten heten, met dezelfde Latijnse stam als in alle andere landen der westerse beschaving, doch sinds Stevin³ de term “wisconst” introduceerde heeft het Nederlands

²We denken aan de kwantoren als lopend over een bepaald domein, zoals bijvoorbeeld de natuurlijke getallen. We nemen aan dat dit domein altijd niet-leeg is. Zonder deze aanname gelden bijvoorbeeld de equivalenties uit opgave 1.15 niet.

³Simon Stevin, Nederlands wis- en natuurkundige (1548–1620).

zijn eigen naam voor dit vakgebied. (Stevin introduceerde nog tal van andere wetenschappelijke termen, waaronder ook het inmiddels in onbruik geraakte “giskunde” voor de waarschijnlijkheidsrekening en het doen van schattingen in de zeevaart.)⁴ Zoals de term reeds aangeeft draait het in de wiskunde om zekerheid. In de dagelijkse praktijk formuleren wiskundigen uitspraken over wiskundige objecten en structuren, die ze vervolgens proberen te bewijzen. Als zij hierin slagen krijgt zo’n uitspraak de status van een *stelling*. Kleinere stellingen worden vaak aangeduid als *propositie*, en hulpstellingen met de term *lemma*. Een wiskundig *bewijs* is een serie redeneerstappen die de geldigheid van een stelling aantoonst. Omdat bewijzen een begin moeten hebben worden de uitgangspunten vastgelegd in zogeheten *axioma’s*, en de toegestane redeneermethoden in *bewijsregels*. Stellingen worden aldus bewezen uit de axioma’s, waarbij gebruik kan worden gemaakt van eerder bewezen stellingen. Om het denken te organiseren gebruiken wiskundigen verder nog *definities*, waarin nieuwe noties worden gedefinieerd in termen van reeds bestaande begrippen. De axioma’s worden geacht evident waar te zijn voor de objecten waar met iets over probeert te bewijzen. Verder is het bij de keuze van axioma’s zaak voldoende axioma’s te hebben om zoveel mogelijk interessante beweringen te kunnen bewijzen, dat wil zeggen, men streeft hier *volledigheid* na. Tegelijkertijd streeft men ernaar, uit het oogpunt van elegantie, geen overbodige aannames te maken, en derhalve het aantal axioma’s zo klein mogelijk te houden. In concrete gevallen kan het echter zeer moeilijk zijn om te bepalen of een axioma echt nodig is of niet. Om het eind van een bewijs te markeren wordt tegenwoordig vaak het symbool $\square$ gebruikt, waar vroeger de afkorting Q.E.D. (voor “quod erat demonstrandum”, ofwel “hetgeen bewezen moest worden”) meer in zwang was. Dit ziet er dan bijvoorbeeld zo uit:

Stelling 1.3.1. (Euclides)⁵ *Er zijn oneindig veel priemgetallen.*

Bewijs. Gegeven priemgetallen $p_1, \dots, p_n$ bewijzen we dat er een priemgetal bestaat dat ongelijk is aan $p_1, \dots, p_n$. Beschouw het getal $N = p_1 \cdot \dots \cdot p_n + 1$. Dan is N zelf priem, of deelbaar door een priemgetal p , in welk geval p ongelijk moet zijn aan $p_1, \dots, p_n$. In beide gevallen is er dus een priemgetal ongelijk aan $p_1, \dots, p_n$. $\square$

Formeel is een wiskundig bewijs een afleiding van een formule uit de axioma’s (die zelf weer formules zijn), met behulp van vaste bewijsregels. In de wiskundige praktijk zijn bewijzen echter meestal redeneringen in een mengvorm van natuurlijke taal en formules, met het idee dat er voldoende formele taal wordt gebruikt om de redenering ondubbelzinnig te maken, en tegelijkertijd zo weinig mogelijk om de redenering voor mensen begrijpelijk te houden. Een precieze definitie van de bewijsregels wordt met name belangrijk als men dingen wil bewijzen *over* wiskundige bewijzen, bijvoorbeeld dat bepaalde uitspraken *niet* bewijsbaar zijn. Formalisering wordt ook noodzakelijk bij toepassingen in de informatica, of als men zeer lange bewijzen wil controleren met behulp van computers. Voor ons volstaat voorlopig echter een informeel bewijsbegrip, en voor de definitie van een formeel bewijs verwijzen we naar het college Logica.

⁴Het hanteren van de landstaal voor wetenschappelijke doeleinden paste overigens in een internationale trend, zie Dijksterhuis [4, III,31]. Stevin geldt tevens als de uitvinder van de decimale breuknotatie [4, III,65].

⁵Grieks wiskundige, leefde rond 300 v.Chr. Euclides is de auteur van de *Elementen*, één van de meest invloedrijke boeken in de geschiedenis, niet alleen in de wiskunde maar ook daarbuiten. Het gegeven bewijs komt uit Boek IX.

Opgaven

Opgave 1.1. Schrijf de waarheidstafel op van de formule $\neg(p \vee \neg q) \rightarrow p \wedge \neg r$. (Merk op dat we hier de conventie voor het weglaten van haakjes gebruiken.)

Opgave 1.2. Laat φ een propositionele formule zijn met variabelen $p_1, \dots, p_n$. Een *bedeling* van deze variabelen is een toekenning van waarheidswaarden, 0 of 1, aan elke variabele.⁶

- (a) Hoeveel bedelingen zijn er voor de variabelen $p_1, \dots, p_n$?
- (b) Hoeveel rijen heeft de waarheidstafel van een formule met 10 variabelen?

Opgave 1.3. Bewijs met behulp van waarheidstafels dat de volgende formules tautologieën zijn:

- (i) $p \vee \neg p$
- (ii) $(p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q) \vee \neg(p \vee q)$

Opgave 1.4. (a) Bewijs dat $p \rightarrow q$ equivalent is met $\neg p \vee q$. Dit betekent dat we de implicatie $\rightarrow$ kunnen *definiëren* met behulp van $\neg$ en $\vee$.

(b) Bewijs dat $p \leftrightarrow q$ equivalent is met $(p \rightarrow q) \wedge (q \rightarrow p)$.

Opgave 1.5. Bewijs de associatieve wetten (2) en (3).

Opgave 1.6. Bewijs de volgende zogenaamde *wetten van De Morgan*.⁷

- (i) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
- (ii) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$

Opgave 1.7. Bewijs de volgende *distributieve wetten*:

- (i) $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$
- (ii) $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$

Opgave 1.8. Bewijs dat $p \rightarrow q$ equivalent is met $\neg q \rightarrow \neg p$. De tweede formule heet de *contrapositie* van de eerste. Deze equivalentie wordt in de wiskunde veelvuldig gebruikt: Om te bewijzen dat een bewering A bewering B impliceert is het voldoende om te bewijzen dat uit de ontkenning van B de ontkenning van A volgt.

Opgave 1.9. Bewijs de volgende regel:

$$\neg \neg p \leftrightarrow p$$

Opgave 1.10. Soms gebruiken we het symbool $\perp$, *falsum* genaamd, om een formule aan te geven die altijd onwaar is, dat wil zeggen, altijd waarheidswaarde 0 heeft. De formule $\perp$ bevat geen variabelen, en is op te vatten als een logische constante. Bewijs dat $\neg p \leftrightarrow (p \rightarrow \perp)$.

⁶Formeel is een bedeling dus een *functie* van de verzameling variabelen naar de verzameling $\{0, 1\}$.

⁷Naar de Britse wiskundige Augustus de Morgan (1806–1871).

Opgave 1.11. Bewijs de volgende regel:

$$(\neg p \rightarrow \perp) \rightarrow p$$

Deze regel heet ook wel “*bewijs uit het ongerijmde*” (Latijn: reductio ad absurdum): Als we een bewering A willen bewijzen is het voldoende om uit de aanname dat A *niet* geldt een tegenspraak af te leiden. Dit is een in de wiskunde zeer veel gebruikte vorm van redeneren.

Opgave 1.12. *Modus ponens* is de regel die zegt dat uit p en $p \rightarrow q$ volgt dat q geldt. Bewijs deze regel.

Opgave 1.13. (a) Bewijs dat elk van de connectieven $\wedge$, $\rightarrow$, en $\leftrightarrow$ uitgedrukt kan worden met alleen $\neg$ en $\vee$. Dit betekent dat we in principe elke propositionele formule kunnen schrijven met alleen $\neg$ en $\vee$. Dit is niet erg praktisch, maar maakt sommige bewijzen makkelijker.

(b) Bewijs dat we elke propositionele formule kunnen schrijven met alleen $\neg$ en $\wedge$.

Opgave 1.14. De *Sheffer stroke*⁸ is een connectief $|$ gedefinieerd door de volgende waarheidstafel:

p	q	$p q$
1	1	0
1	0	1
0	1	1
0	0	1

(a) Bewijs dat $p | q$ equivalent is met $\neg(p \wedge q)$. Om deze reden wordt de Sheffer stroke ook wel “nand” genoemd, voor “not and”.

(b) Bewijs dat $\neg p$ en $p \wedge q$ uitgedrukt kunnen worden door alleen gebruik te maken van $|$. Samen met opgave 1.13 geeft dit dat elke propositionele formule geschreven kan worden met alleen de Sheffer stroke.

Opgave 1.15. Stel dat de variabele x niet voorkomt in ψ . Bewijs de volgende regels:

- (i) $(\forall x \varphi(x) \wedge \psi)$ is equivalent met $\forall x(\varphi(x) \wedge \psi)$.
- (ii) $(\exists x \varphi(x) \vee \psi)$ is equivalent met $\exists x(\varphi(x) \vee \psi)$.
- (iii) $(\exists x \varphi(x) \rightarrow \psi)$ is equivalent met $\forall x(\varphi(x) \rightarrow \psi)$.
- (iv) $(\forall x \varphi(x) \rightarrow \psi)$ is equivalent met $\exists x(\varphi(x) \rightarrow \psi)$.

Opgave 1.16. (a) Bewijs dat $\exists y \forall x \varphi(x, y)$ impliceert dat $\forall x \exists y \varphi(x, y)$.

(b) Geef een voorbeeld waaruit blijkt dat $\forall x \exists y \varphi(x, y)$ in het algemeen niet impliceert dat $\exists y \forall x \varphi(x, y)$.

⁸Genoemd naar de Amerikaans-Poolse logicus Henry M. Sheffer (1882–1964).

Hoofdstuk 2

Verzamelingen

Die Mathematiker sind eine Art Franzosen: Redet man zu ihnen, so übersetzen sie es in ihre Sprache, und dann ist es alsobald ganz etwas Anderes.

J. W. Goethe, Sprüche in Prosa, Nr. 1011.

2.1 Operaties op verzamelingen

De moderne wiskunde kan worden omschreven als de studie van *structuren*, zoals groepen, vectorruimtes, topologische ruimtes, metrische ruimtes, etc.¹ Zulke wiskundige structuren bestaan doorgaans uit een verzameling met daarop een bepaalde structuur, zoals een metriek, een topologie, of operaties zoals optelling en vermenigvuldiging. De moderne wiskunde is aldus gegrondvest op het begrip *verzameling*, en voor een goed begrip ervan is het essentieel dat we met verzamelingen kunnen werken.

Een verzameling bestaat uit *elementen*, en als x een element is van een verzameling X noteren we dit als $x \in X$.² We gebruiken veelal accolades $\{$ en $\}$ om verzamelingen te noteren. Zo is bijvoorbeeld $\{1, 2, 3\}$ de verzameling met de elementen 1, 2, en 3. Soms gebruiken we puntjes om aan te geven dat een verzameling oneindig doorloopt. Zo is $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ de verzameling van natuurlijke getallen. We gebruiken binnen de accolades vaak het symbool $|$ om elementen met bepaalde eigenschappen aan te geven, zoals bijvoorbeeld in $\{x \in \mathbb{N} \mid x \text{ is deelbaar door } 2\}$. (In plaats van $|$ gebruiken we ook wel $:$ als scheidingssymbool.) Er is ook een verzameling zonder elementen: de *lege verzameling*, die we aangeven met $\emptyset$. Deze speelt een rol vergelijkbaar met die van het getal 0. Per definitie zijn twee verzamelingen gelijk als ze dezelfde elementen bevatten. Er is dus bijvoorbeeld geen verschil tussen de verzamelingen $\{1, 2\}$ en $\{2, 1\}$. Uit dit principe volgt ook dat er maar één lege verzameling is. Verzamelingen $\{x\}$ met slechts één element heten *singletons*. Ten overvloede merken we op dat x niet hetzelfde is als $\{x\}$.

Als voor twee verzamelingen X en Y geldt $\forall x(x \in X \rightarrow x \in Y)$, ofwel dat elk element van X ook een element is van Y , dan zeggen we dat X een *deelverzameling*

¹Deze visie op de wiskunde is sterk beïnvloed door een groep 20e-eeuwse Franse wiskundigen, verenigd onder de naam Bourbaki. Voor een beschrijving van de 20e-eeuwse ontwikkelingen in de wiskunde zie Odifreddi [9].

²De lezer zal opmerken dat we hier vermijden te definiëren *wat* een verzameling precies is. Dit is een meer filosofische kwestie (en bovendien een ingewikkelde), die buiten het bereik van deze syllabus valt. Voor de wiskunde is het vooral van belang wat de *regels* zijn volgens welke verzamelingen zich gedragen.

is van Y , en we schrijven dan $X \subseteq Y$.³

We hebben de volgende operaties en begrippen:

- $X \cap Y = \{x \mid x \in X \wedge x \in Y\}$. Deze verzameling heet de *doorsnede* van X en Y .
- $X \cup Y = \{x \mid x \in X \vee x \in Y\}$. Deze verzameling heet de *vereniging* van X en Y .
- $X \setminus Y = \{x \mid x \in X \wedge x \notin Y\}$. Deze verzameling heet het *verschil* van X en Y .
- Als $Y \subseteq X$, dan noemen we $X \setminus Y$ het *complement* van Y in X . Als X stilzwijgend bekend wordt verondersteld schrijven we ook wel kortweg Y^c in plaats van $X \setminus Y$.
- X en Y heten *disjunct* als $X \cap Y = \emptyset$.
- $\mathcal{P}(X) = \{A : A \subseteq X\}$. Deze verzameling van alle deelverzamelingen van X heet de *machtsverzameling* van X .

Als uitbreiding van de notatie uit hoofdstuk 1 schrijven we ook wel $\forall x \in X \varphi(x)$ in plaats van $\forall x(x \in X \rightarrow \varphi(x))$. Evenzo schrijven we vaak $\exists x \in X \varphi(x)$ in plaats van $\exists x(x \in X \wedge \varphi(x))$.

We kunnen ook doorsnedes en verenigingen nemen van *families* van verzamelingen. Als I een (mogelijk oneindige) verzameling indices is, en voor elke $i \in I$ is een verzameling X_i gegeven, dan hebben we de volgende vereniging en doorsnede:

- $\bigcup \{X_i \mid i \in I\} = \{x \mid \exists i(x \in X_i)\}$,
- $\bigcap \{X_i \mid i \in I\} = \{x \mid \forall i(x \in X_i)\}$.

Als alternatief gebruiken we hiervoor ook wel de notaties $\bigcup_{i \in I} X_i$ en $\bigcap_{i \in I} X_i$. Als X een familie van verzamelingen is geeft $\bigcup X$ de vereniging van alle verzamelingen in X aan. Dus $\bigcup X = \bigcup \{x \mid x \in X\}$. Analoog hebben we de notatie $\bigcap X$ voor de doorsnede van alle verzamelingen in X .

Voor eindige verzamelingen X geven we het aantal elementen van X , ook wel de *kardinaliteit* van X genoemd, aan met $|X|$. In hoofdstuk 6 zullen we het begrip kardinaliteit nader onderzoeken.

2.2 Het cartesisch product

We hebben al opgemerkt dat er in het algemeen geen *volgorde* zit in de elementen van een verzameling. Zo is er geen verschil tussen de verzamelingen $\{x, y\}$ en $\{y, x\}$. Als we wèl een onderscheid willen maken in de volgorde tussen x en y gebruiken we de notatie (x, y) , en noemen we dit een *geordend paar*. Zie opgave 2.12 voor een verzamelingstheoretische definitie van dit begrip.

Definitie 2.2.1. Het cartesisch product⁴ van twee verzamelingen X en Y is de verzameling geordende paren $X \times Y = \{(x, y) \mid x \in X \wedge y \in Y\}$.

³In analogie met de symbolen $<$ en $\leq$ gebruiken we $X \subset Y$ om aan te geven dat X een *strikte* deelverzameling is van Y , dat wil zeggen, dat $X \subseteq Y$ en $X \neq Y$. Deze notatie is niet geheel standaard in de literatuur; sommige auteurs gebruiken $\subset$ in plaats van $\subseteq$.

