Inleiding in de wiskunde (NWI-WP029)

Klaas Landsman

Collegejaar 2021–2022, kwartaal 1, week 36–42 (2021)

Versie: 30 oktober 2021

Onderwijsinstituut voor Wiskunde, Natuurkunde en Sterrenkunde (WiNSt)
Institute for Mathematics, Astrophysics, en Particle Physics (IMAPP)
landsman@math.ru.nl

- ***Hoorcollege (voor wiskunde en DB studenten, voor anderen weblectures)***:
  dinsdag 13:30-15:15, HG00.307
  donderdag 13:30-15:15, HG00.304, m.u.v. 16 september (CC 5)
  Eerste college dus: dinsdag 7 september, laatste college: donderdag 21 oktober
- ***Tutorcollege***: donderdag 15:30-17:15
  Mart van den Brekel M.vandenBrekel@science.ru.nl, HG01.028
  Mijke Campschroer Mijke.Campschroer@ru.nl, HG03.054
- ***Werkcollege***: woensdag 10:30-12:15 en vrijdag 08:30-10:15, zalen zie rooster indeling groepen zie Brightspace. Student-Assistenten:
  - Menno Bartels menno.bartels@ru.nl
  - Robin Holen robin.holen@ru.nl
  - Eline de Jager eline.dejager@ru.nl
  - Jochem van Rabenswaaij jochem.vanrabenswaaij@ru.nl
  - Saya Smit saya.smit@ru.nl
  - Gilan Takapui gilan.takapui@ru.nl
- Tentamen: vrijdag 5 november 08:30-11:30, HAL 1 (extra tijd: HG00.308)
- Hertentamen: vrijdag 28 januari 2022, LIN2 (extra tijd: HG00.308)
- Bij tentamen en hertentamen is meenemen syllabus toegestaan)
- Bonusregeling huiswerk: bij cijfer 6–10 voor huiswerk 1–2 punten extra voor tentamen via lineaire interpolatie (maar voor het tentamen zelf moet minimaal een 5 worden gehaald om via deze huiswerkbonus een voldoende te halen).
- Boek: *How to Prove It: A Structured Approach*, Third Edition, door Daniel J. Velleman (Cambridge University Press, 2019). Hier zal in de syllabus naar worden verwezen als: Velleman. Terwijl deze syllabus zakelijk, kort, en bondig is (en alle stof bevat), kletst Velleman er omheen en geeft hij vele voorbeelden.
- Het is aan te bevelen ieder college voor te bereiden door van tevoren alvast relevante passages uit de syllabus en evt. boek te lezen (zie schema op Brightspace).

Het is de bedoeling dat je $\sim \frac{6}{15} \times 40 = 16$ *uur per week aan dit vak besteedt!*

Inhoudsopgave

Inleiding

Je kunt deze (historische) inleiding lezen wanneer je wilt, je hebt er misschien zelfs meer aan als je dit na bijvoorbeeld een maand doet. De technische stof in het college is niet afhankelijk van de inleiding, maar wordt er wel door geduid en verhelderd.

De wiskunde in min of meer de vorm die wij nu nog steeds (tenminste op de universiteit) gebruiken, namelijk het spel met definities, axioma's, stellingen, bewijzen, en abstractie, is hoogstwaarschijnlijk in de vierde eeuw v.Chr. ontstaan in het oude Griekenland en omstreken. Daar ging natuurlijk een hele ontwikkeling aan vooraf: duizenden jaren eerder werd in de Egyptische en Babylonische beschavingen al aan rekenkunde en meetkunde gedaan, met name als hulpmiddel bij zaken als astronomie, landmeting, handel, en belastingheffing. Maar dat was een praktische bezigheid, zonder eigen taal, doel, en methodiek. Van legendarische Griekse geleerden als Thales (ca. 624–545 v.Chr.) en Pythagoras (ca. 570–500 v.Chr.) zijn geen oorspronkelijke geschriften bewaard, maar volgens latere overleveringen deden ze eveneens aan rekenkunde, meetkunde, en harmonieleer; het is omstreden in hoeverre ze echt stellingen bewezen. Het oudst bewaarde voorbeeld van zo iets als een logische redenering (zij het niet over wiskunde) is een "leerdicht" van Parmenides (ca. 515–450 v.Chr.) over de natuur, waarin met wat goede wil zelfs een bewijs uit het ongerijmde te vinden is.[1]

Het is duidelijk dat in die tijd filosofie en wiskunde gezamenlijk optrokken en van elkaar het logisch redeneren afkeken.[2] Deze kruisbestuiving tussen filosofie en wiskunde kwam tot een hoogtepunt in de Academie van Plato (ca. 428–348 v.Chr.) in Athene, waarin o.a. belangrijke wiskundigen als Eudoxus (ca. 410–350 v.Chr.) en Theaetetus (ca. 414–369 v.Chr.) actief waren.[3] Plato's beroemdste leerling Aristoteles (ca. 384–322 v.Chr.) geldt als grondlegger van de logica in meer systematische zin; het is duidelijk dat hij daarmee naast de argumentatieleer en retoriek met name ook het wiskundig redeneren van zijn tijd in kaart probeerde te brengen.[4] In bredere zin kunnen we zeggen dat Plato, Aristoteles, en hun tijdgenoten de volgende principes als de kern van helder denken en daarmee van zowel wiskundig als filosofisch redeneren zagen:

1. Zie bijvoorbeeld `www.parmenides-of-elea.net`.
2. Zie bijvoorbeeld G.E.R. Lloyd, *Magic, Reason, and Experience: Studies in the Origins and Development of Greek Science* (Cambridge University Press, 1999).
3. Zie online Wikipedia (Greek mathematics), of voor wie nog boeken leest, enigszins verouderd maar nog steeds heerlijk leesbaar *Ontwakende Wetenschap* door B.L. van der Waerden (Groningen, 1950). Recenter is D.H. Fowler, *The Mathematics of Plato's Academy* (Oxford, 1987). Alle boeken over de geschiedenis van de wiskunde in het algemeen geven uiteraard ook een overzicht van de Griekse wiskunde. Zie online Wikipedia (history of mathematics) of *Encyplopedia Brittanica* `www.britannica.com/science/mathematics/Ancient-mathematical-sources`, of `www.storyofmathematics.com/`. Goede boeken zijn V.J. Katz, *A History of Mathematics, Third Edition* (Pearson, 2009) en R. Calinger, *A Conceptual History of Mathematics* (Prentice-Hall, 1999).
4. De voor wiskunde relevante werken van Aristoteles zijn de *Analytica Priora* en de *Analytica Posteriora* (onderdeel van de *Organon*).