⁴Naar de Franse filosoof en wiskundige René Descartes (1596–1650)

Als $\mathbb{R}$ de verzameling reële getallen is (zie hoofdstuk 4), dan kunnen we $\mathbb{R} \times \mathbb{R}$ identificeren met het platte vlak: Gegeven een oorsprong kunnen we elk punt in het platte vlak beschrijven door middel van twee coördinaten (x, y) , met x en y in $\mathbb{R}$. We noteren het platte vlak dan ook met $\mathbb{R} \times \mathbb{R}$, of $\mathbb{R}^2$. Net zo kunnen we elk punt in de driedimensionale ruimte beschrijven met drie coördinaten (x, y, z) . Formeel kunnen we het tripel (x, y, z) definiëren als het geordende paar $((x, y), z)$. Gegeven deze definitie schrijven we meestal $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$, of $\mathbb{R}^3$, in plaats van $(\mathbb{R} \times \mathbb{R}) \times \mathbb{R}$. Algemener hebben we op dezelfde manier voor elke $n \in \mathbb{N}$ de n -dimensionale ruimte $\mathbb{R}^n$. Merk op dat, hoewel in het algemeen $(X \times Y) \times Z$ niet hetzelfde is als $X \times (Y \times Z)$, er een natuurlijke afbeelding tussen deze verzamelingen bestaat, zie opgave 3.5. Gegeven verzamelingen $X_1, \dots, X_n$ hebben we in het algemeen het product

$$X_1 \times \dots \times X_n = \{(x_1, \dots, x_n) \mid x_1 \in X_1 \wedge \dots \wedge x_n \in X_n\}.$$

De elementen $(x_1, \dots, x_n)$ heten *n-tupels*.

2.3 Verzamelingenalgebra

In hoofdstuk 1 hebben we gezien dat propositionele formules voldoen aan logische regels, die lijken op die van getallen in de algebra. We kunnen met formules dan ook “rekenen” op een manier die niet essentieel verschilt van het rekenen met getallen. Op een soortgelijke manier kunnen we rekenen met verzamelingen. Aan de definities van $\cap$, $\cup$, en $\setminus$ kunnen we zien dat deze operaties verwant zijn aan de logische operaties $\wedge$, $\vee$, en $\neg$. Voor verzamelingen gelden dan ook regels die analoog zijn aan die voor de propositielogica. Zo hebben we bijvoorbeeld voor een verzameling $A \subseteq X$ dat

$$X \setminus (X \setminus A) = A,$$

hetgeen correspondeert met de regel $\neg\neg p \leftrightarrow p$. Verdere voorbeelden van deze correspondentie zijn:

$$\begin{array}{ll} A \cap \emptyset = \emptyset & p \wedge \perp \leftrightarrow \perp \\ A \cup A = A & p \vee p \leftrightarrow p \end{array}$$

Ook zijn er regels analoog aan de distributieve wetten en de wetten van De Morgan, zie opgaven 2.3 en 2.4.

Verder zien we aan de definitie van $\subseteq$ dat deze relatie verwant is aan de implicatie. Zo hebben we bijvoorbeeld de volgende geldige uitspraken voor verzamelingen, en de corresponderende geldige formules:

$$\begin{array}{ll} \emptyset \subseteq A & \perp \rightarrow p \\ A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C & (p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r) \\ A \subseteq C \wedge B \subseteq C \Leftrightarrow A \cup B \subseteq C & (p \rightarrow r) \wedge (q \rightarrow r) \Leftrightarrow (p \vee q) \rightarrow r \\ C \subseteq A \wedge C \subseteq B \Leftrightarrow C \subseteq A \cap B & (r \rightarrow p) \wedge (r \rightarrow q) \Leftrightarrow r \rightarrow p \wedge q \end{array}$$

De lezer ga zelf de geldigheid van deze formules na. We noemen verder nog de volgende regels:

- (commutativiteit) $A \cap B = B \cap A$ en $A \cup B = B \cup A$.
- (associativiteit) $A \cap (B \cap C) = (A \cap B) \cap C$ en $A \cup (B \cup C) = (A \cup B) \cup C$.

Merk op dat de geldigheid van deze regels direct volgt uit de corresponderende logische geldigheden. Net als bij $\wedge$ en $\vee$ stelt de associativiteit van $\cap$ en $\cup$ ons weer in staat om haakjes weg te laten, en bijvoorbeeld te kunnen schrijven $A \cap B \cap C$ zonder dat verwarring kan ontstaan.

Opgaven

Opgave 2.1. Zij $A = \{0, 3, \mathbb{N}\}$ en $B = \{A, 2, \emptyset\}$. Welke van de volgende beweringen zijn geldig?

- | | | |
|--------------------------------|---|---|
| (a) $1 \in A$. | (d) $A \in B$. | (g) $A \in \mathcal{P}(B)$. |
| (b) $\mathbb{N} \subseteq A$. | (e) $\mathbb{N} \subseteq \mathcal{P}(A)$. | (h) $\emptyset \subseteq B$. |
| (c) A en B zijn disjunct. | (f) $\{\mathbb{N}\} \in \mathcal{P}(A)$. | (k) $\mathcal{P}(A) \cap B = \emptyset$. |

Opgave 2.2. Bewijs dat $A \subseteq X$ dan en slechts dan als $A \cap X = A$.

Opgave 2.3. Bewijs de volgende distributieve wetten:⁵

- (i) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- (ii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Vergelijk dit met opgave 1.7.

Opgave 2.4. Bewijs de volgende versie van de wetten van De Morgan (vergelijk opgave 1.6):

- (i) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$
- (ii) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

Opgave 2.5. Bewijs de volgende beweringen:

- (i) $(A \setminus B) \setminus C = (A \setminus C) \setminus B$.
- (ii) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.
- (iii) $C = \emptyset \iff (A \cup C) \setminus (B \cup C) = (A \setminus B) \cup C$.

Opgave 2.6. Maak met behulp van een plaatje duidelijk dat niet altijd geldt:

- (i) $(A \setminus B) \setminus C = A \setminus (B \setminus C)$.
- (ii) $(A \setminus B) \cup C = (A \cup C) \setminus B$.

Opgave 2.7. Laat $A, B \subseteq X$. Schrijf A^c voor $X \setminus A$. Bewijs de volgende beweringen:

- (i) $A \subseteq B \iff A \cap B^c = \emptyset \iff A \cap B^c = A \cap A^c$.
- (ii) $A \cup B = (A^c \cap B^c)^c$.
- (iii) $A \setminus B = A \cap B^c$.

Net als in de propositielogica (zie opgave 1.13) zien we dus dat $\subseteq$ en $\cup$ uitgedrukt kunnen worden met alleen $\cap$ en $\setminus$.

Opgave 2.8. Laat A een eindige verzameling zijn met n elementen. Wat is de kardinaliteit van $\mathcal{P}(A)$?

Opgave 2.9. Bewijs dat $A \subseteq B$ dan en slechts dan als $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

⁵Dit kan men goed aanschouwelijk maken met een plaatje, een zogenaamd Venn-diagram. Merk echter op dat zulke plaatjes geen overtuigend bewijs vormen. Zo hoeft wat geldt voor deelverzamelingen van het platte vlak nog niet te gelden voor alle verzamelingen. Een plaatje kan wel dienen als tegenvoorbeeld, zie opgave 2.6.

Opgave 2.10. Het *symmetrisch verschil* van twee verzamelingen A en B is gedefinieerd als $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Bewijs de volgende beweringen:

- (i) $A \triangle B = (A \cup B) \setminus (A \cap B)$.
- (ii) De operatie $\triangle$ is commutatief en associatief.
- (iii) $(A \triangle B) \triangle B = A$.

Opgave 2.11. Bewijs de volgende beweringen:

- (i) $\forall i \in I (X_i \subseteq A)$ dan en slechts dan als $\bigcup_{i \in I} X_i \subseteq A$.
- (ii) $\forall i \in I (A \subseteq X_i)$ dan en slechts dan als $A \subseteq \bigcap_{i \in I} X_i$.

Opgave 2.12. Definieer het begrip geordend paar door $(x, y) = \{\{x\}, \{x, y\}\}$. Laat zien dat dit de gewenste eigenschappen heeft van een geordend paar, namelijk dat $(x, y) = (u, v)$ impliceert dat $x = u$ en $y = v$.

Opgave 2.13. Bewijs dat $X \times Y = \emptyset$ dan en slechts dan als $X = \emptyset$ of $Y = \emptyset$.

Opgave 2.14. Laat X en Y verzamelingen zijn, en zij $A \subseteq X \times Y$. Bewijs of weerleg: Er bestaan verzamelingen $U \subseteq X$ en $V \subseteq Y$ zodat $A = U \times V$.

Opgave 2.15. Stel dat $A \subseteq X$ en $B \subseteq Y$. Geldt altijd dat $(X \times Y) \setminus (A \times B) = (X \setminus A) \times (Y \setminus B)$? Bewijs of geef een tegenvoorbeeld.

Hoofdstuk 3

Functies en Relaties

A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas.

G. H. Hardy, A Mathematician's Apology.

3.1 Relaties

Een *relatie* tussen verzamelingen X en Y is een deelverzameling R van het cartesisch product $X \times Y$. Als het paar (x, y) in de relatie R zit zeggen we dat x gerelateerd is aan y , en schrijven we ook wel xRy . Als X bijvoorbeeld een groep personen is, en Y bestaat uit een aantal partijen, dan kunnen we een relatie R tussen X en Y definiëren door xRy als x lid is van partij y . Als $X = Y$ noemen we R ook wel een relatie op X . Een voorbeeld van een relatie op $\mathbb{N}$ is de verzameling $\{(n, m) \mid n \text{ deelt } m\}$.

We hebben de volgende eigenschappen van relaties R op X :

- R is *reflexief* als xRx voor alle $x \in X$.
- R is *symmetrisch* als voor alle $x, y \in X$ geldt $xRy \rightarrow yRx$.
- R is *transitief* als voor alle $x, y, z \in X$ geldt $xRy \wedge yRz \rightarrow xRz$.

Zo is bijvoorbeeld de ordening $\leq$ op $\mathbb{N}$ reflexief en transitief, maar niet symmetrisch.

Soms kunnen we de reflexiviteit en symmetrie van een relatie aanschouwelijk maken in een plaatje. Als bijvoorbeeld R een relatie is op $\mathbb{R}$, dan is R reflexief als de lijn $x = y$ bevat is in R , en R is symmetrisch als R invariant is onder spiegeling in de lijn $x = y$. Van een relatie R op een eindige verzameling X kunnen we een plaatje maken door een kruisje $\times$ te zetten voor paren $(x, y) \in R$. Zo zien we bijvoorbeeld in één oogopslag dat de volgende relatie op $\{1, 2, 3, 4\}$ reflexief is, maar niet symmetrisch.

	1	2	3	4
1	$\times$		$\times$	
2		$\times$		
3	$\times$		$\times$	$\times$
4				$\times$

3.2 Functies

Een *functie* f van een verzameling X naar een verzameling Y is een relatie die aan elke $x \in X$ een $y \in Y$ toevoegt. Een functie is dus een speciaal soort relatie f tussen X en Y , met de eigenschap dat als (x, y) en (x, z) beide in de relatie zitten geldt dat $y = z$. Met andere woorden, voor elke $x \in X$ is er een unieke $y \in Y$ met $(x, y) \in f$. We noemen deze y de *functiewaarde* van x , en schrijven $f(x) = y$, of ook wel $x \mapsto y$. De variabele x heet het *argument* van de functie. Als f een functie is van X naar Y schrijven we $f : X \rightarrow Y$. Functies heten ook wel *afbeeldingen*. De verzameling X heet het *domein* van f , en Y heet ook wel het *codomein*. Het *bereik* van f is de verzameling

$$\{y \in Y \mid \exists x \in X (f(x) = y)\}.$$

Het bereik wordt vaak genoteerd als $\text{im}(f)$, naar het Engelse “image”, en het domein wordt vaak aangegeven met $\text{dom}(f)$. Voor elke $A \subseteq X$ hebben we de verzameling

$$f(A) = \{y \in Y \mid \exists x \in A (f(x) = y)\},$$

het *beeld* van A onder f . In het bijzonder hebben we dus $f(X) = \text{im}(f)$. Omgekeerd hebben we voor elke $A \subseteq Y$ de verzameling

$$f^{-1}(A) = \{x \in X \mid f(x) \in A\},$$

het zogenaamde *volledig origineel*, of *inverse beeld* van A . Merk op dat $f^{-1}(Y) = \text{dom}(f)$.

We hebben de volgende elementaire eigenschappen van functies:

- f is een *injectie* als voor alle x en y in X , $x \neq y$ impliceert dat $f(x) \neq f(y)$.
- f is een *surjectie* als er voor elke $y \in Y$ een $x \in X$ is zodat $f(x) = y$.
- f is een *bijjectie* als f zowel injectief als surjectief is.

Zo is bijvoorbeeld de functie $f : \mathbb{R} \rightarrow \mathbb{R}$ gedefinieerd door $f(x) = x^2$ noch injectief, noch surjectief. De functie $x \mapsto \sin x$ is niet injectief en niet surjectief als functie van $\mathbb{R}$ naar $\mathbb{R}$, maar wel bijjectief als functie van $[-\frac{1}{2}\pi, \frac{1}{2}\pi]$ naar $[-1, 1]$. Als we willen bepalen of een functie surjectief of injectief is is het dus van belang om te erbij te vermelden wat het bedoelde domein en codomein is.

Als $f : X \rightarrow Y$ bijjectief is, is er bij elke $y \in Y$ precies één $x \in X$ zodat $f(x) = y$. Bijjecties worden om die reden ook vaak *1-1-correspondenties* genoemd.

Voor elke verzameling X hebben we de functie $f : X \rightarrow X$ gedefinieerd door $f(x) = x$. Deze functie heet de *identiteit* op X , en noteren we met id_X . Merk op dat id_X altijd een bijjectie is.

Als $f : X \rightarrow Y$ injectief is is f een bijjectie tussen X en $f(X)$. We kunnen in dit geval een functie $g : f(X) \rightarrow X$ definiëren door $g(y) = x$, waar $x \in X$ het unieke element is met $f(x) = y$. Deze g heet de *inverse* van f op $f(X)$, en we gebruiken voor g de notatie f^{-1} . Merk op dat we de notatie f^{-1} ook al gebruikt hebben voor inverse beelden, maar dat zal geen verwarring geven. Functies met een inverse heten *inverteerbaar*. Zo is bijvoorbeeld $\sqrt{x}$ de inverse van de functie x^2 op $[0, \infty)$.¹ Merk

¹Zoals we reeds opmerkten bestaat er een bepaalde mate van onduidelijkheid als we spreken over “de functie x^2 ”, zonder het bedoelde domein erbij te vermelden. Ook kan het gebruik van x^2 , in plaats van $f(x) = x^2$, verwarring scheppen, omdat er ook de functie $f(y) = x^2$ mee bedoeld kan zijn. In het eerste geval is bijvoorbeeld de afgeleide $2x$, en in het tweede geval 0. Het gebruik van zinsneden als “de functie x^2 ” is echter volkomen ingeburgerd, en in gevallen waar verwarring kan ontstaan is deze gemakkelijk te vermijden door preciezer te zijn.

op dat we de inverse van x^2 alleen beschouwen op $[0, \infty)$, omdat x^2 niet injectief is op $\mathbb{R}$.

Als $f : X \rightarrow Y$ en $g : Y \rightarrow Z$, dan kunnen we f en g *samenstellen* tot een functie $h : X \rightarrow Z$ door $h(x) = g(f(x))$. Deze samengestelde functie h noteren we met $g \circ f$. Dit wordt ook wel uitgesproken als “ g na f ”.

Propositie 3.2.1. *Een functie $f : X \rightarrow Y$ is bijectief dan en slechts dan als er een functie $g : Y \rightarrow X$ bestaat met $g \circ f = \text{id}_X$ en $f \circ g = \text{id}_Y$.*

Bewijs. Als f bijectief is kunnen we voor g de inverse f^{-1} nemen. Per definitie van de inverse geldt dat $f^{-1}(f(x)) = x$ voor alle $x \in X$, ofwel $f^{-1} \circ f = \text{id}_X$. Net zo geldt $f \circ f^{-1} = \text{id}_Y$.