- Gebruik van de rede;[5]
- Ondubbelzinnigheid;
- Streven naar waarheid;
- Abstractie/generalisatie.

Een groot deel van de toendertijd bekende wiskunde werd aan het eind van de vierde eeuw v.Chr. gestroomlijnd en opgeschreven in de *Elementen* van Euclides (ca. 325–270 v.Chr.), het oudst bewaarde en nog steeds beroemdste wiskundeboek aller tijden.[6] Dit was 2000 jaar lang hét model van wiskunde vanuit een axiomatisch-deductieve opbouw (definities, axioma's, stellingen, bewijzen), vroeger ook op middelbare scholen! Direct na Euclides kwamen nog grote wiskundigen als Archimedes (ca. 287–212 v.Chr.) en Apollonios (ca. 260–190 v.Chr.), waarna een langdurige periode van verval intrad.

Dat er door de oude Grieken intensief over de wiskunde is nagedacht toen deze discipline ontstond ligt voor de hand, maar er zijn ook twee latere perioden geweest waarin haar grondvesten schudden en de aard van wiskunde daardoor sterk is veranderd:

1. De 17e eeuw, waarin Isaac Newton (1642–1727) het repertoire van de wiskunde enorm uitbreidde door de invoering van de differentiaal- en integraalrekening;
2. Een tijdvak van ruwweg 50 jaar rond 1900, waarin de verzamelingenleer en logica als basis van de wiskunde werden ingevoerd en bovendien de relatie tussen wiskunde en werkelijkheid (die bij Newton en de oude Grieken nog vooropstond) werd losgelaten: wiskunde werd abstract en stond voortaan op zichzelf. Een centrale figuur in deze transformatie was David Hilbert (1862–1943).

Newton was, na Galileo Galilei (1564–1642) en Christiaan Huygens (1629–1695), een van de eersten (en nog steeds veruit de beste) die wiskunde op natuurkunde toepasten, hetgeen de basis vormde van de wetenschappelijke revolutie van de 17e eeuw.[7]

5. Bij Plato–en eerder bij Parmenides–sloeg dit door naar een algeheel wantrouwen van zintuigelijke waarnemingen. Plato dacht dat de zintuigelijk toegankelijke wereld eigenlijk een schijnwereld is die een vertroebeld beeld geeft van een intellectueel toegankelijke perfecte wereld van wiskundige 'vormen' (ook wel genoemd 'ideeën'). Aristoteles vond juist het omgekeerde: de wereld om ons heen is de echte wereld, en de wiskunde geeft daar een geïdealiseerd (en dus ook vertekend) beeld van. Het grote meningsverschil tussen Plato en Aristoteles over de filosofie van de wiskunde werd door de laatste in de boeken M en N van zijn *Metafysica* uiteengezet. Een verwant probleem is dat van de (vermeende) *waarheid* van wiskundige uitspraken. In de werkelijkheid om ons heen lijkt niets waar, het is eigenlijk maar een rommeltje. Hoe kan deze werkelijkheid dan een exacte wiskundige beschrijving hebben? Hoe meer nadruk de waarheid van de wiskunde krijgt, hoe lastiger het is de toepasbaarheid ervan te begrijpen.

6. Online te vinden in de klassieke vertaling van Thomas Heath uit 1908 in drie delen, die ook uitvoerige commentaren bevat: zie `www.wilbourhall.org/pdfs/Heath_Euclid_I.pdf` voor deel I en analoog voor delen II en III `www.wilbourhall.org/pdfs/Heath_Euclid_II.pdf` en `www.wilbourhall.org/pdfs/Heath_Euclid_III.pdf`. Zie ook Wikipedia (Euclid's Elements) en talloze boeken hierover, zoals E.J. Dijksterhuis, *De Elementen van Euclides* (Noordhoff, 1930), I. Mueller, *Philosophy of Mathematics and Deductive Structure in Euclid's Elements* (MIT Press, 1981) en, iets breder (maar minder diep) R. Hartshorne, *Geometry: Euclid and Beyond* (Springer, 1997).

7. De toepassing van wiskunde op natuurkunde is 2000 jaar vertraagd dankzij Aristoteles, die kennis indeelde in wat wij nu een matrix noemen: de ene as zegt of het object van kennis "onafhankelijk bestaand" of "afhankelijk bestaand" (d.w.z. van de mens) is, en de andere as zegt of het object "onveranderlijk" of "veranderlijk" is. Het enige object op het kruispunt van "onveranderlijk" en "onafhankelijk bestaand" is God, terwijl het diagonale kruispunt van "veranderlijk" en "afhankelijk bestaand" leeg is.

Newton was de grootste wiskundige sinds de oudheid. Vanuit modern perspectief ontwikkelde hij—in een unificatiestap die zijn weerga in de wetenschapsgeschiedenis niet kent—naast de al bestaande meetkunde en rekenkunde (en tot op zekere hoogte algebra) een derde tak van de wiskunde, namelijk de calculus. Hiermee reduceerde Newton alle methoden die sinds de oudheid waren ontwikkeld voor de berekening van lengtes, oppervlakten, inhouden, snelheden, versnellingen, minima en maxima, enzovoort, tot twee (inverse) operaties, namelijk differentiatie en integratie. Newton schreef optimistisch: "*could this ever be done all problems whatever might be resolved.*"

Niemand twijfelde aan de geldigheid van de stellingen van de meetkunde en de rekenkunde. Maar in de calculus gebeurden soms rare dingen. Wat betekent bijvoorbeeld de snelheid van een voorwerp op een bepaald tijdstip? In eerste instantie is snelheid een gemiddelde over een eindig tijdsinterval (zoveel kilometer per uur bijvoorbeeld), maar wat gebeurt er precies als dit tijdsinterval naar nul gaat, zoals in het werk van Newton? Dit stond in nauw verband met de status van 'infinitesimalen', de 'oneindig kleine' grootheden als dx die oorspronkelijk de basis van de calculus vormden, al schudde Newton ze in zijn latere werk af ten gunste van meetkundig gedefinieerde limieten (inmiddels ook alweer vervangen). Al waren er rekenregels voor, niemand begreep eigenlijk wat infinitesimalen of limieten waren. Naast limieten was Newton een fanatiek gebruiker van oneindige reeksen, waarmee hij bijvoorbeeld integralen uitrekende. Dat leidde echter tot verwarring. Men kende de zogenaamde meetkundige reeks

$$1 + x + x^2 + x^3 + x^4 + \cdots$$

en zag in dat dit voor kleine x een steeds betere benadering van $1/(1-x)$ vormde. Voor $x = -1$ echter is de reeks $1-1+1-1+\cdots$, waarover de meningen verschilden. De een groepeerde de termen als $(1-1)+(1-1)+\cdots$ en beweerde dat er daarom 0 uit kwam. De ander schreef de reeks als $1-(1-1)-(1-1)+\cdots$ en kreeg dus 1 als resultaat. Een derde noemde de reeks S en bewees dat $1-S=S$, wat $S=\frac{1}{2}$ geeft. Kortom, de betrouwbaarheid van de wiskunde leek verdwenen, terwijl dat juist haar bepalende eigenschap zou moeten zijn! Daar stonden dan wel de enorme successen van Newton en zijn opvolgers in zowel de zuivere als de toegepaste wiskunde tegenover.

Newtons belangrijkste opvolger was Leonhard Euler (1707–1783), die de wiskunde en mathematische fysica van de 18e eeuw domineerde. Euler zag wel in dat er problemen waren met de calculus, en kwam daar gedeeltelijk aan tegemoet door de krommen van Newton (die bewegende deeltjes voorstelden) te vervangen door het begrip 'functie'. Dat deed hij in eerste instantie (in *Introductio in Analysin Infinitorum* uit 1748) door middel van een formule, meestal een (eindige of oneindige) machtreeks, zoals bij de exponentiële functie, of door een voorschrift, zoals bij de logaritme, die hij introduceerde als de inverse van de exponentiële functie. Later werkte hij met functies als grootheden die van een andere grootheid afhangen (zoals we nu nog doen).

Op het kruispunt van "onveranderlijk" en "afhankelijk bestaand" plaatste Aristoteles de wiskunde, terwijl hij natuurkunde neerzette op het tegenovergestelde kruispunt van "veranderlijk" en "onafhankelijk bestaand". Hierdoor hadden wiskunde en natuurkunde in zijn ogen niets met elkaar te maken.

Maar hiermee werden de moeilijkheden met de wiskunde eigenlijk alleen nog maar erger, want alle problemen met convergentie en limieten kwamen zo met dubbele kracht terug en leidden tevens tot nieuwe vragen: is iedere functie zoals oorspronkelijk gedefinieerd door Euler (dus door een formule of voorschrift) inderdaad te schrijven als machtreeks? Is een machtreeks altijd continu? Differentieerbaar? Glad (willekeurig vaak differentieerbaar)? Is een continue functie overal differentieerbaar behalve in eindig veel punten (denk aan een zaagtand)? Enzovoort. Bovendien voerden Euler en zijn tijdgenoten partiële differentiaalvergelijkingen in, zoals die voor de trillende snaar

$$\partial^2 u/\partial t^2 = c^2 \partial^2 u/\partial x^2,$$

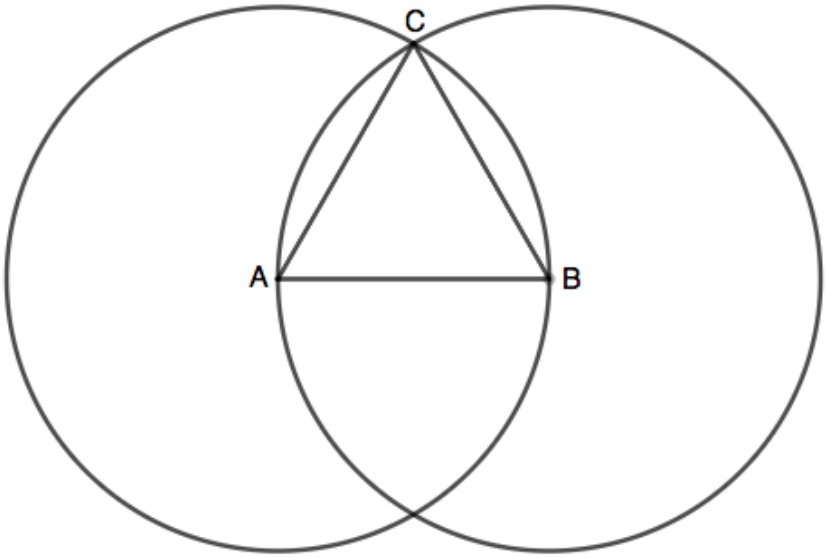
voor $u = u(x, t)$, waarbij allerlei nieuwe vragen en onduidelijkheden ontstonden, zoals over het bestaan en de uniciteit van de oplossing (bij gegeven randvoorwaarden) en over de mogelijkheid om willekeurige oplossingen te schrijven als machtreeksen in sin en cos. Men wist zich met dergelijke kwesties gewoon geen raad. Intussen bleek de Analyse wel het krachtigste middel ooit om de wereld te beschrijven, en verdrong zij gaandeweg de traditionele disciplines van de wiskunde, zoals de meetkunde.

Kortom, men ging onverdroten door maar maakte zich tegelijk zorgen. Deze zorgen werden versterkt doordat na de Franse Revolutie de gewoonte ontstond om Analyse op universiteiten te onderwijzen: tot aan de Franse Revolutie waren vooraanstaande wiskundigen i.h.a. verbonden aan koninklijke academies of hoven (behalve Newton, die aan de Universiteit van Cambridge werkte). Zij gaven daar hoogstens onderwijs aan een kleine elite. Op de universiteiten onderwezen destijds tweederangs figuren totaal verouderde kennis. Daardoor werd het noodzakelijk om een stevige grondslag voor de Analyse te ontwikkelen van het soort die de studenten uit de meetkunde gewend waren. Op de middelbare scholen werd destijds als wiskunde namelijk uitsluitend Euclidische meetkunde onderwezen, meestal uit de *Elementen* van Euclides zelf. In Nederland bestond het wiskundeonderwijs nog tot 1960 uit Euclidische meetkunde, rekenen, goniometrie, trigonometrie, en enige algebra. De Analyse wordt in Nederland dus pas sinds 1961 op scholen onderwezen, bijna drie eeuwen na haar ontstaan!