Stel omgekeerd dat voor $g : Y \rightarrow X$ geldt dat $g \circ f = \text{id}_X$ en $f \circ g = \text{id}_Y$. Dan $f(g(y)) = y$ voor alle $y \in Y$, dus f is surjectief. Als $f(x_0) = f(x_1)$ dan $x_0 = g(f(x_0)) = g(f(x_1)) = x_1$, dus f is ook injectief. $\square$

Zij $f : X \rightarrow X$ een functie. Dan definiëren we de n -de iteratie f^n van f recursief door $f^0 = \text{id}_X$, en

$$f^{n+1} = f \circ f^n.$$

In het bijzonder hebben we $f^1 = f$. Voor een gegeven $x \in X$ heet de rij

$$x, f(x), f^2(x), f^3(x), \dots$$

de *baan* van x . Het itereren van functies is een veel gebruikt concept in de wiskunde, met name in de theorie van dynamische systemen. Zie ook opgave 3.6.

Naast functies met één argument x beschouwen we ook wel functies met meerdere argumenten $x_1, \dots, x_n$. Formeel is dit niets anders dan een functie $f : X_1 \times \dots \times X_n \rightarrow Y$ gedefinieerd op een cartesisch product. Het aantal argumenten n heet de *ariteit* van f .

3.3 Equivalentierelaties

Een essentieel aspect van de wiskunde is *abstractie*, dat wil zeggen, het weglaten van onnodige details en eigenschappen van het onderwerp van studie. Hoewel bijvoorbeeld lijnen in de praktijk altijd een bepaalde dikte hebben, hebben de lijnen in de Euclidische meetkunde helemaal geen dikte. Grappigerwijze *vergroot* deze idealisering juist de toepasbaarheid van de theorie. Of we kunnen bijvoorbeeld in bepaalde situaties waarin alleen telt op welke dag iemand geboren is redeneren over mensen, waarbij we personen met dezelfde verjaardag als gelijk beschouwen. Deze laatste situatie, waarin we groepen objecten indelen volgens een bepaald criterium, komt in de wiskunde veelvuldig voor, en wordt geformaliseerd door het begrip equivalentierelatie.

Definitie 3.3.1. Een relatie R op een verzameling X heet een *equivalentierelatie*, of kortweg een *equivalentie*, als geldt dat R reflexief, symmetrisch, en transitief is. Voor elke $x \in X$ hebben we de verzameling

$$\{y \in X \mid xRy\}$$

van elementen die equivalent zijn met x . We noemen deze verzameling de *equivalentieklasse* van x . De verzameling equivalentieklassen geven we aan met X/R . We spreken dit uit als “ X modulo R ”, of als “ X uitgedeeld naar R ”.

We geven een aantal voorbeelden van equivalentierelaties:

- (i) Het meest elementaire voorbeeld van een equivalentierelatie is de gelijkheidsrelatie $=$.² Deze is duidelijk reflexief, symmetrisch, en transitief. Elke equivalentieklasse bevat precies één element.
- (ii) Beschouw de verzameling van alle lijnen in het platte vlak $\mathbb{R}^2$. Gegeven twee lijnen l_0 en l_1 , laat $l_0 \sim l_1$ als l_0 en l_1 parallel zijn. Dan is $\sim$ een equivalentie, die we informeel kunnen beschrijven door te zeggen dat we de lijnen in $\mathbb{R}^2$ beschouwen modulo hun richting.
- (iii) Het boven gegeven voorbeeld van het hebben van dezelfde verjaardag is een equivalentierelatie op de verzameling van alle mensen. Er zijn 366 equivalentieklassen.
- (iv) Laat $n \in \mathbb{Z}$, met $n \geq 1$. We definiëren een equivalentierelatie $\equiv$ op $\mathbb{Z}$ door $x \equiv y$ als x en y dezelfde rest hebben bij deling door n . Anders geformuleerd: $x \equiv y$ als $x - y$ een veelvoud is van n . In dit geval zeggen we dat x *congruent* is met y modulo n . Notatie: $x \equiv y \pmod{n}$. De verzameling equivalentieklassen wordt in dit geval meestal genoteerd als $\mathbb{Z}/n\mathbb{Z}$.
- (v) Definieer de relatie $\sim$ op $\mathbb{R}$ door: $x \sim y$ als $x - y = 2k\pi$ voor zekere $k \in \mathbb{Z}$. Dan is $\sim$ een equivalentierelatie, en we kunnen $\mathbb{R}/\sim$ opvatten als de verzameling *hoeken*.
- (vi) De *norm* $\|v\|$ van een vector $v = (x, y)$ in $\mathbb{R}^2$ is gedefinieerd als $\|v\| = \sqrt{x^2 + y^2}$. Dit geeft een equivalentie op $\mathbb{R}^2$ gedefinieerd door $v \sim w$ als $\|v\| = \|w\|$. De equivalentieklassen zijn concentrische cirkels in $\mathbb{R}^2$.
- (vii) Bij elke surjectieve afbeelding $f : X \rightarrow Y$ kunnen we een relatie op X definiëren door: $x \sim y$ als $f(x) = f(y)$. Dan is $\sim$ een equivalentierelatie, met als equivalentieklassen de verzamelingen $f^{-1}(y)$, met $y \in Y$. De verzameling $f^{-1}(y)$ heet ook wel de *vezel* van y . Omgekeerd kan elke equivalentierelatie op deze manier beschreven worden, zie opgave 3.15.

Definitie 3.3.2. Een *partitie* van een verzameling X is een familie $\{X_i\}_{i \in I}$ van deelverzamelingen van X waarvoor geldt:

- de X_i zijn disjunct, dat wil zeggen, $X_i \cap X_j = \emptyset$ voor alle $i, j \in I$ met $i \neq j$,
- de X_i vormen een *overdekking* van X , dat wil zeggen, $\bigcup_{i \in I} X_i = X$.

De lezer kan zelf nagaan dat als R een equivalentierelatie is op X , de equivalentieklassen een partitie vormen van X . Omgekeerd hoort bij elke partitie een equivalentierelatie (opgave 3.12).

Als $\sim$ een equivalentierelatie is op een verzameling X , dan geven we de equivalentieklasse van $x \in X$ vaak aan met $[x]$. Als $y \in [x]$ dan noemen we y een *representant* van de equivalentieklasse $[x]$. Een *verzameling representanten* voor $\sim$ is een deelverzameling van X die voor elke equivalentieklasse precies één representant bevat. Zo is bijvoorbeeld $[0, 2\pi)$ een verzameling representanten voor de equivalentierelatie uit voorbeeld (v) boven. Immers, modulo 2π is elke hoek gelijk aan een hoek in $[0, 2\pi)$. Merk op dat er verschillende verzamelingen representanten kunnen zijn; in dit voorbeeld is $(-\pi, \pi]$ ook een verzameling representanten. Het is vaak makkelijker om te werken met een verzameling representanten dan met de equivalentieklassen zelf.

²Het symbool voor gelijkheid werd ingevoerd door de Welshe wiskundige Robert Recorde (ca.1512–1558), volgens wie niets gelijkjer kon zijn dan twee parallelle lijnstukjes van dezelfde lengte.

Stel dat f een functie is op op X met de eigenschap

$$[x] = [y] \Rightarrow f(x) = f(y) \quad (5)$$

voor alle $x, y \in X$. In dat geval kunnen we een functie F op $X/\sim$ definiëren door

$$F([x]) = f(x).$$

Dit is een zinvolle definitie, omdat de definitie van $F([x])$ wegens (5) niet afhangt van de keuze van de representant x . We zeggen dat de aldus gedefinieerde functie F *welgedefinieerd* is. Als we dus werken met een equivalentie $\sim$ op X kunnen we in het algemeen blijven werken met de elementen van X , in plaats van met de equivalentieklassen, zolang hetgeen we doen niet afhangt van de keuze van de representanten. We zullen dit bijvoorbeeld doen bij de definities van $+$ en $\cdot$ op $\mathbb{Z}$ en $\mathbb{Q}$ in hoofdstuk 4.

3.4 Functieverzamelingen

Definitie 3.4.1. Voor gegeven verzamelingen X en Y hebben we de functieverzameling $Y^X = \{f \mid f : X \rightarrow Y\}$ van alle functies van X naar Y .

We hebben ons functiebegrip gebaseerd op het begrip verzameling. In sommige situaties is het juist handig om een verzameling te zien als een functie. In het volgende beschouwen we deelverzamelingen van een vaste verzameling X . Bij elke verzameling $A \subseteq X$ hoort een zogenaamde *karakteristieke functie* χ_A , gedefinieerd als volgt:

$$\chi_A(x) = \begin{cases} 1 & \text{als } x \in A, \\ 0 & \text{als } x \notin A. \end{cases}$$

Voor elke $A \subseteq X$ is χ_A dus een functie van X naar $\{0, 1\}$. Omgekeerd hoort bij elke functie $\chi : X \rightarrow \{0, 1\}$ een verzameling A namelijk

$$A = \{x \in X \mid \chi(x) = 1\}.$$

We zien dus dat de correspondentie $A \mapsto \chi_A$ een *bijectie* is tussen de verzamelingen $\mathcal{P}(X)$ en $\{0, 1\}^X$. Vaak wordt de verzameling $\{0, 1\}$ eenvoudigweg geschreven als 2, zodat we deze laatste verzameling ook kunnen schrijven als 2^X . We hebben dus bewezen:

Propositie 3.4.2. Voor elke verzameling X is er een bijectie tussen de verzamelingen $\mathcal{P}(X)$ en 2^X .

Het cartesisch product $X \times Y$ van twee verzamelingen werd gedefinieerd in Definitie 2.2.1. We kunnen ook het cartesisch product van nemen van families van verzamelingen: Als I een (mogelijk oneindige) verzameling indices is, en voor elke $i \in I$ is een verzameling X_i gegeven, dan definiëren we het cartesisch product van de familie $\{X_i\}_{i \in I}$ door

$$\prod_{i \in I} X_i = \left\{ f : I \rightarrow \bigcup_{i \in I} X_i \mid \forall i \, f(i) \in X_i \right\}.$$

In het bijzonder hebben we in het geval dat alle X_i gelijk zijn dat

$$\prod_{i \in I} X = X^I.$$

In het speciale geval dat $I = \mathbb{N}$ kunnen we $X^{\mathbb{N}}$ opvatten als de verzameling van alle oneindige rijtjes van elementen uit X . Merk tenslotte nog op dat voor $I = \{0, 1\}$ het cartesisch product $\prod_{i \in I} X_i$ niet helemaal hetzelfde is als $X_0 \times X_1$, maar dat we deze verzamelingen toch wel met elkaar kunnen identificeren, door het paar $(x, y) \in X \times Y$ gelijk te stellen aan de functie $f : \{0, 1\} \rightarrow X \cup Y$ met $f(0) = x$ en $f(1) = y$.

3.5 Ordeningen

Een *partiële ordening* (afgekort met p.o.) is een paar $(X, \leq)$ bestaande uit een verzameling X en een binaire relatie $\leq$ op X , zodanig dat voor alle $x, y, z \in X$ geldt

- (i) $x \leq x$ (reflexiviteit),
- (ii) $x \leq y \wedge y \leq x \Rightarrow x = y$ (antisymmetrie),
- (iii) $x \leq y \wedge y \leq z \Rightarrow x \leq z$ (transitiviteit).

Voorbeelden van partiële ordeningen zijn:

- De verzamelingen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, en $\mathbb{R}$ met hun gebruikelijke ordeningsrelaties $\leq$.
- Voor elke verzameling X is de machtsverzameling $\mathcal{P}(X)$ met de inclusierelatie $\subseteq$ een p.o.
- De verzameling lineaire deelruimtes van een vectorruimte, geordend door inclusie.
- Laat G een acyclische graaf zijn, en laat xRy als er een pad in G is van knoop x naar knoop y . Dan is R een p.o. op G .
- Orden de verzameling $\mathbb{N}^{\mathbb{N}}$ als volgt. Voor $f, g \in \mathbb{N}^{\mathbb{N}}$, laat $f \leq g$ als geldt dat $f(i) \leq g(i)$ voor alle $i \in \mathbb{N}$. Dan is $\leq$ een p.o. op $\mathbb{N}^{\mathbb{N}}$.

Een p.o. $(X, \leq)$ heet *totaal* (of *lineair*) als geldt dat voor alle $x, y \in X$, $x \leq y$ of $y \leq x$. Zo is $(\mathbb{Z}, \leq)$ bijvoorbeeld lineair, maar de voorouderrelatie is dat niet (waarom?). Als geldt dat $x \not\leq y$ en $y \not\leq x$ dan heten x en y *onvergelijkbaar* of *incompatibel*. Een p.o. $(X, \leq)$ is dus totaal dan en slechts dan als er geen incompatibele elementen zijn in X . Ga na dat als X minstens twee elementen bevat de p.o. $(\mathcal{P}(X), \subseteq)$ niet totaal is.

Definitie 3.5.1. Een afbeelding f tussen twee p.o.'s $(X, \leq_X)$ en $(Y, \leq_Y)$ heet een *orde-isomorfisme* als f bijectief is en voor alle $x, y \in X$ geldt

$$x \leq_X y \Leftrightarrow f(x) \leq_Y f(y).$$

Ordeningen heten *isomorf* als er een orde-isomorfisme tussen hen bestaat.

De ordeningen $(\mathbb{N}, \leq)$ en $(\mathbb{Z}, \leq)$ zijn bijvoorbeeld niet isomorf, zie opgave 3.18. Aan de andere kant zijn bijvoorbeeld $(\mathbb{N}, \leq)$ en $(\{1, 2, 3, \dots\}, \leq)$ wel isomorf. Isomorphe ordeningen hoeven dus niet dezelfde verzamelingen te zijn, maar zijn gelijk *als ordening*.

Stelling 3.5.2. Elke partiële ordening $(X, \leq)$ is isomorf met $(W, \subseteq)$ voor een zekere $W \subseteq \mathcal{P}(X)$.

Bewijs. Definieer voor elke $x \in X$ de “downset”

$$D_x = \{y \in X \mid y \leq x\}$$

en laat $W = \{D_x \mid x \in X\}$. Definieer de afbeelding $\varphi : X \rightarrow W$ door $x \mapsto D_x$. Dan is φ een isomorfisme (opgave 3.20). $\square$

Stelling 3.5.2 is een voorbeeld van een *representatiestelling*: Hij laat zien dat we elke partiële ordening kunnen opvatten als een ordening van *verzamelingen*.

Opgaven

Opgave 3.1. Bepaal van elk van de volgende relaties op de verzameling mensen of ze reflexief, symmetrisch, of transitief zijn:

- (a) “is kind van”.
- (b) “is nakomeling van”.
- (c) “is familielid van”.
- (d) “heeft dezelfde verjaardag als”.

Opgave 3.2. Zij $A = \{-6, -5, -4, \dots, 4, 5, 6\}$. Bepaal van elk van de volgende relaties op A of ze reflexief, symmetrisch, of transitief zijn. We beschouwen de paren (x, y) uit $A \times A$ die voldoen aan:

- (i) $x - y < 0$.
- (ii) $x \leq y$.
- (iii) $x + y \leq 0$.
- (iv) $|x| = |y|$.

Opgave 3.3. Geef een voorbeeld van een functie $f : \mathbb{R} \rightarrow \mathbb{R}$ die surjectief is maar niet injectief. Geef een ook voorbeeld van een functie $f : \mathbb{R} \rightarrow \mathbb{R}$ die injectief is maar niet surjectief.

Opgave 3.4. Stel dat X een eindige verzameling is en dat $f : X \rightarrow X$. Bewijs dat f injectief is dan en slechts dan als f surjectief is.

Opgave 3.5. Bewijs dat er voor alle verzamelingen X , Y , en Z een bijectie bestaat tussen de verzamelingen $(X \times Y) \times Z$ en $X \times (Y \times Z)$.

Opgave 3.6. Stel dat $f : X \rightarrow X$ injectief is, en dat $x \in X \setminus f(X)$. Bewijs dat alle elementen in de baan $\{f^n(x)\}_{n \in \mathbb{N}}$ van x verschillend zijn.

Opgave 3.7. Laat $f : X \rightarrow X$ een functie zijn, en stel dat $f^n = \text{id}_X$ voor een $n \geq 1$. Bewijs dat f een bijectie is.

Opgave 3.8. Stel dat $f : X \rightarrow Y$, $g : Y \rightarrow Z$, en $h : Z \rightarrow W$. Bewijs dat $h \circ (g \circ f) = (h \circ g) \circ f$. Net als eerder bijvoorbeeld bij $\wedge$ en $\cap$ kunnen we dus de haakjes weglaten, en eenvoudigweg schrijven $h \circ g \circ f$.