Zoals je later in de colleges Analyse 1 en 2 zult leren werden de problemen met dit vak opgelost door een goede grondslag, via precieze begrippen van convergentie en continuïteit, integraal, reële getallen, enzovoort.[8] Dit had tot gevolg dat de Analyse net als de Euclidische meetkunde op axiomatische grondslag werd gevest. Daardoor werd de Analyse een formele aangelegenheid, waarbij aanschouwelijkheid, intuïtie en toepassingen steeds minder belangrijk werden. Een soortgelijke trend speelde zich in andere gebieden van de wiskunde af. Zelfs de Euclidische meetkunde bleek niet perfect. Sommige definities (bijvoorbeeld van een punt) waren onduidelijk en bepaalde bewijzen waren niet strict deductief vanuit de axioma's (maar gebruikten intuïtie of waren zelfs ronduit onvolledig). Dit geldt zelfs al voor Propositie 1 in Boek 1 van Euclides, waarin

8. Belangrijke wiskundigen die hieraan bijdroegen waren Augustin-Louis Cauchy (1789–1857), Peter Lejeune Dirichlet (1805–1859), Karl Weierstrass (1815–1897), Eduard Heine (1821–1881), Bernhard Riemann (1826–1866), Richard Dedekind (1831–1916), Georg Cantor (1845–1918), en Hilbert.

het bestaan van een gelijkzijdige driehoek met gegeven basis wordt 'bewezen.' Als deze basis een rechte lijn van A naar B is, wordt dit gedaan door twee cirkels te tekenen: een met middelpunt A, de ander met middelpunt B, beide met straal gelijk aan de gegeven basis. Het derde hoekpunt van de gezochte driehoek is dan een van de twee kruispunten van deze cirkels (zie plaatje). Maar het volgt helemaal niet uit de axioma's van Euclides dat deze cirkels elkaar kruisen! Je ziet wel direct dat dit zo moet zijn, maar dat volgt uit de *visualisatie* (technischer: de *interpretatie*) van de axioma's (een punt is ook een echt punt, een lijn is een echte lijn, enz.) en niet uit de axioma's zelf. Een alien die deze interpretatie niet kent, of een computerprogramma, kan dus zelfs Propositie 1 in Boek 1 van de *Elementen* niet bewijzen!



Dit leidde tot een nieuwe axiomatisering van de meetkunde door Hilbert (*Grundlagen der Geometrie*, 1899), waarin aanschouwelijkheid tenminste in het uiteindelijke bewijs geen enkele rol meer speelt (meetkundige intuïtie kan uiteraard wel worden gebruikt om het bewijs, als mens, te *vinden*). Nog belangrijker dan Hilberts (ten opzichte van Euclides) verbeterde axioma's en bewijzen was daarbij zijn eis dat begrippen als 'punt, lijn, en vlak' in eerste instantie slechts een notatie zijn en net zo goed vervangen kunnen worden door 'liefde, wet, schoorsteenveger', zolang ze maar worden gebruikt zoals de axioma's voorschrijven. Zo schreef Hilbert op 29 december 1899 aan Frege:

> *"Ik wil niets als bekend veronderstellen (…) Als ik bij mijn punten aan een willekeurig systeem van dingen denk, zoals bijvoorbeeld: liefde, wet, schoorsteenveger …, en dan mijn geheel van axioma's als relaties tussen deze dingen aanneem, dan gelden mijn stellingen, zoals die van Pythagoras, ook voor deze dingen."*[9]

9. "Ich will nichts als bekannt voraussetzen (…) Wenn ich unter meinen Punkten irgendwelche Systeme von Dingen, z.B. das System: Liebe, Gesetz, Schornsteinfeger …, denke und dann meine sämtlichen Axiome als Beziehungen zwischen diesen Dingen annehme, so gelten meine Sätze, z.B. der Pythagoras, auch von diesen Dingen."

Dit was een reactie op een eerdere brief van Frege, waarin deze ten onrechte opmerkt dat Hilbert begrippen als punt en lijn bekend veronderstelt, zodat hij het (in tegenstelling tot Euclides) niet nodig vond om ze expliciet te definiëren (een "kardinaal misverstand" volgens Hilbert).[10] De grote Britse logicus Boole (1815–1864) zei hierover:

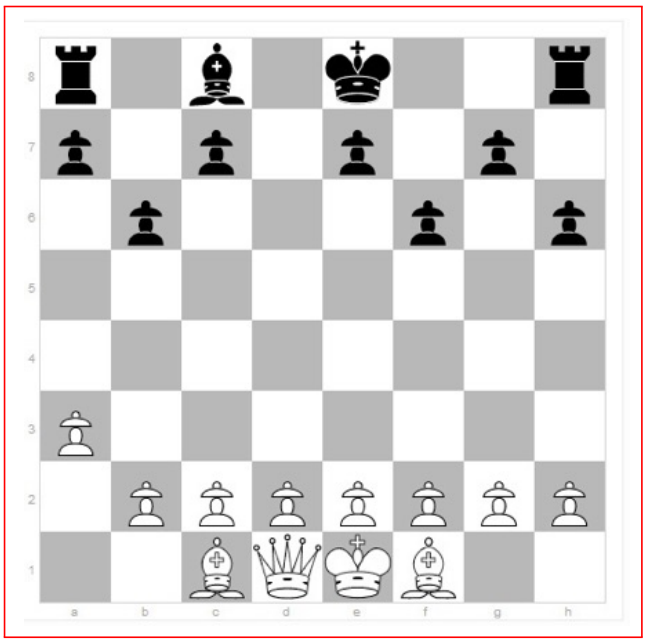
> *"They who are acquainted with the present state of the theory of Symbolic Algebra, are aware of the validity of the processes of analysis does not depend upon the interpretation of the symbols which are employed, but solely upon the laws of their combination."*
>
> (George Boole, *Mathematical Analysis of Logic*, Preface)

Na de Analyse werd dus ook de Euclidische meetkunde geformaliseerd, hetgeen nogal ironisch was, omdat deze ruim 2000 jaar als het summum van precisie en zekerheid was beschouwd! Ook ontstonden in de 19e eeuw nieuwe, abstracte en in eerste instantie compleet realiteitsvreemde gebieden als algebraïsche rekenkunde, projectieve meetkunde, lineaire algebra, algebraïsche logica, en differentiaalmeetkunde (met name in willekeurige dimensies), waarvan de mogelijke toepassingen in ieder geval op dat moment ver te zoeken waren. Gek genoeg leidde juist de abstractie van de wiskunde in de 20e eeuw tot meer en diepere toepassingen; de uitvinders van de computer, Alan Turing (1912–1954) en John von Neumann (1903–1957), waren niet toevallig wiskundigen en logici, en ook Hilbert, een van de grootste wiskundigen ooit, leverde belangrijke bijdragen aan de toegepaste wiskunde, bijvoorbeeld aan de (algemene) relativiteitstheorie van Albert Einstein (1879–1955) en, vooral via zijn leerlingen von Neumann alsmede Hermann Weyl (1885–1955), aan de kwantummechanica die rond 1925 in de fysica opkwam. Zulke toepassingen zouden onmogelijk zijn zonder het abstracte karakter van de moderne wiskunde zoals ingevoerd door Hilbert e.a.: juist de abstractie maakt het namelijk mogelijk om dezelfde wiskundige theorie in schijnbaar totaal verschillende situaties in te zetten, ook als deze inzet totaal onverwacht is. Dit verschijnsel is op zich niet typisch voor de twintigste eeuw: het gebruik van kegelsneden (d.w.z. ellipsen, parabolen, en hyperbolen) om beweging in een gravitatieveld te beschrijven (zoals door Galilei op aarde en Kepler en Newton in de kosmos) was mogelijk omdat deze geometrische figuren al door de oude Grieken (met name Apollonius) waren beschreven, zonder enig idee van deze latere toepassing in de natuurkunde.