Opgave 3.9. Stel dat $f : X \rightarrow Y$ en $g : Y \rightarrow Z$. Bewijs dat voor elke $A \subseteq Z$ geldt

$$(g \circ f)^{-1}(A) = f^{-1}(g^{-1}(A)).$$

Opgave 3.10. Gegeven een functie $f : X \rightarrow Y$ en een deelverzameling $A \subseteq X$ definiëren we de *restrictie* (of *beperking*) van f tot A als

$$f \upharpoonright A = f \cap (A \times Y).$$

(Als een functie g een restrictie is van f dan heet f ook wel een *voortzetting* van g .)

- (a) Laat zien dat $f \upharpoonright A = f \circ \text{id}_A$.
- (b) Stel dat $A, B \subseteq X$. Bewijs dat $(f \upharpoonright A) \upharpoonright B = f \upharpoonright (A \cap B)$.
- (c) Stel dat $C \subseteq Y$. Bewijs dat $(f \upharpoonright A)^{-1}(C) = A \cap f^{-1}(C)$.

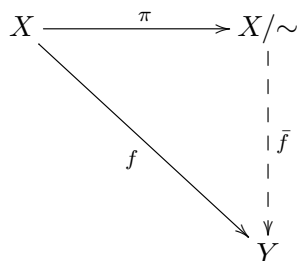
Opgave 3.11. Stel dat R en S equivalentierelaties zijn. Geldt dat $R \cup S$ weer een equivalentierelatie is? En $R \cap S$?

Opgave 3.12. (a) Zij R een equivalentierelatie op X . Bewijs dat de equivalentie-
klassen een partitie vormen van X .

(b) Zij $\{X_i\}_{i \in I}$ een partitie van X . Definieer een relatie R op X door: xRy als er een $i \in I$ bestaat zodat $x \in X_i$ en $y \in X_i$. Bewijs dat R aldus gedefinieerd een equivalentierelatie is, met de X_i als equivalentie-
klassen.

Opgave 3.13. Geef bij elk van de boven gegeven voorbeelden (i)-(vi) van equivalentierelaties een verzameling representanten aan.

Opgave 3.14. Zij gegeven een equivalentierelatie $\sim$ op een verzameling X . Geef de equivalentieklasse van x aan met $[x]$, en definieer $\pi : X \rightarrow X/\sim$ door $\pi(x) = [x]$. De afbeelding π heet de *canonieke afbeelding*. Stel dat $f : X \rightarrow Y$ een functie is zodat $x \sim y \Rightarrow f(x) = f(y)$. Bewijs dat er een unieke functie $\bar{f} : X/\sim \rightarrow Y$ bestaat zodat $f = \bar{f} \circ \pi$.



Opgave 3.15. In voorbeeld (vii) boven merkten we op dat elke surjectieve afbeelding $f : X \rightarrow Y$ aanleiding geeft tot een equivalentierelatie op X . Laat zien dat omgekeerd elke equivalentierelatie van deze vorm is: Voor elke equivalentie R op X bestaat er een surjectie $f : X \rightarrow Y$ zodat de equivalentie-
klassen van R precies de vezels $f^{-1}(y)$ zijn.

Opgave 3.16. Teken een plaatje van de p.o. $(\mathcal{P}(\{0, 1, 2\}), \subseteq)$.

Opgave 3.17. Bewijs dat er 19 mogelijke partiële ordeningen zijn op $\{0, 1, 2\}$.

Opgave 3.18. (a) Bewijs dat $(\mathbb{N}, \leq)$ en $(\mathbb{Z}, \leq)$ niet orde-isomorf zijn.

(b) Bewijs dat $(\mathbb{Z}, \leq)$ en $(\mathbb{Q}, \leq)$ niet orde-isomorf zijn.

Opgave 3.19. Gegeven een p.o. $(X, \leq)$, definieer de *omgekeerde ordening* $(X, \leq^*)$ door $y \leq^* x$ als $x \leq y$. Als uit de context duidelijk is wat $\leq$ is geven we deze ordening korthedshalve aan met X^* .

- (a) Bewijs dat $\mathbb{Z}$ en $\mathbb{Z}^*$ orde-isomorf zijn.
- (b) Is $\mathbb{N}^*$ orde-isomorf met $\mathbb{N}$?

Opgave 3.20. Bewijs dat de afbeelding φ uit het bewijs van Stelling 3.5.2 een isomorfisme is.

Opgave 3.21. Een *preordering* op een verzameling X is een relatie R op X die reflexief en transitief is.

(a) Laat zien dat we uit elke preordering R een equivalentierelatie $\sim_R$ kunnen definiëren door $x \sim_R y$ als xRy en yRx .

(b) Gegeven de equivalentie $\sim_R$ uit (a), geef voor elke $x \in X$ de equivalentieklasse van x aan met $[x]$. Definieer een relatie S op $X/\sim_R$ door

$$[x]S[y] \Leftrightarrow xRy.$$

Laat zien dat S welgedefinieerd is. Bewijs vervolgens dat S een partiële ordening is op $X/\sim_R$.

Opgave 3.22.* Gegeven twee lineaire ordeningen $(X, \leq_X)$ en $(Y, \leq_Y)$ definiëren we de zogenaamde *lexicografische ordening* op het product $X \times Y$ door: $(x_0, y_0) \leq (x_1, y_1)$ als

$$\begin{aligned} x_0 &\neq x_1 \text{ en } x_0 \leq_X x_1, \text{ of} \\ x_0 &= x_1 \text{ en } y_0 \leq_Y y_1. \end{aligned}$$

We kunnen ons dit voorstellen als de ordening verkregen uit X door elk element van X te vervangen door een kopie van Y . Bewijs dat de lexicografische ordening niet commutatief is, dat wil zeggen, de ordening op $X \times Y$ is in het algemeen niet isomorf met die op $Y \times X$.

Hoofdstuk 4

Getallen

Of all escapes from reality, mathematics is the most successful ever.
G.-C. Rota [11, p70].

4.1 Getallenstelsels

In de loop van de geschiedenis zijn verschillende soorten getallen in de wiskunde geïntroduceerd, waarbij het kunnen oplossen van vergelijkingen steeds een belangrijke rol heeft gespeeld. In dit hoofdstuk bespreken we de diverse getallenstelsels. De *natuurlijke getallen* $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ zijn we al eerder tegengekomen. We beschouwen deze als gegeven, en gaan niet verder in op hoe ze te definiëren zijn.¹ Naast de natuurlijke getallen hebben we verder:

- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, de verzameling *gehele* getallen. De getallen in $\mathbb{Z} \setminus \mathbb{N}$ heten *negatief*.
- $\mathbb{Q} = \{\frac{n}{m} : n, m \in \mathbb{Z}, m \neq 0\}$, de verzameling *rationale* getallen. De getallen in $\mathbb{Q} \setminus \mathbb{Z}$ heten *gebroken*.
- $\mathbb{R}$ is de verzameling *reële* getallen met oneindig doorlopende decimale ontwikkeling, zoals bijvoorbeeld

$$\pi = 3,1415926535897\dots$$

De getallen in $\mathbb{R} \setminus \mathbb{Q}$ heten *irrationaal*.

- $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$, de verzameling *complexe* getallen. Hier is i een nieuw getal met de eigenschap dat $i^2 = -1$. De getallen in $\mathbb{C} \setminus \mathbb{R}$ heten *imaginair*.

Deze verzamelingen getallen vormen een stijgende rij:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

¹Dit brengt de bekende uitspraak van de Duitse wiskundige Leopold Kronecker (1823–1891) in herinnering: “Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.” Een wat nuchterder opmerking in dit verband is die van Russell [12, p3]: “Since all terms that are defined are defined by means of other terms, it is clear that human knowledge must always be content to accept some terms as intelligible without definition, in order to have a starting-point for its definitions.” Een axiomatische behandeling van de natuurlijke getallen werd voor het eerst gegeven door Dedekind [3]. Hierop baseerde Peano vervolgens de nu gangbare axiomatisering PA (voor Peano Arithmetic).

Zoals de lezer aan de negatieve benamingen kan zien werden de nieuwe getallen steeds met scepsis ontvangen alvorens geaccepteerd te raken. De noodzaak van de uitbreidingen van het getalbegrip is inzichtelijk te maken door te kijken naar oplosbaarheid van vergelijkingen:

- $x + 5 = 0$ is oplosbaar in $\mathbb{Z}$, maar niet in $\mathbb{N}$.
- $3x - 2 = 0$ is oplosbaar in $\mathbb{Q}$, maar niet in $\mathbb{Z}$.
- $x^2 - 2 = 0$ is oplosbaar in $\mathbb{R}$, maar niet in $\mathbb{Q}$.
- $x^2 + 1 = 0$ is oplosbaar in $\mathbb{C}$, maar niet in $\mathbb{R}$.

De bovenstaande lijst getallenstelsels is zeker niet volledig, maar vanuit het oogpunt van het oplossen van vergelijkingen is $\mathbb{C}$ een natuurlijk punt om te stoppen, aangezien elke polynoomvergelijking in één variabele een oplossing heeft in $\mathbb{C}$. Voor een bewijs van deze zogenaamde Hoofdstelling van de Algebra verwijzen we naar het college *Complexe Functies*.

Naast de bovenstaande algebraïsche motivatie voor het uitbreiden van het getalbegrip speelde historisch ook de meetkunde een belangrijke rol. Breuken komen hierin als verhoudingen op een natuurlijke manier naar voren, en in de Griekse oudheid werden rationale verhoudingen gezien als ideaal. Echter uit dezelfde Griekse meetkunde kwam de ontdekking van irrationale verhoudingen voort, zoals de verhouding van de diagonaal van een vierkant tot zijn zijden, die volgens de stelling van Pythagoras² gelijk is aan $\sqrt{2}$. (Zie opgave 4.1.)

In de volgende paragrafen bespreken we de diverse getallenstelsels in iets meer detail. Voor een uitgebreidere behandeling, en een behandeling van andersoortige getallen zoals p-adische getallen, verwijzen we de lezer naar het boek van Keune [8].

4.2 De gehele getallen

We construeren de verzameling $\mathbb{Z}$ van gehele getallen uit die van de natuurlijke getallen $\mathbb{N}$ als volgt. We definiëren een equivalentierelatie op $\mathbb{N} \times \mathbb{N}$ door

$$(a, b) \sim (c, d) \iff a + d = b + c. \quad (6)$$

We denken hierbij aan het paar (a, b) als $a - b$. De lezer dient zelf na te gaan dat $\sim$ inderdaad een equivalentierelatie is. We definiëren $\mathbb{Z}$ als de verzameling equivalentieclassen $\mathbb{N} \times \mathbb{N} / \sim$. We geven de equivalentieklasse van het paar (a, b) aan met $\overline{(a, b)}$

We definiëren nu de optelling $+$ en vermenigvuldiging $\cdot$ op $\mathbb{Z}$ door

$$\begin{aligned} \overline{(a, b)} + \overline{(c, d)} &= \overline{(a + c, b + d)}, \\ \overline{(a, b)} \cdot \overline{(c, d)} &= \overline{(ac + bd, ad + bc)}. \end{aligned}$$

We moeten nagaan dat dit welgedefinieerd is, dat wil zeggen, dat deze definities op de equivalentieclassen $\overline{(a, b)}$ niet afhangen van de keuze van de representanten (a, b) . Hiervoor verwijzen we naar opgave 4.2.

²Pythagoras van Samos, Grieks wiskundige en theoloog, 6e eeuw v.Chr. Aristoteles vatte de leer der Pythagoreërs bondig samen met de uitspraken “de dingen zijn getallen” en het poëtische “de gehele hemel is harmonie en getal”. Hierbij zij aangemerkt dat met de term “getal” louter natuurlijke getallen en hun verhoudingen werden bedoeld, zie Dijksterhuis [4].

We hebben een natuurlijke injectie van $\mathbb{N}$ naar $\mathbb{Z}$, gegeven door $n \mapsto \overline{(n, 0)}$. We kunnen $\mathbb{N}$ dus opvatten als een deelverzameling van $\mathbb{Z}$.³ Het moge duidelijk zijn dat de optelling en vermenigvuldiging op $\mathbb{N}$ overeenkomen met die op het beeld van $\mathbb{N}$ in $\mathbb{Z}$.

4.3 De rationale getallen

We construeren nu de verzameling $\mathbb{Q}$ van rationale getallen uit die van de gehele getallen $\mathbb{Z}$. We definiëren een equivalentierelatie op paren in $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ door

$$(a, b) \sim (c, d) \iff ad = bc. \quad (7)$$

We denken hierbij aan (a, b) als de breuk $\frac{a}{b}$. De lezer dient weer zelf na te gaan dat $\sim$ inderdaad een equivalentierelatie is. We definiëren $\mathbb{Q}$ als de verzameling equivalentieclasses $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim$, en we geven de equivalentieklasse van het paar (a, b) weer aan met $\overline{(a, b)}$.

We definiëren de optelling $+$ en vermenigvuldiging $\cdot$ op $\mathbb{Q}$ door

$$\begin{aligned} \overline{(a, b)} + \overline{(c, d)} &= \overline{(ad + bc, bd)}, \\ \overline{(a, b)} \cdot \overline{(c, d)} &= \overline{(ac, bd)}. \end{aligned}$$

Net als in de constructie van $\mathbb{Z}$ moeten we weer nagaan dat dit welgedefinieerd is. Zie hiervoor opgave 4.3.

We hebben een natuurlijke inbedding van $\mathbb{Z}$ in $\mathbb{Q}$, gegeven door $n \mapsto \overline{(n, 1)}$. De optelling en vermenigvuldiging op $\mathbb{Z}$ komen weer overeen met die op het beeld van $\mathbb{Z}$ in $\mathbb{Q}$, zoals de lezer makkelijk nagaat.

4.4 De reële getallen

De constructie van de reële getallen $\mathbb{R}$ uit de rationale getallen $\mathbb{Q}$ wordt behandeld in het college Analyse 1. Het idee is om reële getallen te benaderen met rijtjes in $\mathbb{Q}$. Omdat verschillende rijtjes in $\mathbb{Q}$ hetzelfde reële getal kunnen definiëren kijken we naar equivalentieclasses van rijtjes. Formeel gaat dit als volgt: Een rij getallen $(x_n)_{n \in \mathbb{N}}$ in $\mathbb{Q}$ heet een *Cauchyrij*⁴ als er voor elke $k \in \mathbb{N}$ een $N \in \mathbb{N}$ bestaat zodat voor alle $n, m \geq N$ geldt dat $|x_n - x_m| < 2^{-k}$. In formeel-logische notatie:

$$\forall k \exists N \forall n, m \geq N (|x_n - x_m| < 2^{-k}).$$

We noemen twee Cauchyrijen (x_n) en (y_n) equivalent, notatie $(x_n) \sim (y_n)$, als

$$\forall k \exists n \forall m \geq n (|x_m - y_m| < 2^{-k}). \quad (8)$$

$\mathbb{R}$ wordt nu gedefinieerd als de verzameling van equivalentieclasses van de relatie $\sim$. Men kan nu gemakkelijk de aritmetische operaties op $\mathbb{Q}$ uitbreiden naar $\mathbb{R}$. De ordening op $\mathbb{R}$ is gedefinieerd door

$$(x_n) < (y_n) \iff \exists k \exists n \forall m \geq n (x_m < y_m - 2^{-k}).$$

Voor een nadere uitwerking van het bovenstaande verwijzen we naar het college Analyse 1, en het daarbij gebruikte boek van Tao [14]. In het bijzonder wordt daar bewezen dat $\mathbb{R}$ *volledig* is, dat wil zeggen, dat elke Cauchyrij in $\mathbb{R}$ convergeert.

³Merk op dat we in het algemeen, als $f : X \rightarrow Y$ een injectie is, X kunnen opvatten als deelverzameling van Y door X te identificeren met het beeld $f(X)$. We noemen in dat geval f ook wel een *inbedding* van X in Y .

⁴Naar de Franse wiskundige Augustin-Louis Cauchy (1789–1857).

4.5 De complexe getallen

De *complexe getallen* $\mathbb{C}$ definiëren we als de verzameling van alle objecten van de vorm $a + bi$, met $a, b \in \mathbb{R}$. Als $z = a + bi$ een complex getal is dan noemen we a het *reële deel*, en b het *imaginaire deel* van z , en noteren dit respectievelijk met $\operatorname{Re}(z) = a$ en $\operatorname{Im}(z) = b$. Complexe getallen van de vorm $0 + bi$ heten *zuiver imaginair*, en schrijven we eenvoudigweg als bi . Complexe getallen van de vorm $a + 0i$ noemen we *reëel*, en we vatten $\mathbb{R}$ op als deelverzameling van $\mathbb{C}$ middels de inbedding $x \mapsto x + 0i$.

We definiëren een optelling $+$ en een vermenigvuldiging $\cdot$ op $\mathbb{C}$ door:

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \quad (9)$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i. \quad (10)$$

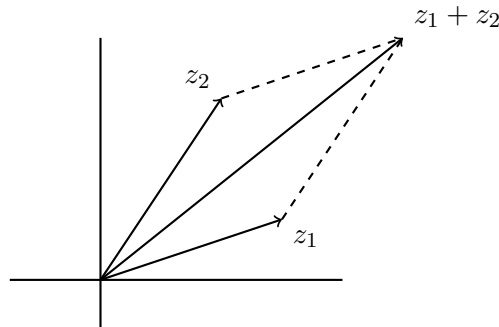
In het bijzonder zien we dat $i^2 = -1$. Met dit laatste in gedachten zien we dat de regel voor vermenigvuldiging neerkomt op uitschrijven volgens dezelfde regels als voor een gewoon product in $\mathbb{R}$. Er zijn ook inverse operaties van $+$ en $\cdot$, zie opgave 4.5.

We kunnen complexe getallen $a + bi$ in het platte vlak representeren als punten (a, b) . In dit geval noemen we de x -as de *reële as* en de y -as de *imaginaire as*. Voor $z = a + bi$ definiëren we de *absolute waarde* van z als

$$|z| = \sqrt{a^2 + b^2}.$$

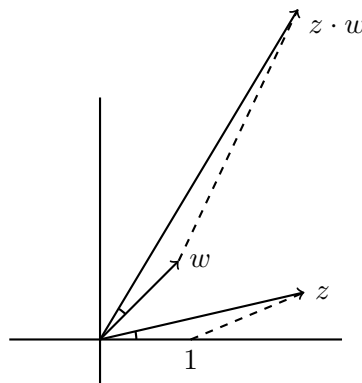
Dit komt overeen met de lengte van de vector (a, b) in $\mathbb{R}^2$.

De som van twee complexe getallen z en w kunnen we nu meetkundig interpreteren als het optellen van twee vectoren, net als in $\mathbb{R}^2$:



De juistheid van deze interpretatie volgt onmiddellijk uit de definitie (9).

Het product van twee complexe getallen z en w kunnen we als volgt meetkundig interpreteren:

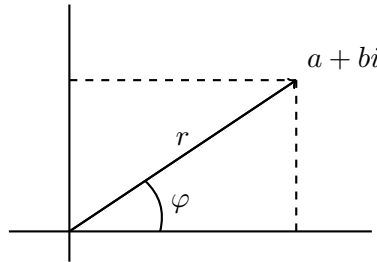


Als φ de hoek is die de vector z maakt met de positieve reële as, en ψ de hoek die w maakt met de positieve reële as, en $|z|$ en $|w|$ zijn de respectievelijke lengtes van z en w , dan is het product $z \cdot w$ de vector met hoek $\varphi + \psi$ en lengte $|z| \cdot |w|$. De correctheid van deze interpretatie is het makkelijkst in te zien met behulp van poolcoördinaten, die we nu bespreken.

Voor een complex getal $z \neq 0$ definiëren we het *argument* van z als de hoek φ die de vector z maakt met de positieve reële as. Voor $z = 0$ is het argument ongedefinieerd. Als $z = a + bi$, en we schrijven $r = |z|$, dan geldt $a = r \cos \varphi$ en $b = r \sin \varphi$, zodat we z kunnen schrijven als

$$z = r(\cos \varphi + i \sin \varphi).$$

We noemen het paar (r, φ) de *poolcoördinaten* van z .



Stel nu dat $z = r_1(\cos \varphi + i \sin \varphi)$ en $w = r_2(\cos \psi + i \sin \psi)$. Dan hebben we dat

$$\begin{aligned} z \cdot w &= r_1 r_2 ((\cos \varphi \cos \psi - \sin \varphi \sin \psi) + i(\cos \varphi \sin \psi + \sin \varphi \cos \psi)) \\ &= r_1 r_2 ((\cos(\varphi + \psi)) + i(\sin(\varphi + \psi))). \end{aligned}$$

Uit dit laatste zien we de correctheid van de boven gegeven meetkundige interpretatie van de vermenigvuldiging.

Tenslotte kunnen we machtsverheffing in $\mathbb{C}$ definiëren door

$$e^{a+bi} = e^a(\cos b + i \sin b).$$

Deze definitie kan gemotiveerd worden door bijvoorbeeld te kijken naar Taylorreeksontwikkelingen, zie het college *Complexe Functies*.⁵ Merk op dat voor $z = a + bi$ geldt dat $|e^z| = e^a$, en dat het argument van e^z gelijk is aan b . We kunnen het complexe getal met poolcoördinaten (r, φ) dus schrijven als $re^{i\varphi}$. In het bijzonder zien we dat geldt:

$$e^{\pi i} + 1 = 0.$$

Dit is wel de mooiste vergelijking uit de wiskunde genoemd; hij bevat op de meest beknopte manier de belangrijkste constanten en de elementaire operaties optellen, vermenigvuldigen, en machtsverheffen.

Opgaven

Opgave 4.1. Laat zien dat $\sqrt{2} \notin \mathbb{Q}$. (Hint: stel $\sqrt{2} = \frac{n}{m}$, met $n, m \in \mathbb{N}$. Kwadrateer en tel het aantal factoren 2.)

Opgave 4.2. (a) Ga na dat de operaties $+$ en $\cdot$ op $\mathbb{Z}$ welgedefinieerd zijn.

(b) Laat zien hoe de operatie $-$ op $\mathbb{Z}$ gedefinieerd kan worden.

⁵De definitie van e^z en de motivatie ervan met machtreksen stammen van de Zwitserse wiskundige Leonhard Euler (1707–1783), zie Stillwell [13, p315].

Opgave 4.3. (a) Ga na dat de operaties $+$ en $\cdot$ op $\mathbb{Q}$ welgedefinieerd zijn.
 (b) Laat zien hoe de operatie $1/q$ op $\mathbb{Q}$ gedefinieerd kan worden.

Opgave 4.4. Ga na dat de relatie $\sim$ gedefinieerd in (8) een equivalentierelatie is.

Opgave 4.5. In deze opgave laten we zien dat we ook kunnen aftrekken en delen in $\mathbb{C}$. Stel dat $z = a + bi$.

(a) Ga na dat voor $-z = -a - bi$ geldt dat $z + (-z) = 0$. In plaats van $z + (-w)$ schrijven we gewoon $z - w$.

(b) Stel nu dat $|z| \neq 0$. Ga na dat geldt

$$(a + bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \right) = 1.$$

Dus elk complex getal $z \neq 0$ heeft een multiplicatieve inverse, die we aangeven met $1/z$.

(c) Ga na dat geldt

$$\frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.$$

Opgave 4.6. Laat $z, w \in \mathbb{C}$. Bewijs de volgende eigenschappen van de absolute waarde:

- (i) $|z \cdot w| = |z| \cdot |w|$.
- (ii) $\left| \frac{z}{w} \right| = \frac{|z|}{|w|}$.
- (iii) $|z^n| = |z|^n$ voor alle $n \in \mathbb{N}$.
- (iv) $|z + w| \leq |z| + |w|$ (driehoeksongelijkheid).

Opgave 4.7. De *complex geconjugeerde* van een complex getal $z = a + bi$ is het getal $\bar{z} = a - bi$. Meetkundig is dit de vector verkregen uit z door te spiegelen in de reële as. Bewijs de volgende identiteiten:

- (i) $|\bar{z}| = |z|$.
- (ii) $z \cdot \bar{z} = z^2$.
- (iii) $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$.

Hoofdstuk 5

Inductie

To be a good mathematician, or a good gambler, or good at anything, you must be a good guesser. In order to be a good guesser, you should be, I would think, naturally clever to begin with.

G. Polya [10, p111].

5.1 Volledige inductie

Voor de natuurlijke getallen $\mathbb{N}$ geldt het volgende principe:

Volledige inductie. *Stel dat P een deelverzameling is van $\mathbb{N}$ waarvoor geldt:*

- (i) $0 \in P$.
- (ii) *Voor alle $n \in \mathbb{N}$, als $n \in P$ dan ook $n + 1 \in P$.*

Dan geldt $P = \mathbb{N}$.

Het principe van volledige inductie is geen stelling, maar een axioma over de natuurlijke getallen. Het stelt ons in staat om dingen te bewijzen volgens het volgende schema: Stel dat we een uitspraak willen bewijzen van de vorm $\forall n \in \mathbb{N} \varphi(n)$. Dan is het voldoende om te bewijzen dat

- (i) $\varphi(0)$,
- (ii) $\forall n (\varphi(n) \rightarrow \varphi(n + 1))$.

Namelijk, door het principe van volledige inductie toe te passen op de verzameling $P = \{n \mid \varphi(n)\}$ volgt hieruit dat $\forall n \in \mathbb{N} \varphi(n)$. Een bewijs van deze vorm heet een *bewijs met volledige inductie*, en dit is een van de meest voorkomende bewijsvormen in de wiskunde. Stap (i) heet de *basis* van de inductie, en stap (ii) heet de *inductiestap*. In de inductiestap bewijzen we $\varphi(n + 1)$ uit de aanname $\varphi(n)$. Deze aanname $\varphi(n)$ heet de *inductiehypothese*. Als voorbeeld bewijzen we het volgende:¹

Propositie 5.1.1. *Voor alle $n \in \mathbb{N}$ geldt*

$$\sum_{i=0}^n i = \frac{1}{2}n(n+1). \quad (11)$$

¹Volgens een bekende anekdote kreeg de Duitse wiskundige Carl Friedrich Gauss (1777–1855) als schooljongen de opdracht om de som $1 + 2 + 3 + \dots + 100$ uit te rekenen. In luttele seconden kwam hij tot het juiste antwoord, kennelijk door de formule (11) in te zien. De anekdote kent vele varianten; zie ook het vlot geschreven, maar nogal onbetrouwbare boek van Bell [1].

Bewijs. We bewijzen dit met volledige inductie.

Basis: Voor $n = 0$ is zowel het linker- als het rechterlid van (11) gelijk aan nul, dus geldt de formule.

Inductiestap: De inductiehypothese is dat de formule (11) geldt voor n , en we moeten nu bewijzen dat hij geldt voor $n + 1$. We hebben:

$$\begin{aligned} \sum_{i=0}^{n+1} i &= \sum_{i=0}^n i + (n+1) \\ &= \frac{1}{2}n(n+1) + (n+1) && \text{(wegens de inductiehypothese)} \\ &= \frac{1}{2}(n+1)(n+2). \end{aligned}$$

Dit besluit de inductiestap, en daarmee het inductiebewijs. $\square$

Allerlei variaties van het bewijs met inductie zijn mogelijk. Zo kunnen we uitspraken van de vorm $\forall n \geq m(\varphi(n))$ bewijzen door als basis van de inductie $n = m$ te nemen, in plaats van $n = 0$ (zie opgave 5.3). Een andere variant wordt besproken in opgave 5.10.

5.2 Binomiaalcoëfficiënten

Voor elke $n \in \mathbb{N}$ is de uitdrukking $n!$ (uitgesproken als “*n faculteit*”) gedefinieerd als

$$n! = 1 \cdot 2 \cdot \dots \cdot n.$$

Voor $n = 0$ definiëren we $0! = 1$.

Een *permutatie* van $\{1, \dots, n\}$ is een bijectieve afbeelding van $\{1, \dots, n\}$ naar $\{1, \dots, n\}$. Voor een gegeven n geven we de verzameling permutaties van $\{1, \dots, n\}$ aan met S_n .

Propositie 5.2.1. *Voor elke $n \geq 1$ geldt $|S_n| = n!$.*

Bewijs. We bewijzen dit met inductie naar n . Voor $n = 1$ geldt de bewering, want $1! = 1$. Stel nu dat $|S_n| = n!$; we bewijzen dat $|S_{n+1}| = (n+1)!$. Als f een permutatie is van $\{1, \dots, n+1\}$, dan zijn er $n+1$ mogelijkheden voor $f(n+1)$. Voor elke keuze van $f(n+1)$ is de beperking van f tot $\{1, \dots, n\}$ een bijectie tussen twee verzamelingen met n elementen. Wegens de inductiehypothese zijn er hiervan $n!$,² dus in totaal zijn er $(n+1)n! = (n+1)!$ mogelijkheden voor f . $\square$

Laat nu n en k getallen zijn in $\mathbb{N}$ met $n \geq k$. Dan definiëren we

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

We spreken $\binom{n}{k}$ uit als “ n boven k ” (Engels: “ n choose k ”); dit getal is gelijk aan het aantal manieren om k elementen uit een verzameling van n elementen te kiezen, zie Propositie 5.2.3. De getallen $\binom{n}{k}$ heten *binomiaalcoëfficiënten* wegens Stelling 5.2.4.

Propositie 5.2.2. (De regel van Pascal)³ *Voor elke $n > k > 0$ geldt*

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

²Het is makkelijk in te zien dat de aanname $|S_n| = n!$ equivalent is met de bewering dat er $n!$ bijecties zijn tussen elke twee verzamelingen met n elementen.

³Naar de Franse filosoof en wiskundige Blaise Pascal (1623–1662).

Bewijs. Uitschrijven van de definitie geeft

$$\begin{aligned} \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} &= \frac{k(n-1)! + (n-k)(n-1)!}{k!(n-k)!} \\ &= \frac{n!}{k!(n-k)!} \end{aligned} \quad \square$$

Propositie 5.2.2 geeft het volgende plaatje van de binomiaalcoëfficiënten, de zogenaamde driehoek van Pascal.⁴

$$\begin{array}{ccccccc} & & & & 1 & & \\ & & & & & & \\ & & & 1 & & 1 & \\ & & & & & & \\ & & 1 & & 2 & & 1 \\ & & & & & & \\ & 1 & & 3 & & 3 & & 1 \\ & & & & & & \\ & 1 & & 4 & & 6 & & 4 & & 1 \\ & & & & & & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \end{array}$$

Bovenaan staat $\binom{0}{0}$, en de n -de rij begint met $\binom{n}{0}$ en eindigt met $\binom{n}{n}$. Verder is elke binomiaalcoëfficiënt steeds de som van de twee erboven, zoals voorgeschreven door de vergelijking in Propositie 5.2.2. Dit geeft tevens een snelle recursieve procedure om deze coëfficiënten te berekenen. In het bijzonder zien we ook dat $\binom{n}{k}$ een geheel getal is voor alle n en k .

Propositie 5.2.3. *Zij $n \in \mathbb{N}$, en laat X een verzameling zijn met n elementen. Dan geldt voor alle $0 \leq k \leq n$,*

$$\binom{n}{k} = |\{A \subseteq X : |A| = k\}|.$$

Bewijs. Met inductie naar n . Voor $n = 0$ klopt de bewering want $\binom{0}{0} = 1$, en er is maar één lege verzameling. Stel nu dat de bewering geldt voor $n - 1$, en zij X een verzameling met n elementen. We bewijzen dat de uitspraak geldt voor X . Neem $x \in X$ vast. Dan zijn er voor elke $A \subseteq X$ twee mogelijkheden: $x \in A$ of $x \notin A$. We tellen nu de A met k elementen als volgt. Voor de A met $x \in A$ hebben we een keuze van $k - 1$ elementen uit $X - \{x\}$, en wegens de inductiehypothese zijn er hier $\binom{n-1}{k-1}$ van. Voor de A met $x \notin A$ hebben we een keuze van k elementen uit $X - \{x\}$, en wegens de inductiehypothese is hun aantal $\binom{n-1}{k}$. Samen geeft dit, gebruik makend van Propositie 5.2.2, $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$ verzamelingen A met k elementen. $\square$

We bewijzen nu het binomium van Newton,⁵ waaraan de binomiaalcoëfficiënten hun naam te danken hebben.

Stelling 5.2.4. (Binomium van Newton) *Voor alle $a, b \in \mathbb{R}$ en $n \in \mathbb{N}$ geldt*

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

⁴De driehoek was reeds ver voor Pascal bekend in de Indiase oudheid, alsook later in China, Perzië, en Europa, maar Pascal gaf de eerste toepassingen ervan in zijn *Traité du triangle arithmétique* (1653). Dit boek is overigens ook de plaats waar het principe van volledige inductie voor het eerst expliciet is beschreven.

⁵Naar de Britse wis- en natuurkundige Isaac Newton (1642–1727).