In de 19e eeuw vond dus opnieuw een ontwikkeling plaats die de wiskunde veranderde. Van Aristoteles en Euclides tot en met Newton en Euler ging de wiskunde, ondanks haar abstractie, over de werkelijkheid en was zij 'waar'. De Euclidische meetkunde beschreef de ruimte om ons heen, getallen kom je overal tegen, en de Analyse beschreef de natuur(kunde) of was tenminste concreet. Nu zou niemand het in zijn hoofd halen om in de Ooijpolder naar een 10-dimensionale vector-ruimte of een C*-algebra te zoeken. De wiskunde is (net als de kunst) *autonoom* geworden.[11]

10. Ook de wiskundig nauwelijks geschoolde onderwijskundigen die in de jaren '80 het 'realistische' wiskundeonderwijs in Nederland hebben ingevoerd (later 'contextrijk' geheten) begrepen dit niet.
11. Een mooi boek hierover is *Plato's Ghost: The modernist Transformation of Mathematics* van Jeremy Gray (Princeton University Press, 2008).

De conclusie is dat wiskunde twee verschillende kanten heeft, die samen het vak vormen. De ene kant heet *syntax*: dit is een puur symbolische kant, die met een spel als schaken te vergelijken is. Wiskundige uitspraken zijn dan bepaalde welgedefinieerde combinaties van symbolen; we zullen later precies zien hoe dat werkt. Een voorbeeld is de uitspraak $2 + 2 = 5$, die weliswaar onjuist is, maar welgedefinieerd, evenals $2 + 2 = 4$. Daarentegen is $2 + 2$ geen uitspraak. Deze symbolen betekenen in eerste instantie nog niets, hoewel het handig kan zijn als je er een bepaalde voorstelling bij hebt (zoals bij het symbool 2 het getal "twee", bij het symbool $+$ de optelling "plus", enzovoort). Dan zijn er definities en axioma's die de symbolen aan elkaar relateren (er is geen stricte scheiding tussen definities en axioma's). Stellingen zijn uitspraken die je uit de axioma's en definities af kunt leiden (hoe dat precies gebeurt bespreken we zo dadelijk), zoals $2 + 2 = 4$. Zulke stellingen zeggen (nog) niets over de werkelijkheid.



Het schaakspel geeft een analogie. Bord en stukken staan voor wiskundige symbolen, definities voor de loop der stukken, axioma's voor de beginstand, en bewijsregels voor de spelregels. Een wiskundige *uitspraak* is analoog aan een *stand*, d.w.z. een configuratie van de schaakstukken op het bord. Een wiskundige *Stelling* is een uitspraak die kan worden bewezen; een *stelling* op het schaakbord is een stand die volgens de regels uit de beginstand kan ontstaan (vraag: kan dat in het diagram, met zwart aan zet?).

De vraag is dan wat de precieze spelregels = bewijsregels van de wiskunde zijn. In de *Elementen* van Euclides worden deze niet formeel opgeschreven, hoewel er duidelijk en meestal overtuigend van alles wordt bewezen. De logica van Aristoteles was deels geïnspireerd door de wiskunde, maar was veel te beperkt (en ook niet primair bedoeld) om deze te formaliseren (zijn syllogismen zijn zelfs niet afdoende voor de wiskunde van zijn tijd). De juiste en volledige bewijsregels voor de (huidige) wiskunde werden voor het eerst in de periode 1920–1930 door Hilbert en diens leerlingen opgeschreven.[12]

12. Belangrijk voorwerk werd verricht door o.a. Gottlob Frege (1848–1925), Giuseppe Peano (1858–

In min of meer die vorm staan ze ook in deze syllabus, zij het niet in volledige algemeenheid (maar zoals noodzakelijk en voldoende voor de wiskundige praktijk). Een simpel voorbeeld van een bewijsregel (tevens de belangrijkste uit de hele wiskunde) is de al in de oudheid bekende en door Aristoteles beschreven *Modus Ponens*:

Als B volgt uit A, en A geldt, dan geldt ook B (uit $A \to B$ en A volgt B).

Waar Hilbert en zijn leerlingen ondanks verwoede pogingen echter niet in slaagden was om deze bewijsregels ook zelf weer te bewijzen als 'noodzakelijke' gevolgen van het menselijk denken o.i.d.: dit op zich nobele doel lijkt ook inherent circulair.

De tweede kant van de wiskunde heet (net als in de taalkunde) *semantiek*: hierbij gaat het om de *betekenis* van de syntax. De formele taal wordt daarbij op de een of andere manier *geïnterpreteerd*. Je kunt de symbolen P, L, en V uit de abstracte Euclidische meetkunde bijvoorbeeld interpreteren als punten, lijnen en vlakken in de natuurlijke zin. Hierbij ga je er vanuit dat deze laatste ook echt bestaan. Zo'n interpretatie is zinvol als de 'echte' punten, lijnen en vlakken aan precies dezelfde relaties voldoen als de abstracte symbolen dat volgens de axioma's doen. Vaak is dat maar bij benadering het geval. De stellingen op syntactisch niveau erven de interpretatie van de symbolen en zeggen dan iets over de werkelijkheid. Maar wat ze zeggen is meestal slechts een benadering, omdat de interpretatie zelf al slechts een benadering was:

> *"Voor zover de conclusies van de wiskunde met de werkelijkheid te maken hebben zijn ze niet zeker, en voor zover ze zeker zijn verwijzen ze niet naar de werkelijkheid."* Albert Einstein (1921).[13]

Het college *Inleiding in de wiskunde* is een eerste kennismaking met de formele kant van de wiskunde. Deze begint met een zuiver logisch deel, de propositielogica, die tevens een voorbeeld geeft van een op zichzelf staande wiskundige theorie met axioma's, stellingen, en bewijzen. Deze theorie is veel eenvoudiger (en praktischer!) dan Euclidische meetkunde en is daarmee zeer geschikt om mee te beginnen. Het is een feite een primitieve vorm van wiskunde zonder variabelen. Daarna komt de verzamelingenleer, waar je de gehele bekende wiskunde, dus met name ook variabelen, mee kunt beschrijven: kort gezegd is ieder wiskundig object een verzameling, vaak getooid met een extra structuur die ook weer in termen van verzamelingen is gedefinieerd. Alle definities en constructies in de wiskunde gaan dus uiteindelijk over verzamelingen–iets waar je in het voortgezet onderwijs echter weinig van merkt, net zo min als van streng (d.w.z. axiomatisch-deductief) bewijzen. Via deze taal raak je ook vertrouwd met de technieken voor bewijsvoering in de wiskunde die verder gaan dan propositielogica. Vrijwel al je gelijktijdige en toekomstige wiskundevakken breiden deze definities en constructies vervolgens verder uit: het is alsof je vanuit relatief weinig spelregels steeds meer partijen van het desbetreffende spel gaat spelen, met een schier oneindige rijkdom.

Veel plezier!

1932), Ernst Zermelo (1871–1953), Bertrand Russell (1872–1970), en Alfred N. Whitehead (1861–1947).

13. "Insofern sich die Sätze der Mathematik auf die Wirklichkeit beziehen, sind sie nicht sicher, und insofern sie sicher sind, beziehen sie sich nicht auf die Wirklichkeit." Uit *Geometrie und Erfahrung*.

1

Wiskunde zonder variabelen: Propositielogica

De eerste stap in de formele opbouw van de wiskunde is de ontwikkeling van een *logische taal*. Wiskundige formules bevatten vaak variabelen ("x" etc.), maar we bespreken nu eerst een deel van de wiskundige taal waar die nog niet in voorkomen, genaamd *propositielogica*. Hoewel dit gebied van de wiskunde pas in de 19e eeuw ontstond en begin 20e eeuw werd voltooid,[1] is het een formalisering van het "syllogistisch" redeneren dat de oude Grieken al kenden en zou het al op het vwo behandeld kunnen worden. Ook de logische taal voor wiskunde mét variabelen berust hier op.

Het doel van een wiskundige taal is om wiskundige *uitspraken* (ook genaamd *proposities*) te formuleren, zoals $2 + 2 = 4$ of de stelling van Pythagoras. Zo'n uitspraak is uiteindelijk een grammaticale constructie. We moeten daartoe aangeven wat:

- de *notatie* is (d.w.z. welke symbolen in de logische taal voorkomen),
- de *regels* zijn om symbolen te combineren tot een welgedefinieerde uitspraak.

Vervolgens zijn er twee manieren waarop een wiskundige uitspraak kan "kloppen":

- De uitspraak kan worden *bewezen* vanuit axioma's en bewijsregels (*syntax*);
- De uitspraak is *waar* vanuit de interpretatie van de symbolen erin (*semantiek*).

Dat deze twee aspecten in principe verschillend zijn is een inzicht uit de 20e eeuw. We zullen zien dat ze wel zeer nauw samenhangen. Het bewijzen is een puur *syntactische* constructie, dat wil zeggen: net als een uitspraak zelf is een bewijs ervan een bepaalde combinatie van regels en symbolen. Een computer zou het kunnen leveren. Een wiskundig bewijs is te vergelijken met het correct volgen van de regels van het schaakspel (zie ook p. 9). Daarbij maakt het niet uit of de koning Willem Alexander is. Het gaat bij zowel schaken (en andere spellen) als bewijzen uitsluitend om het volgen van de regels, en die zijn onafhankelijk van de interpretatie van de schaakstukken (of van hun vorm en materiaal). Ook axioma's, waarvan men tot de 19e eeuw dacht dat ze waar waren, zijn slechts een afspraak, zoals de beginstelling van een spel als schaken. De (on)waarheid van een uitspraak daarentegen hangt samen met de *betekenis* oftewel *interpretatie* van de symbolen (waar een bewijs juist weer geen gebruik van maakt).

1. Naast Boole, Frege, Russell, en Hilbert noemen we ook van Charles S. Peirce (1839–1914), Ludwig Wittgenstein (1889–1951), en Emil Post (1897–1954), die elk de straks te bespreken waarheidstabellen uitvonden. Een goede inleiding is ook het boekje *Logica in Actie* van J. van Benthem, zie Brightspace.

1.1 Notatie

De *notatie* van de propositielogica bestaat uit twee groepen symbolen:

1. De ***zuiver logische symbolen*** zijn: $\boxed{\neg,\ \wedge,\ \vee,\ \rightarrow,\ \bot}$. Dit zijn de afkortingen voor resp. *niet, en, of, impliceert* en *falsum*, de altijd onware propositie. Maar let op! De hier gegeven betekenis van de zuiver logische symbolen is in principe niet nodig, omdat deze *betekenis* volgt uit de later op te stellen regels voor het *gebruik* van de symbolen (dit gebeurt apart voor waarheid en voor bewijzen).
2. De ***niet-logische symbolen*** van een theorie in de propositielogica zijn vastgelegd in een lijst $\{P_1, P_2, \ldots\}$, ook wel geschreven als $\{P, Q, R, \ldots\}$, zoals in Velleman. Deze symbolen staan voor ***atomaire*** of ***elementaire*** proposities, die het eenvoudigste voorbeeld zijn van uitspraken (zie volgende punt).[2] Syntactisch zijn de P_i symbolen. Semantisch kun je ze binnen of buiten de wiskunde interpreteren zoals je wilt, zoals bijvoorbeeld: P betekent "$7+5=12$" en Q staat voor "het regent" (en het is november). Zie ook vele voorbeelden in Velleman, §1.1.
3. We gebruiken ook haakjes $(\ ,\ )$. Deze zijn soms overbodig als we afspreken dat:
   - $\neg$ sterker bindt dan $\vee$ en $\wedge$ (die even sterk binden);
   - $\vee$ en $\wedge$ op hun beurt weer sterker binden dan $\rightarrow$.

Voorbeeld: $P_1 \rightarrow P_2 \vee P_3$ is hetzelfde als $P_1 \rightarrow (P_2 \vee P_3)$, maar in $(P_1 \rightarrow P_2) \vee P_3$ zijn de haakjes noodzakelijk! Dit geldt nog sterker voor een uitdrukking als $P_1 \vee P_2 \wedge P_3$, die *niet eens gedefinieerd is zonder haakjes*: het is ofwel $(P_1 \vee P_2) \wedge P_3$ ofwel $P_1 \vee (P_2 \wedge P_3)$.