Bewijs. Met inductie naar n . Voor $n = 0$ geldt de vergelijking, want $\binom{0}{0} = 1$. We bewijzen dat de vergelijking geldt voor $n + 1$, aannemende dat hij geldt voor n . Wegens de inductiehypothese hebben we

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

In de laatste stap gebruiken we dat $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$, en dat $\binom{n}{0} = \binom{n+1}{0}$ en $\binom{n}{n} = \binom{n+1}{n+1}$. $\square$

5.3 Formule-inductie

Naast bewijzen met inductie bestaan er ook inductieve definities. Ter illustratie beschouwen we de verzameling van propositieformules. Deze kunnen we formeel definiëren als volgt:

- (i) Elke propositionele variabele p is een formule.
- (ii) Als φ en ψ formules zijn, dan zijn ook $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, en $\varphi \rightarrow \psi$ formules.

Punt (i) van deze definitie vormt de basis van de definitie, en punt (ii) fungeert als inductiestap. Samen geven (i) en (ii) een manier om de verzameling van formules van onder af aan op te bouwen.⁶ Een definitie van deze vorm heet een *inductieve definitie*. We kunnen over verzamelingen die inductief zijn gedefinieerd dingen bewijzen met inductie. Als we bijvoorbeeld een eigenschap van formules willen bewijzen volstaat het om (i) te bewijzen dat alle variabelen deze eigenschap hebben (dit is de basis van de inductie), en (ii) dat als φ en ψ de eigenschap hebben (dit is de inductiehypothese), dat dit dan ook geldt voor de samenstellingen $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, en $\varphi \rightarrow \psi$. We hebben in dit geval dus een inductiestap voor elk connectief! Als voorbeeld bewijzen we:

Propositie 5.3.1. *Voor elke propositionele formule bestaat er een equivalente formule die alleen de connectieven $\neg$ en $\vee$ bevat.*

Bewijs. We bewijzen met formule-inductie dat de uitspraak geldt voor een willekeurige formule χ . De uitspraak is evident waar als χ uit slechts een enkele variabele bestaat. Dit is de inductiebasis. Voor de inductiestap nemen we aan dat φ en ψ formules zijn die alleen $\neg$ en $\vee$ bevatten. Het is evident dat dit dan ook geldt voor $\chi = \neg\varphi$ en $\chi = \varphi \vee \psi$, dus we hoeven alleen nog de inductiestap voor $\varphi \wedge \psi$ en $\varphi \rightarrow \psi$ te behandelen. Stel $\chi = \varphi \wedge \psi$. Dan geldt dat χ equivalent is met $\neg(\neg\varphi \vee \neg\psi)$, en deze laatste formule heeft weer de gewenste eigenschap wegens de inductiehypothese. Stel tenslotte dat $\chi = \varphi \rightarrow \psi$. Dan is χ equivalent met $\neg\varphi \vee \psi$, en deze formule heeft weer de gewenste eigenschap. $\square$

⁶Een alternatieve manier om de verzameling propositieformules “van boven af” te definiëren is om te zeggen dat het de *kleinste* verzameling is die (i) alle propositionele variabelen bevat, en (ii) afgesloten is onder de operaties $\neg$, $\wedge$, $\vee$, en $\rightarrow$.

We kunnen ook een inductieve definitie geven van de verzameling formules in de predikaatlogica (opgave 5.12), en we hebben dus weer de mogelijkheid om eigenschappen van deze verzameling formules met inductie te bewijzen. Zo kunnen we bijvoorbeeld met inductie bewijzen (opgave 5.14) dat elke predikaatlogische formule equivalent is met een formule in *prenex-normaalvorm*:

$$Q_1x_1Q_2x_2\ldots Q_nx_n(\varphi(x_1,\ldots,x_n)).$$

Hier is elke Q_i een kwantor, $\forall$ of $\exists$, en is de formule φ kwantorvrij. De rij kwantoren aan het begin heet de *prenex* van de formule, en φ de *matrix*.

5.4 Recursie

Recursie en inductie worden vaak in één adem genoemd, en zijn dan ook nauw verwant. Een functie $f : \mathbb{N} \rightarrow \mathbb{N}$ is *recursief* gedefinieerd als de waarde $f(n+1)$ gedefinieerd is in termen van $f(n)$, of, algemener, in termen van $f(m)$ met $m < n$. Een voorbeeld is de rij van Fibonacci:⁷

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \dots$$

Elk getal in de rij wordt verkregen door de som van de twee voorafgaande getallen te nemen: $F(n+2) = F(n+1) + F(n)$, en om de rij te beginnen hebben we $F(0) = 1$ en $F(1) = 1$.

Een ander bekend voorbeeld zijn de recursieve definities van Grassmann⁸ van de optelling en vermenigvuldiging op $\mathbb{N}$:

$$\begin{array}{ll} x + 0 = x & x \cdot 0 = 0 \\ x + (y + 1) = (x + y) + 1 & x \cdot (y + 1) = (x \cdot y) + x. \end{array}$$

De eerste recursie definieert $x + y$ in termen van de operatie $S(x) = x + 1$, en de tweede recursie definieert $x \cdot y$ in termen van de optelling.

In het algemeen hebben we het volgende schema van *primitieve recursie*.

Propositie 5.4.1. (Dedekind [3]) *Gegeven functies $g : \mathbb{N}^n \rightarrow \mathbb{N}$ en $h : \mathbb{N}^{n+2} \rightarrow \mathbb{N}$ bestaat er een unieke functie $f : \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ zodat*

$$\begin{aligned} f(0, \vec{y}) &= g(\vec{y}), \\ f(x+1, \vec{y}) &= h(f(x, \vec{y}), x, \vec{y}). \end{aligned}$$

voor alle $x \in \mathbb{N}$ en $\vec{y} \in \mathbb{N}^n$.

Bewijs. Uniciteit: Stel dat f_0 en f_1 verschillende functies zijn die beide voldoen aan het gegeven schema, en stel dat $x \in \mathbb{N}$ het kleinste getal is zodat $f_0(x, \vec{y}) \neq f_1(x, \vec{y})$ voor zekere $\vec{y}$. Als $x = 0$ dan geldt $f_0(x, \vec{y}) = g(\vec{y}) = f_1(x, \vec{y})$, dus moet gelden dat $x > 0$, zeg $x = z + 1$. Maar dan

$$f_0(z+1, \vec{y}) = h(f_0(z, \vec{y}), z, \vec{y}) = h(f_1(z, \vec{y}), z, \vec{y}) = f_1(z+1, \vec{y}),$$

⁷Naar de Italiaanse wiskundige Leonardo van Pisa (ca.1170 – ca.1250), bekend onder de naam Fibonacci. De rij van Fibonacci komt in de natuur veelvuldig voor, en is verder onder meer beroemd vanwege de relatie met de gulden snede, zie de illustratie op de voorzijde. De lengtes van de zijden van de vierkanten in deze illustratie volgen, van binnen naar buiten, de rij van Fibonacci, en de spiraal is opgebouwd door in elk vierkant een cirkelboog te tekenen die de hoeken verbindt.

⁸Hermann Grassmann, Duits wiskundige en linguïst (1809–1877). De recursieve definities zijn uit het *Lehrbuch der Arithmetik* (1861).

een tegenspraak.

Existentie: We bewijzen met inductie naar x dat er een functie f bestaat die voor alle getallen tot en met x en alle $\vec{y}$ voldoet aan het gegeven schema. Voor $x = 0$ kunnen we nemen $f(0, \vec{y}) = g(\vec{y})$ voor alle $\vec{y}$. Stel nu (inductiehypothese) dat f voor alle getallen tot en met x en alle $\vec{y}$ voldoet. Als we nu definiëren $f(x+1, \vec{y}) = h(f(x, \vec{y}), x, \vec{y})$ voor alle $\vec{y}$, dan voldoet f voor alle getallen tot en met $x+1$ aan het schema. Met inductie volgt nu dat er een f bestaat die voor alle x aan het schema voldoet. $\square$

Merk op dat het recursieschema uit Propositie 5.4.1 ook zin heeft voor $n = 0$: De functie g moet dan gelezen worden als een constante.

Definitie 5.4.2. Definieer de volgende basisfuncties:

- de constante 0 (opgevat als functie zonder argumenten),
- de opvolgerfunctie $S(x) = x + 1$,
- de projectiefuncties $\pi_i^n : \mathbb{N}^n \rightarrow \mathbb{N}$ gedefinieerd door $\pi_i^n(x_1, \dots, x_n) = x_i$.

Een functie $f : \mathbb{N}^n \rightarrow \mathbb{N}$ heet *primitief recursief* als hij verkregen kan worden uit de basisfuncties door eindig veel toepassingen van het schema van primitieve recursie en het samenstellen van functies.⁹

Naast de optelling en vermenigvuldiging zijn veel andere aritmetische operaties op $\mathbb{N}$, zoals machtsverheffen en de faculteetsfunctie, primitief recursief, zie opgaven 5.15 en 5.16. Hoewel het n -de Fibonacci-getal $F(n)$ gedefinieerd is met behulp van de *twee* voorgangers $F(n-1)$ en $F(n-2)$, in plaats van alleen met $F(n-1)$, is deze rij toch ook primitief recursief, zie opgave 5.17.

Opgaven

Opgave 5.1. Bewijs dat voor alle $n \in \mathbb{N}$ geldt dat

$$\sum_{k=0}^n k^2 = \frac{1}{6}n(n+1)(2n+1).$$

Opgave 5.2. Bewijs dat voor elke $n \in \mathbb{N}$ en elke $r \neq 1$ geldt dat

$$\sum_{i=0}^n r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Dit is de zogenaamde *meetkundige reeks*, en het getal r heet de *reden*.

Opgave 5.3. Stel dat $m \in \mathbb{N}$, en dat P een deelverzameling is van $\mathbb{N}$ waarvoor geldt:

- $m \in P$.
- Voor alle $n \in \mathbb{N}$, als $n \in P$ dan ook $n+1 \in P$.

Bewijs met inductie dat geldt $\forall n \geq m (n \in P)$.

⁹De primitief recursieve functies spelen onder andere een belangrijke rol in het bewijs van Gödels onvolledigheidsstellingen. Dit werk was tevens de aanzet tot de *recursietheorie*, tegenwoordig in het Engels meestal aangeduid als *Computability Theory*.

Opgave 5.4. Beschouw de rij $a, a + v, a + 2v, \dots$, waarvan de k -de term gelijk is aan $a + (k - 1)v$. Dit is de zogenaamde *rekenkundige reeks* met verschil v . Bewijs dat voor elke $n \geq 1$ geldt:

$$\sum_{k=1}^n (a + (k - 1)v) = \frac{1}{2}n(2a + (n - 1)v).$$

Opgave 5.5. (a) Bewijs dat $\sum_{k=0}^n \binom{n}{k} = 2^n$ voor alle $n \in \mathbb{N}$.

(b) Bewijs dat $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$ voor alle $n \geq 1$.

Opgave 5.6. Bewijs voor alle $n \in \mathbb{N}$ en elke reële $a \geq -1$ de volgende *ongelijkheid van Bernoulli*:¹⁰

$$(1 + a)^n \geq 1 + na.$$

Opgave 5.7. Bewijs dat voor elke $n \geq 1$ de n -de afgeleide van de functie $f(x) = \ln x$ gelijk is aan

$$\frac{(-1)^{n-1}(n-1)!}{x^n}.$$

Opgave 5.8. Laat twee n -maal differentieerbare functies f en g gegeven zijn. Geef de n -de afgeleide van f aan met $f^{(n)}$. Bewijs de *regel van Leibniz*:¹¹

$$(f \cdot g)^{(n)} = \sum_{k=0}^n \binom{n}{k} f^{(n-k)} g^{(k)}.$$

Opgave 5.9.* Bewijs dat voor elke $n \geq 6$,

$$\frac{n^n}{3^n} < n! < \frac{n^n}{2^n}.$$

Opgave 5.10. Beschouw de volgende variant van het principe van volledige inductie:

Stel dat P een deelverzameling is van $\mathbb{N}$ waarvoor geldt: Voor alle $n \in \mathbb{N}$, als $\forall m < n (m \in P)$ dan ook $n \in P$. Dan geldt $P = \mathbb{N}$.

Bewijs de geldigheid van dit principe met volledige inductie.

Opgave 5.11. (a) Het *inclusie-exclusie-principe* voor twee eindige verzamelingen A en B zegt dat

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Bewijs dit.

(b) Bewijs dat voor elk drietal eindige verzamelingen A , B , en C geldt dat

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

(c) Laat $I = \{1, \dots, n\}$ een eindige indexverzameling zijn, en A_i een eindige verzameling voor elke $i \in I$. Bewijs de volgende algemene vorm van het inclusie-exclusie-principe met inductie naar $n = |I|$:

$$\left| \bigcup_{i \in I} A_i \right| = \sum_{J \subseteq I, J \neq \emptyset} (-1)^{|J|+1} \left| \bigcap_{j \in J} A_j \right|.$$

¹⁰Naar de Zwitserse wiskundige Jacob Bernoulli (1655–1705).

¹¹Gottfried Wilhelm von Leibniz (1646–1716), Duits wiskundige en filosoof.

Opgave 5.12. Geef een inductieve definitie van de verzameling formules in de predikaatlogica.

Opgave 5.13.* Bewijs met inductie dat elke propositionele formule geschreven kan worden in de vorm

$$\bigwedge_i \bigvee_j a_{ij}$$

waarbij elke a_{ij} hetzij een variabele, hetzij de negatie van een variabele is. Dit is de zogeheten *conjunctieve normaalvorm* van een formule.

Opgave 5.14. Bewijs met inductie dat elke predikaatlogische formule geschreven kan worden in prenex-normaalvorm.

Opgave 5.15. Bewijs dat $+$ en $\cdot$ primitief recursief zijn

Opgave 5.16. (a) Bewijs dat de functie $n \mapsto n!$ primitief recursief is.

(b) Bewijs dat de functie $(m, n) \mapsto m^n$ primitief recursief is.

Opgave 5.17.* Bewijs dat de functie $n \mapsto F(n)$, waar $F(n)$ het n -de Fibonacci-getal is, primitief recursief is. (Voor deze opgave is een primitief recursieve paringsfunctie $(x, y) \mapsto \langle x, y \rangle$ van $\mathbb{N}^2$ naar $\mathbb{N}$ nodig, met primitief recursieve inversen $\pi_0(\langle x, y \rangle) = x$ en $\pi_1(\langle x, y \rangle) = y$. Zie ook opgave 6.6.)

Hoofdstuk 6

Kardinaliteit

Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können.

D. Hilbert, Über das Unendliche, 1926.

6.1 Gelijkmachtigheid

Op de lagere school leren we tellen met de elementen van $\mathbb{N} = \{0, 1, 2, \dots\}$. In een fruitschaal liggen bijvoorbeeld evenveel appels als peren als hun *aantal* gelijk is. Er is echter nog een meer elementaire manier van tellen, die het voordeel heeft ook te werken voor oneindige verzamelingen. Als we bij elke appel in de schaal precies één peer kunnen aanwijzen dan weten we ook dat hun aantal gelijk is, ook als we niet weten hoe groot dat aantal is.¹ Met andere woorden, de aantallen appels en peren zijn gelijk als er een *bijjectie* bestaat tussen de twee verzamelingen. De Duitse wiskundige Georg Cantor zag in dat dit idee ook toegepast kon worden op oneindige verzamelingen, en analyseerde als eerste systematisch de grootte van oneindige verzamelingen. Hij werd hiertoe aangezet door problemen in de analyse waaraan hij werkte.²

Galileo Galilei³ merkte in zijn (door de inquisitie verboden) hoofdwerk [6] reeds op dat, hoewel niet alle natuurlijke getallen een kwadraat zijn, de verzameling kwadraten in één-één-correspondentie te brengen is met de verzameling van alle natuurlijke getallen. Deze paradoxale situatie wordt uiteengezet in een mooie dialoog tussen Simplicio, Sagredo, en Salviati [6, p32, 33]. De conclusie is dat begrippen als even groot, groter, en kleiner, zin hebben voor eindige verzamelingen, maar niet voor oneindige. De theorie van Cantor zal ons echter in het hiernavolgende laten zien dat deze begrippen wel degelijk zin hebben voor oneindige verzamelingen, en dat het begrip één-één-correspondentie daartoe precies de sleutel is.

¹Uit psychologisch onderzoek (bijvoorbeeld het werk van Karen Wynn) is bekend dat zeer jonge kinderen reeds in het bezit zijn van intuïties over aantallen: Hun aandacht blijft langer gevangen door twee groepjes objecten die verschillen in aantal dan door gelijke groepjes. Dit is in overeenstemming met de ideeën van de Nederlandse wiskundige L. E. J. Brouwer (1881–1966), volgens wie wiskundige intuïtie voortalg is.