Definitie 1.1 *De* **uitspraken** *van de propositielogica zijn alle uitdrukkingen in de bovenstaande symbolen die als volgt–en niet anders!–tot stand komen:*

i) *Ieder niet-logisch symbool* P_i *(of* $P, Q, \ldots$*) is een uitspraak, evenals* $\bot$*;*

ii) *Als* A *een uitspraak is, dan is* $\neg A$ *dat ook;*

iii) *Als* A *en* B *uitspraken zijn, dan zijn* $A \wedge B$*,* $A \vee B$*, en* $A \rightarrow B$ *dat ook.*

Dit is een *iteratief* voorschrift: als je regel **ii)** toepast op regel **i)** kom je op $A := \neg P_1$, en dan kun je volgens **iii)** met zeg $B := P_4$ maken: $A \rightarrow B$, oftewel $\neg P_1 \rightarrow P_4$. En daaruit kun je maken $(\neg P_1 \rightarrow P_4) \vee P_2$, enz.[3] Zie voorbeelden in Velleman, §1.1, en de uitspraken (1.11) en (1.26) - (1.41), met $\rightarrow$ in plaats van $\leftrightarrow$, of zoals bedoeld, met (1.21).

Het zal je opvallen dat we twee taalniveaus hebben: de symbolische taal als boven, en de taal waarin we daarover spreken en wiskunde doen. De laatste heet de ***metataal***. Onze metataal is een combinatie van natuurlijke taal (in dit geval Nederlands, inclusief "desda" voor "dan en slechts dan") en af en toe een symbool als $=$, $:=$, of $\Rightarrow$.[4]

2. Formeel is deze lijst een aftelbare verzameling, maar dat begrip moeten we nog officieel definiëren. Belangrijk is vooral dat we willekeurig veel atomaire proposities tot onze beschikking hebben.
3. Let op: we gebruiken het (niet-logische) symbool $:=$ hier informeel om een uitspraak een naam te geven. De notatie $A := \neg P_1$ betekent dus: de uitdrukking wordt afgekort als A. Als logisch symbool treedt $=$ pas op in de eerste-orde logica, zie §2.2. Hier is het nog een symbool in de metataal, zie onder.
4. Ook de metataal kan in principe geformaliseerd worden (zonder in een vicieuze cirkel te geraken).

1.2 Semantiek en waarheid

We onderbreken de opbouw van de syntax en gaan verder met de ***semantiek*** van de propositielogica. Deze bestaat uit een voorschrift (officieel geheten: ***valuatie***) ν dat van iedere atomaire propositie P_i zegt of deze waar is of niet. Als P_i waar is onder het voorschrift ν schrijven we $\nu(P_i) = 1$, en als P_i niet waar is, $\nu(P_i) = 0$ (soms staat er slordig $P_i = 1$ of $P_i = 0$, maar ook dat is *ten opzichte van een bepaald voorschrift* ν). Met andere woorden: ν is een afbeelding of functie van de lijst (later: verzameling) atomaire proposities $\{P_1, P_2, \ldots\}$ (of een eindig deel daarvan) naar de verzameling $\{0, 1\}$: de begrippen "afbeelding" en "functie" betekenen dat bij iedere P_i een getal 0 of 1 hoort. Ieder voorschrift ν is hierbij wiskundig gesproken mogelijk. In de praktijk wordt ν bepaald door zowel de betekenis van alle P_i (bijvoorbeeld P_1 zegt: "het regent") als de toestand in de wereld (d.w.z. of het daadwerkelijk regent). Als zuiver wiskundigen hebben we daar niets mee te maken en kunnen we gewoon zo'n ν kiezen, oftewel een geordende lijst $\langle \nu(P_1), \ldots, \nu(P_n) \rangle$, zonder te denken aan betekenissen en toestanden. Het is handig om ν ook te definiëren op het falsum $\bot$, nl. door $\boxed{\nu(\bot) = 0}$ voor alle ν.

De essentie is nu dat een valuatie ν, die in eerste instantie dus alleen zegt of iedere *atomaire propositie* P_i (on)waar is, ook de (on)waarheid bepaalt van een willekeurige *uitspraak* A die is opgebouwd uit de P_i. Ook hier betekent de notatie $\nu(A) = 1$ "A is waar" en $\nu(A) = 0$ staat voor "A is onwaar". De manier waarop $\nu(A)$ wordt bepaald is onderdeel van de *definitie* van propositielogica als wiskundige theorie: het is een *afspraak* of spelregel, maar wel een hele natuurlijke, die uitdrukt hoe we logisch denken over de symbolen $\neg$, $\wedge$, $\vee$, $\rightarrow$. We beginnen met $\neg P$ en spreken af: $\boxed{\text{als } \nu(P) = 0 \text{ dan geldt } \nu(\neg P) = 1, \text{ en als } \nu(P) = 1 \text{ dan } \nu(\neg P) = 0.}$ Feitelijk definieert deze regel het symbool $\neg$ als "niet". Nu de binaire combinaties van P en Q, zoals $P \wedge Q$. De regels worden handig gecodeerd in de ***waarheidstabellen*** (Engels: *truth tables*)

P	$\neg P$
0	1
1	0

P	Q	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

De grote tabel rechts moet als volgt worden gelezen: als $\nu(P) = 0$ en $\nu(Q) = 0$, dan is $\nu(P \wedge Q) = 0$. Als $\nu(P) = 1$ en $\nu(Q) = 0$, dan is $\nu(P \vee Q) = 1$. Enzovoort. Net als bij $\bot$ geeft dit simpelweg weer dat $\wedge$ "en" is, $\vee$ "of", en $\rightarrow$ "impliceert" (de kolom onder $\leftrightarrow$ komt later aan bod en kan nu worden overgeslagen). Dit geldt echter niet alleen voor *atomaire proposities* P en Q: als A en B *willekeurige uitspraken* zijn, dan kun je ook A en B volgens de regels combineren tot nieuwe uitspraken. En om de waarde ν van die nieuwe uitspraken te berekenen gebruik je precies de bovenstaande waarheidstabellen, met A en B in plaats van resp. P en Q, waarbij A en B *willekeurige* uitspraken zijn:

A	¬A
0	1
1	0

A	B	A ∧ B	A ∨ B	A → B	A ↔ B
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

- Als $\nu(A) = 0$, dan $\nu(\neg A) = 1$ en als $\nu(A) = 1$, dan $\nu(\neg A) = 0$.
- Als $\nu(A) = 0$ en $\nu(B) = 0$, dan $\nu(A \wedge B) = 0$, $\nu(A \vee B) = 0$, en $\nu(A \to B) = 1$.
- Als $\nu(A) = 0$ en $\nu(B) = 1$, dan $\nu(A \wedge B) = 0$, $\nu(A \vee B) = 1$, en $\nu(A \to B) = 1$.