²Georg Cantor (1845–1918). Cantors wiskundige odyssee is op een zeer gedegen manier beschreven in de biografie van Dauben [2]. Bijna even legendarisch als Cantors bijdragen is de tegenwerking die hij daarbij ondervond, onder andere van gevestigde wiskundigen als Poincaré en Kronecker. Volgens deze laatste was Cantor zelfs een charlatan en een bederver van de jeugd [2, p1]. Hier stonden dan weer de lovende woorden van Dedekind, en later ook Hilbert en Russell, tegenover.

³Galileo Galilei (1564–1642). Aartsvader van de moderne wetenschap.

Definitie 6.1.1. Een verzameling A heet *gelijkmachtig* met een verzameling B als er een bijectie is van A naar B . Notatie: $A \sim B$. In dit geval zeggen we ook dat A en B dezelfde *kardinaliteit* hebben. We schrijven $A \leq B$ als er een injectie is van A naar B , en $A < B$ als $A \leq B$ maar niet $A \sim B$. A heet *eindig* als er een $n \in \mathbb{N}$ is zodat $A \sim \{1, \dots, n\}$. We noemen een verzameling *oneindig* als hij niet eindig is.

Merk op dat voor eindige verzamelingen geldt dat $A \sim B$ dan en slechts dan als $|A| = |B|$. We gebruiken deze laatste schrijfwijze ook wel voor oneindige verzamelingen, hoewel we hier moeten oppassen omdat aan de notatie $|A|$ buiten deze context nog geen betekenis is toegekend.⁴ Voorlopig is $|A| = |B|$ dus louter op te vatten als alternatieve schrijfwijze voor $A \sim B$.

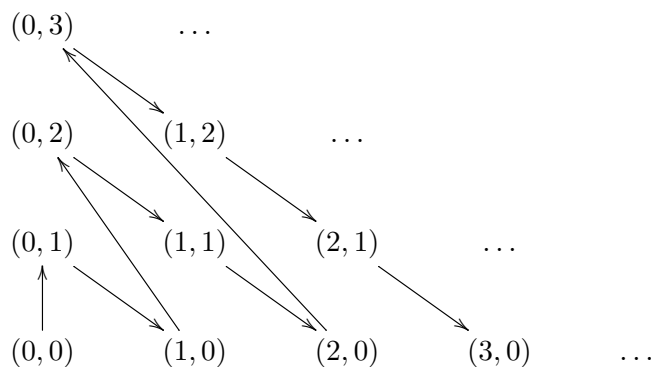
6.2 Aftelbare verzamelingen

Laat $E = \{2n : n \in \mathbb{N}\}$ de verzameling even getallen zijn. Ofschoon E een echte deelverzameling is van $\mathbb{N}$ geldt $E \sim \mathbb{N}$.⁵ Het volgende plaatje maakt in één oogopslag duidelijk dat er een bijectie is tussen E en $\mathbb{N}$:

0	1	2	3	4	5	6	...
0	2	4	6	8	10	12	...

Op soortgelijke wijze volgt dat $\mathbb{N} \sim \mathbb{Z}$ (opgave 6.4). Dus hoewel $\mathbb{Z} \setminus \mathbb{N}$ oneindig veel elementen bevat zijn deze verzamelingen toch even groot.

Beschouw nu de verzameling $\mathbb{N} \times \mathbb{N}$ van alle paren natuurlijke getallen (n, m) . Voor elke eerste coördinaat n zijn er oneindig veel mogelijke tweede coördinaten m mogelijk, dus $\mathbb{N} \times \mathbb{N}$ bestaat in zekere zin uit oneindig veel kopieën van $\mathbb{N}$. Toch zijn ook deze verzamelingen even groot! We maken een bijectie als volgt:



We kunnen deze paringsfunctie van $\mathbb{N} \times \mathbb{N}$ naar $\mathbb{N}$ expliciet definiëren door

$$\frac{1}{2}((x+y+1)^2 - (x+y+1)) + x = \frac{1}{2}((x+y)^2 + 3x + y), \quad (12)$$

zie opgave 6.6.

Op soortgelijke manier kunnen we laten zien dat $\mathbb{Q} \sim \mathbb{N}$ (opgave 6.10). We hebben dus

$$\mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{Q}.$$

Er zijn dus evenveel natuurlijke getallen als breuken!

⁴De moeilijkheid om de kardinaliteit $|A|$ van een verzameling A in het algemeen te definiëren is van dezelfde soort als de problemen die optreden bij het definiëren van het begrip verzameling.

⁵We zien hier dat het adagium van de oude Grieken “het geheel is groter dan het deel” niet opgaat.

Definitie 6.2.1. Een verzameling heet *aftelbaar* als hij eindig is of gelijkmachting met $\mathbb{N}$. In het laatste geval heet hij *aftelbaar oneindig*.

De naam “aftelbaar” wordt wellicht het best geïllustreerd door formulering (iii) in de volgende stelling: We kunnen aan een surjectie $f : \mathbb{N} \rightarrow A$ denken als een aftelling, mogelijk met herhalingen, van de elementen van A .

Stelling 6.2.2. *De volgende uitspraken zijn equivalent:*

- (i) A is aftelbaar.
- (ii) $A \leq \mathbb{N}$.
- (iii) $A = \emptyset$ of er is een surjectie $f : \mathbb{N} \rightarrow A$.

Bewijs. (i) $\Rightarrow$ (ii). Dit is triviaal.

(ii) $\Rightarrow$ (iii). Stel dat $g : A \rightarrow \mathbb{N}$ injectief is en dat $A \neq \emptyset$, zeg $a \in A$. Definieer een surjectie $f : \mathbb{N} \rightarrow A$ als volgt. Voor elke $n \in \mathbb{N}$ met $n \in g(A)$, definieer $f(n)$ als het unieke element $b \in A$ met $g(b) = n$. Als $n \notin g(A)$, laat $f(n) = a$. Dan is f surjectief, want als $b \in A$ dan $f(g(b)) = b$.

(iii) $\Rightarrow$ (i). Stel dat $f : \mathbb{N} \rightarrow A$ surjectief is, en dat A oneindig is. We definiëren een bijectie $g : A \rightarrow \mathbb{N}$. Merk op dat

$$A = \{f(n) : n \in \mathbb{N}\},$$

dus het is voldoende om $g(f(n))$ te definiëren voor elke n . Definieer $g(f(0)) = 0$. Stel nu $n > 0$, en stel dat we $g(f(m))$ reeds gedefinieerd hebben voor alle $m < n$. Als $f(n) = f(m)$ voor een $m < n$ dan is $g(f(n)) = g(f(m))$ al gedefinieerd. Anders definiëren we $g(f(n))$ als het kleinste element in

$$\mathbb{N} \setminus \{g(f(0)), \dots, g(f(n-1))\}.$$

Merk op dat deze verzameling niet-leeg is omdat $\mathbb{N}$ oneindig is. De functie g aldus gedefinieerd is injectief: Het is duidelijk uit de definitie dat als $g(f(n)) = g(f(m))$ dat dan $f(n) = f(m)$. Stel voor het bewijs van de surjectiviteit van g dat $m \notin g(A)$. Dan geldt dat voor alle $n \in \mathbb{N}$ dat $g(f(n)) \in \{0, \dots, m-1\}$, dus g is een injectie van A naar een eindige verzameling, dus A is eindig, in tegenspraak met de aanname. $\square$

We hebben gezien dat $\mathbb{N}$, $\mathbb{Z}$, en $\mathbb{Q}$ alle aftelbaar zijn. Op dit punt gekomen begint bij de lezer wellicht het vermoeden te rijzen dat dat alle oneindige verzamelingen even groot zijn als $\mathbb{N}$. We zullen nu echter zien dat dit niet zo is.

6.3 Overaftelbare verzamelingen

Definitie 6.3.1. Een oneindige verzameling die niet aftelbaar is heet *overaftelbaar*.

We bewijzen nu een van de beroemdste stellingen over oneindigheid. De gevolgde bewijsmethode is bijna nog belangrijker dan de stelling zelf, en heeft talloze andere toepassingen in de wiskunde gevonden.

Stelling 6.3.2. (Cantor) $\mathbb{R} > \mathbb{N}$, dat wil zeggen, $\mathbb{R}$ is overaftelbaar.

Bewijs. Het is voldoende om te bewijzen dat de verzameling $2^{\mathbb{N}}$ van alle oneindige binaire rijtjes overaftelbaar is. Immers, elke binaire rij $x : \mathbb{N} \rightarrow \{0, 1\}$ definieert een uniek reëel getal, namelijk het getal dat als k -de element van de decimale ontwikkeling $x(k)$ heeft. Gegeven een aftelbaar oneindige lijst van binaire rijen construeren we een binaire rij die niet op de lijst voorkomt. Dit bewijst dat elke aftelling van $2^{\mathbb{N}}$, en dus ook van $\mathbb{R}$, onvolledig is. Zij dus x_i , met $i \in \mathbb{N}$, een aftelbare rij elementen uit $2^{\mathbb{N}}$. We construeren $y \in 2^{\mathbb{N}}$ zodat $y \neq x_i$ voor alle $i \in \mathbb{N}$ als volgt. Laat $x_i(j)$ het j -de getal zijn in het rijtje x_i . Definieer het i -de getal $y(i)$ van y door

$$y(i) = 1 - x_i(i).$$

Dan is y een binaire rij met $y \neq x_i$ voor elke i , hetgeen is wat we wilden bewijzen. $\square$

Als we de rijtjes x_i in het bewijs van Stelling 6.3.2 als volgt onder elkaar schrijven,

$$\begin{array}{ccccccc} x_0(0) & & x_0(1) & & x_0(2) & & x_0(3) & & \dots \\ & \searrow & & & & & & & \\ x_1(0) & & x_1(1) & & x_1(2) & & x_1(3) & & \dots \\ & & \searrow & & & & & & \\ x_2(0) & & x_2(1) & & x_2(2) & & x_2(3) & & \dots \\ & & & \searrow & & & & & \\ x_3(0) & & x_3(1) & & x_3(2) & & x_3(3) & & \dots \end{array}$$

dan zien we dat de elementen $x_i(i)$ precies de diagonaal van dit plaatje vormen. De gevolgde methode om de y uit het bewijs te construeren heet daarom ook wel de *diagonalisatiemethode*.

Lemma 6.3.3. *Als $C \subseteq A$ en $f : A \rightarrow C$ is een injectie, dan $A \sim C$.*

Bewijs. Definieer voor alle $x \in A$,

$$h(x) = \begin{cases} f(x) & \text{als } x \in \bigcup_{n \in \mathbb{N}} f^n(A \setminus C) \\ x & \text{anders.} \end{cases}$$

Dan $h : A \rightarrow C$, en we claimen dat h een bijectie is. Ten eerste is h surjectief: Stel dat $y \in C$. Als $y = f^n(a)$ voor zekere $a \in A \setminus C$ dan $n \geq 1$, en $y = f(f^{n-1}(a)) = h(f^{n-1}(a))$. Anders is $y = h(y)$, dus in beide gevallen treedt y op als beeld. Ook is h injectief: Op $\bigcup_n f^n(A \setminus C)$ is h gelijk aan f en dus injectief, en daarbuiten is h de identiteit, en deze gevallen zijn gescheiden. $\square$

We kunnen het idee voor het bewijs van Lemma 6.3.3 als volgt informeel beschrijven. Om een bijectie van A naar C te maken kunnen we om te beginnen de elementen $C \subseteq A$ op C afbeelden. Maar wat doen we dan met de elementen in $A \setminus C$? Antwoord: We beelden deze af op $f(A \setminus C)$. Dit verschuift het probleem naar $f(A \setminus C)$. We beelden de elementen hiervan nu af op $f(f(A \setminus C))$, en deze laatste vervolgens op $f(f(f(A \setminus C)))$, etc. Zo voortgaande lossen we het probleem op door het “naar oneindig” te verschuiven.

Met behulp van Lemma 6.3.3 kunnen we nu gemakkelijk de volgende belangrijke stelling bewijzen:

Stelling 6.3.4. (Cantor-Schröder-Bernstein-Dedekind)⁶ *Als $A \leq B$ en $B \leq A$ dan $A \sim B$.*

⁶De stelling wordt in de literatuur toegeschreven aan de genoemde auteurs, in alle mogelijke combinaties. Voor de achtergrond van de stelling zie Dauben [2, p172].

Bewijs. Stel dat $f : A \rightarrow B$ en $g : B \rightarrow A$ injecties zijn. Dan is $g \circ f : A \rightarrow g(B)$ injectief (als samenstelling van injecties), en $g(B) \subseteq A$, dus wegens Lemma 6.3.3 geldt $A \sim g(B) \sim B$. $\square$

Stelling 6.3.4 is een handig hulpmiddel bij het bewijzen dat verzamelingen gelijk-machtig zijn; in plaats van een bijectie te construeren volstaat het om twee injecties te maken, hetgeen vaak veel makkelijker is. Als voorbeeld geven we de volgende

Stelling 6.3.5. $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$.

Bewijs. Wegens Stelling 6.3.4 is het voldoende om twee injecties tussen deze verzamelingen te definiëren.

$\mathcal{P}(\mathbb{N}) \leq \mathbb{R}$: In paragraaf 3.4 hebben we reeds gezien dat $\mathcal{P}(\mathbb{N}) \sim 2^{\mathbb{N}}$, en in het bewijs van Stelling 6.3.2 zagen we dat $2^{\mathbb{N}} \leq \mathbb{R}$ (zie ook opgave 6.17), dus er volgt dat $\mathcal{P}(\mathbb{N}) \leq \mathbb{R}$.

$\mathbb{R} \leq \mathcal{P}(\mathbb{N})$: Elke $x \in \mathbb{R}$ definieert een unieke verzameling

$$\{q \in \mathbb{Q} \mid q < x\}.$$

(Deze verzameling heet de *Dedekind-snede*⁷ van x .) Er is dus een injectie van $\mathbb{R}$ naar $\mathcal{P}(\mathbb{Q})$. Aangezien $\mathbb{Q} \sim \mathbb{N}$ volgt dat $\mathbb{R} \leq \mathcal{P}(\mathbb{Q}) \sim \mathcal{P}(\mathbb{N})$. $\square$

Uit Stelling 6.3.5 volgt met weinig moeite dat $\mathbb{R} \times \mathbb{R} \sim \mathbb{R}$ (zie opgave 6.13). Er zijn dus evenveel punten in het platte vlak als op een lijn! Toen Cantor dit resultaat vond stuurde hij een bewijs aan zijn collega Richard Dedekind. Hij schreef dat tot dat Dedekind er zijn goedkeuring aan zou hechten hij niets kon zeggen dan: “je le vois, mais je ne le crois pas.”⁸

Uit Stelling 6.3.5 en Stelling 6.3.2 tezamen zien we dat $\mathbb{N}$ meer deelverzamelingen heeft dan elementen. De volgende stelling zegt dat dit zo is voor *elke* verzameling.

Stelling 6.3.6. (Cantor) *Voor elke verzameling A geldt $\mathcal{P}(A) > A$.*

Bewijs. De afbeelding $x \mapsto \{x\}$ laat zien dat $A \leq \mathcal{P}(A)$. Stel nu dat er een bijectie $f : A \rightarrow \mathcal{P}(A)$ bestaat. Definieer

$$D = \{x \in A \mid x \notin f(x)\}.$$

Omdat f surjectief is bestaat er een $d \in A$ met $f(d) = D$. Maar dan geldt

$$\begin{aligned} d \in f(d) &\Leftrightarrow d \in D && \text{(omdat } f(d) = D) \\ &\Leftrightarrow d \notin f(d) && \text{(wegens de definitie van } D) \end{aligned}$$

Dit is een tegenspraak, en we concluderen dat een bijectie f zoals boven kennelijk niet kan bestaan. $\square$

Gevolg 6.3.7. *Er zijn oneindig veel soorten oneindigheid!*

Bewijs. Volgens Stelling 6.3.6 is er voor elke verzameling A een strikt grotere. $\square$

⁷Naar de Duitse wiskundige Richard Dedekind (1831–1916).

⁸Brief van 29 juni 1877, Briefwechsel Cantor-Dedekind. Zie ook Dauben [2, p54 e.v.].

6.4 Axiomatische verzamelingenleer

Rond 1900 werd een aantal paradoxen in de verzamelingenleer ontdekt. De beroemdste is de volgende *Russell-paradox*.⁹ Laat V de verzameling van alle verzamelingen zijn:

$$V = \{A \mid A \text{ is een verzameling}\}.$$

Merk op dat $V \in V$. Beschouw nu de verzameling

$$D = \{A \mid A \notin A\},$$

en stel de vraag: Geldt $D \in D$? Per definitie geldt dat $A \in D \Leftrightarrow A \notin A$. Als we nu $A = D$ invullen krijgen we $D \in D \Leftrightarrow D \notin D$, een contradictie.

De Russell-paradox laat zien dat een “naïeve” benadering van de verzamelingenleer leidt tot contradicties. Om een consistente theorie te krijgen zullen we preciezer moeten zijn over wat we bedoelen met het begrip verzameling, en onze uitgangspunten moeten vastleggen in axioma's. ZFC is de verzameling axioma's opgesteld door Ernst Zermelo en Abraham Fraenkel aan het begin van de 20e eeuw, en die tegenwoordig geldt als het standaard axiomastelsel voor de verzamelingenleer. (De C uit ZFC staat voor “Axiom of Choice”, ofwel het *keuzeaxioma*, een axioma met een bijzondere rol dat nader behandeld wordt in het college Logica.)

Het idee om de verzamelingenleer te bevrijden van paradoxen zoals die van Russell is om het universum van verzamelingen van de grond af op te bouwen met operaties zoals $\mathcal{P}$, en alleen verzamelingen toe te staan die “geconstrueerd” kunnen worden met behulp van eerder geconstrueerde verzamelingen. Op die manier worden circulariteiten zoals $V \in V$ en de paradoxen vermeden.

De theorie van oneindigheid en de begrippen die we tot nu toe besproken hebben werden voor het eerst bestudeerd door de reeds genoemde Georg Cantor. Cantor was onder andere geïnteresseerd in de grootte van $\mathbb{R}$. Omdat $\mathbb{R}$ gerepresenteerd kan worden door een ononderbroken getallenlijn heet $\mathbb{R}$ ook wel het *continuüm*. Op dit punt van onze onderzoeken weten we dat $\mathbb{N} < \mathbb{R}$. Het ligt voor de hand te vragen of $\mathbb{R}$ de eerstvolgende oneindige verzameling is na $\mathbb{N}$, of dat er nog iets tussen ligt. Omdat Cantor er niet in slaagde om verzamelingen van kardinaliteit tussen die van $\mathbb{N}$ en $\mathbb{R}$ te vinden sprak hij het volgende vermoeden uit:

Continuümhypothese (CH). Er bestaan geen verzamelingen A zodat $\mathbb{N} < A < \mathbb{R}$.

Om te bepalen of deze bewering waar is of niet zouden we hem willen bewijzen of weerleggen met behulp van de voornoemde axioma's van de verzamelingenleer ZFC. Dit blijkt nu echter niet mogelijk! Gödel¹⁰ bewees in 1938 dat CH *consistent* is met ZFC, dat wil zeggen, dat het niet mogelijk is om $\neg\text{CH}$ te bewijzen in ZFC. Aan de andere kant bewees Cohen¹¹ in 1963 dat $\neg\text{CH}$ eveneens consistent is met ZFC. De stellingen van Gödel en Cohen tezamen zeggen dat CH *onafhankelijk* is van ZFC, dat wil zeggen, noch bewezen noch weerlegd kan worden op basis van deze axioma's. Voor het bewijs van deze stellingen verwijzen we naar het college Axiomatische Verzamelingenleer.

⁹Genoemd naar de Britse wiskundige, filosoof, en literator Bertrand Russell (1872–1970).

¹⁰Kurt Gödel, Oostenrijks wiskundige (1906–1978).

¹¹Paul Cohen, Amerikaans wiskundige (1934–2007).

Opgaven

Opgave 6.1. Bewijs dat de gelijkmachtheidsrelatie $\sim$ uit Definitie 6.1.1 reflexief, symmetrisch, en transitief is.¹²

Opgave 6.2. Laat A en B eindige verzamelingen zijn. Laat zien dat $A \sim B$ precies als er een $n \in \mathbb{N}$ is zodat zowel A als B n elementen heeft.

Opgave 6.3. Laat zien dat $\mathbb{N}$ de kleinste oneindige verzameling is, in de zin dat als A oneindig is geldt dat $\mathbb{N} \leq A$.

Opgave 6.4. Bewijs dat $\mathbb{N} \sim \mathbb{Z}$.

Opgave 6.5. Bewijs dat $[0, 1] \sim [0, 2]$.

Opgave 6.6. Laat zien dat de functie (12) een bijectie van $\mathbb{N} \times \mathbb{N}$ naar $\mathbb{N}$ definieert.

Opgave 6.7. Bewijs dat $\mathbb{Z} \times \mathbb{Z} \sim \mathbb{Z}$.

Opgave 6.8. Bewijs dat $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \sim \mathbb{N}$.

Opgave 6.9. Laat zien dat de verzameling van alle mogelijke teksten, geschreven in het Nederlands, aftelbaar is.

Opgave 6.10. Bewijs dat $\mathbb{Q} \sim \mathbb{N}$.

Opgave 6.11. Bewijs dat als A_i aftelbaar is voor elke $i \in \mathbb{N}$ dan is ook de vereniging $\bigcup_{i \in \mathbb{N}} A_i$ aftelbaar. (Hint: Gebruik $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.)

Opgave 6.12. (i) Laat zien dat als $a < b$ en $x < y$ in $\mathbb{R}$ dat dan $(a, b) \sim (x, y)$.

(ii) Bewijs dat $(0, 1) \sim \mathbb{R}$. (Hint: $\tan x$ en (i).)

Opgave 6.13. Bewijs de volgende beweringen:

(i) $\mathcal{P}(\mathbb{N}) \sim 2^{\mathbb{N}}$.

(ii) $2^{\mathbb{N}} \times 2^{\mathbb{N}} \sim 2^{\mathbb{N}}$.

(iii) $\mathbb{R} \times \mathbb{R} \sim \mathbb{R}$.

(iv) $\mathbb{R} \sim \mathbb{C}$.

Opgave 6.14. Een getal $x \in \mathbb{R}$ heet *irrationaal* als $x \in \mathbb{R} - \mathbb{Q}$. Laat zien dat er overaftelbaar veel irrationale getallen zijn.

Opgave 6.15. Een *polynoom* (letterlijk: “veelterm”) over $\mathbb{Q}$ is een functie van de vorm

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0,$$

waar de coëfficiënten a_i elementen zijn uit $\mathbb{Q}$ voor elke i . Het getal n heet de *graad* van f . (We nemen hier aan dat $a_n \neq 0$.) Laat zien dat de verzameling polynomen over $\mathbb{Q}$ aftelbaar is.

Opgave 6.16. Een getal $x \in \mathbb{R}$ heet *algebraïsch* als er een polynoom over $\mathbb{Q}$ (zie opgave 6.15) bestaat waarvan x een nulpunt is. Een getal $x \in \mathbb{R}$ dat niet algebraïsch is heet *transcendent*.

¹²We kunnen echter niet zeggen dat $\sim$ een equivalentierelatie is, omdat er geen vaste verzameling is waarop deze relatie gedefinieerd is.

- (i) Laat zien dat de verzameling algebraïsche getallen aftelbaar is. (Hint: Gebruik opgave 6.15 en het feit dat elk polynoom van graad n ten hoogste n nulpunten heeft in $\mathbb{R}$.)
- (ii) Laat zien dat de verzameling transcendente getallen overaftelbaar is. (In het bijzonder *bestaan* zulke getallen. Concrete voorbeelden van transcendente getallen zijn e en π , maar dit is niet gemakkelijk te bewijzen!)¹³

Opgave 6.17. Ga na dat de inbedding van $2^{\mathbb{N}}$ in $\mathbb{R}$ uit het bewijs van Stelling 6.3.2 inderdaad een injectie is.

Opgave 6.18. Ga na wat de functie h uit het bewijs van Lemma 6.3.3 is voor het speciale geval dat $A = (0, 1]$, $C = (0, 1)$, en $f(x) = \frac{1}{2}x$.

Opgave 6.19. We definiëren een afbeelding van $\mathcal{P}(\mathbb{N})$ naar $\mathbb{R}$: Gegeven $A \subseteq \mathbb{N}$ definiëren we een reëel getal x als volgt. Laat

$$x_i = \begin{cases} 2 & \text{als } i \in A \\ 0 & \text{anders} \end{cases}$$

en definieer

$$x = \sum_{i \in \mathbb{N}} x_i \cdot \frac{1}{3^i}.$$

Bewijs dat deze afbeelding een injectie is. (Het beeld van deze functie is een deelverzameling van $[0, 3]$, en heet de *Cantorverzameling*. Het is een voorbeeld van een *fractaal*. Je hebt nodig dat $\sum_{j>i} \frac{1}{3^j} = \frac{1}{2} \frac{1}{3^i}$.)

Opgave 6.20. (Barbiersparadox) De barbier B scheert precies de mannen uit het dorp die zichzelf niet scheren. Scheert B zichzelf? (Vergelijk dit met de Russell-paradox.)

¹³Liouville bewees het bestaan van transcendente getallen in 1844. Cantor bewees de overaftelbaarheid in 1874. De transcendentie van e werd bewezen door Hermite in 1873, en die van π door Lindemann in 1882.

Bibliografie

- [1] E. T. Bell, *Men of mathematics*, Simon and Schuster, 1937.
- [2] J. W. Dauben, *Georg Cantor: His mathematics and philosophy of the infinite*, Princeton University Press, 1979.
- [3] R. Dedekind, *Was sind und was sollen die Zahlen?*, 1888. (Opgenomen in Gesammelte mathematische Werke, p335–391.)
- [4] E. J. Dijksterhuis, *De mechanisering van het wereldbeeld*, Meulenhoff, 1950.
- [5] H. C. Doets en A. S. Troelstra, *Inleiding in de wiskunde en verzamelingenleer*, Mathematisch Instituut, Universiteit van Amsterdam, 1983.
- [6] G. Galilei, *Discorsi e dimostrazioni matematiche, intorno à due nuove scienze*, Lodewijk Elzevir, Leiden, 1638. (Facsimile uitgave, Elsevier, 2013.)
- [7] G. van der Geer, *Basiswiskunde*, Universiteit van Amsterdam, 2009.
- [8] F. Keune, *Getallen, van natuurlijk naar imaginair*, 2e druk, Epsilon, 2011.
- [9] P. Odifreddi, *The mathematical century*, Princeton University Press, 2004.
- [10] G. Polya, *Induction and analogy in mathematics*, Mathematics and plausible reasoning Vol. 1, Princeton University Press, 1954.
- [11] G.-C. Rota, *Indiscrete thoughts*, Birkhäuser 1997.
- [12] B. Russell, *Introduction to mathematical philosophy*, Allen and Unwin, 1919.
- [13] J. Stillwell, *Mathematics and its history*, 3rd edition, Springer, 2010.
- [14] T. Tao, *Analysis I*, Hindustan Book Agency, 2006.

Index

- $\Rightarrow$, 4
- $\perp$, 8
- $\emptyset$, 10
- $X \times Y$, 11
- $|X|$, 11, 39
- $\mathbb{R}^n$, 12
- $A \triangle B$, 14
- $f(A)$, 16
- $f^{-1}(A)$, 16
- $\text{dom}(f)$, 16
- $\text{im}(f)$, 16
- id_X , 16
- f^{-1} , 16
- $g \circ f$, 17
- f^n , 17
- X/R , 17
- $\mathbb{Z}/n\mathbb{Z}$, 18
- $[x]$, 18
- $\mathcal{P}(X)$, 11
- Y^X , 19
- 2^X , 19
- χ_A , 19
- $f \upharpoonright A$, 22
- $|z|$, 27
- $\bar{z}$, 29
- $\binom{n}{k}$, 31
- $n!$, 31
- S_n , 31
- $A \sim B$, 39
- $A \leq B$, 39
- absolute waarde, 27
- afbeelding, 16
- aftelbaar, 40
- aftelbaar oneindig, 40
- algebraïsch, 44
- antisymmetrie, 20
- argument, 16, 28
- Aristoteles, 25
- ariteit, 17
- associativiteit, 5, 12, 14
- axioma, 7
- baan, 17
- barbiersparadox, 45
- bedeling, 8
- beeld, 16
- beperking, 22
- bereik, 16
- Bernoulli, 36
- Bernstein, 41
- bewijs, 7
 - met volledige inductie, 30
 - uit het ongerijmde, 9
- bijjectie, 16
- binomiaalcoëfficiënt, 31
- binomium van Newton, 32
- Bourbaki, 10
- Brouwer, 38
- canonieke afbeelding, 22
- Cantor, 38, 40–43
- Cantorverzameling, 45
- cartesisch product, 11, 19
- Cauchy, 26
- Cauchyrij, 26
- CH, 43
- codomein, 16
- Cohen, 43
- commutativiteit, 12, 14, 23
- complement, 11
- complex geconjugeerde, 29
- complexe getallen, 27
- congruent, 18
- conjunctieve normaalvorm, 37
- connectieven, 3
- consistent, 43
- contingent, 5
- continuüm, 43
- continuümhypothese, 43
- contradictie, 5
- contrapositie, 8
- De Morgan, 8, 12, 13
- Dedekind, 24, 34, 38, 41, 42
- Dedekind-snedes, 42

- deelverzameling, 10
- definitie, 7
- Descartes, 11
- desda, 3
- diagonalisatie, 41
- disjunct, 11
- distributieve wetten, 8, 13
- domein, 16
- driehoeksongelijkheid, 29
- eindig, 39
- equivalent, 5
- equivalentieklasse, 17
- equivalentierelatie, 17
- Euclides, 7
- Euler, 28
- faculteit, 31
- falsum, 8
- Fibonacci, i, 34
- formule
 - geldige, 5
 - predikaat-, 6
 - propositionele, 5
- fractaal, 45
- Fraenkel, 43
- functie, 16
- Gödel, 35, 43
- Galilei, 38
- gelijkmachting, 39
- geordend paar, 11
- getal
 - algebraïsch, 44
 - complex, 27
 - gebroken, 24
 - geheel, 25
 - imaginair, 24, 27
 - irrationaal, 24
 - natuurlijk, 24
 - negatief, 24
 - rationaal, 26
 - reëel, 26, 27
 - transcendent, 44
- graad, 44
- Grassmann, 34
- gulden snede, 34
- Hermite, 45
- Hilbert, 38
- identiteit, 16
- iff, 3
- imaginaire deel, 27
- inbedding, 26
- inclusie-exclusie-principe, 36
- incompatibel, 20
- inductiebasis, 30, 33
- inductiehypothese, 30, 33
- inductieve definitie, 33
- injectie, 16
- inverse, 16
- inverse beeld, 16
- inverteerbaar, 16
- isomorf, 20
- iteratie, 17
- karacteristieke functie, 19
- kardinaliteit, 11, 39
- keuzeaxioma, 43
- klassieke logica, 6
- Kronecker, 24, 38
- kwantor
 - existentiële, 6
 - universele, 6
- Leibniz, 36
- Lindemann, 45
- Liouville, 45
- machtsverzameling, 11
- matrix, 34
- meetkundige reeks, 35
- modulo, 17
- modus ponens, 9
- nand, 9
- Newton, 32
- onafhankelijk, 43
- oneindig, 39
- onvergelijkbaar, 20
- orde-isomorfisme, 20
- ordening
 - lexicografische, 23
 - lineaire, 20
 - partiële, 20
 - totale, 20
- overaftelbaar, 40
- overdekking, 18
- PA, 24
- paringsfunctie, 37, 39
- Pascal, 31, 32

- Peano, 24
- permutatie, 31
- p.o., 20
- Poincaré, 38
- polynoom, 25, 44
- poolcoördinaten, 28
- predikaatlogica, 6
- prenex-normaalvorm, 34
- preordening, 23
- primitief recursief, 35
- propositie, 3
- propositielogica, 3
- Pythagoras, 25

- reële deel, 27
- Recorde, 18
- recursietheorie, 35
- recursieve definitie, 34
- reden, 35
- reflexief, 15
- rekenkundige reeks, 36
- relatie, 15
- representant, 18
- restrictie, 22
- Russell, 3, 24, 38, 43
- Russell-paradox, 43, 45

- samengestelde functie, 17
- Schröder, 41
- Sheffer stroke, 9
- singleton, 10
- stelling, 7
- Stevin, 6
- surjectie, 16
- symmetrisch, 15
- symmetrisch verschil, 14

- tautologie, 5
- tegenvoorbeeld, 6, 13
- transcendent, 44
- transitief, 15
- tupel, 12

- uitdelen, 17

- variabele
 - propositionele, 3
- veelterm, 44
- verzameling, 10
- verzameling representanten, 18
- vezel, 18

- volledig origineel, 16
- volledige inductie, 30, 32
- voortzetting, 22

- waarheidstafel, 4
- welgedefinieerd, 19

- Zermelo, 43
- ZFC, 43