Enzovoort. Hieruit volgt hoe je $\nu(C)$ bepaalt voor een willekeurige uitspraak C. Deze is volgens de drie regels opgebouwd uit de logische symbolen en de P_i. Als $C = P_i$ of $C = \bot$ ben je meteen klaar, want $\nu(P_i)$ is gegeven en $\nu(\bot) = 0$. Zo niet, dan is C gelijk aan $\neg A$, of $A \wedge B$, of $A \vee B$, of $A \to B$, voor bepaalde uitspraken A en B. Als $C = \neg A$, dan volgt $\nu(C)$ volgens de tabel uit $\nu(A)$. Als $A = P_i$ of $A = \bot$ ben je klaar, zo niet, dan is A ook weer opgebouwd uit kleinere uitspraken waar je ν op los kunt laten. Als $C = A \wedge B$, dan bepaal je $\nu(A)$ en $\nu(B)$, zo nodig door A en B ook weer op te breken in kleinere uitspraken, en dan volgt uit de tabel $\nu(C)$. Analoog voor $A \vee B$, of $A \to B$. De iteratieve berekening van $\nu(C)$ volgt dus precies de iteratieve constructie van C.

We kunnen deze procedure ook een tikje anders (en handiger) opschrijven: tot nu toe waren de symbolen $\neg$, $\wedge$, $\vee$, en $\to$ bedoeld om *uitspraken* A en B aan elkaar te plakken. Nu gebruiken we dezelfde symbolen om de *getallen* 0 en 1 aan elkaar te plakken, volgens de regels die uit de waarheidstabellen afgelezen kunnen worden, dus

$$\neg 0 = 1; \quad \neg 1 = 0; \tag{1.1}$$

$$0 \wedge 0 = 0; \quad 0 \wedge 1 = 0; \quad 1 \wedge 0 = 0; \quad 1 \wedge 1 = 1; \tag{1.2}$$

$$0 \vee 0 = 0; \quad 0 \vee 1 = 1; \quad 1 \vee 0 = 1; \quad 1 \vee 1 = 1; \tag{1.3}$$

$$0 \to 0 = 1; \quad 0 \to 1 = 1; \quad 1 \to 0 = 0; \quad 1 \to 1 = 1. \tag{1.4}$$

Nu kunnen we de waarde $\nu(A)$ van een uitspraak A uitrekenen via de volgende regels:

$$\nu(\bot) = 0; \tag{1.5}$$

$$\nu(\neg A) = \neg\nu(A); \tag{1.6}$$

$$\nu(A \wedge B) = \nu(A) \wedge \nu(B); \tag{1.7}$$

$$\nu(A \vee B) = \nu(A) \vee \nu(B); \tag{1.8}$$

$$\nu(A \to B) = \nu(A) \to \nu(B). \tag{1.9}$$

De volgende voorbeelden illustreren wat wordt bedoeld en hoe je moet rekenen. Eerst

$$\nu(\neg P \vee Q) = \nu(\neg P) \vee \nu(Q) = \neg\nu(P) \vee \nu(Q). \tag{1.10}$$

Stel nu dat $\nu(P) = 1$ en $\nu(Q) = 0$. Uit (1.6) volgt $\neg\nu(P) = 0$ en in (1.3) staat $0 \vee 0 = 0$, zodat $\nu(\neg P \vee Q) = 0$. Met $\nu(P) = 0$ en $\nu(Q) = 0$ komt er echter $\nu(\neg P \vee Q) = 1$ (ga na). Nu geven we een voorbeeld waarin slechts de implicatie $\to$ voorkomt. Nu de uitspraak

$$A := (P_1 \to (P_2 \to P_3)) \to ((P_1 \to P_2) \to (P_1 \to P_3)). \tag{1.11}$$

We kiezen een valuatie ν en weten dus $\nu(P_1)$, $\nu(P_2)$, en $\nu(P_3)$. Net als boven vinden we:

$$\begin{aligned}\nu(A) &= \nu((P_1 \to (P_2 \to P_3)) \to ((P_1 \to P_2) \to (P_1 \to P_3))) \\ &= \nu(P_1 \to (P_2 \to P_3)) \to \nu((P_1 \to P_2) \to (P_1 \to P_3)) \\ &= (\nu(P_1) \to \nu(P_2 \to P_3))) \to (\nu(P_1 \to P_2) \to \nu(P_1 \to P_3)) \\ &= (\nu(P_1) \to (\nu(P_2) \to \nu(P_3))) \to ((\nu(P_1) \to \nu(P_2)) \to (\nu(P_1) \to \nu(P_3))). \qquad (1.12)\end{aligned}$$

Stel nu dat $\nu(P_1) = 1$, $\nu(P_2) = 0$, en $\nu(P_3) = 1$. Dan volgt uit (1.4):

$$\nu(P_2) \to \nu(P_3) = (0 \to 1) = 1; \quad \nu(P_1) \to \nu(P_2) = (1 \to 0) = 0; \qquad (1.13)$$

$$\nu(P_1) \to \nu(P_3) = (1 \to 1) = 1; \quad \nu(A) = (1 \to 1) \to (0 \to 1) = (1 \to 1) = 1. \qquad (1.14)$$

We zullen later, in §5.2, met behulp van *inductie* het volgende bewijzen:[5]

Stelling 1.2 *Voor iedere uitspraak* C *die atomaire proposities* P_1 *t/m* P_n *bevat, en iedere lijst van mogelijke waarden* $\nu(P_1)$ *t/m* $\nu(P_n)$*, elk gelijk aan 0 of 1, is er een unieke waarde* $\nu(C)$*, gelijk aan 0 of 1, die kan worden berekend door* C *op te knippen in kleinere proposities en (herhaaldelijk) de regels* (1.5) *t/m* (1.9) *toe te passen. In het bijzonder hangt de waarde* $\nu(C)$ *niet af van de precieze manier waarop je* C *opknipt.*

Hier is nog een zienswijze. Een valuatie ν kent per definitie aan een uitspraak A het getal $\nu(A)$ toe. Maar omgekeerd kunnen we ook zeggen dat A dit getal juist aan ν toekent! Het is maar wat je als gegeven en wat je als variabel beschouwt. Oftewel:

Een uitspraak A *in propositielogica die de atomaire proposities* P_1 *t/m* P_n *bevat kent aan iedere geordende lijst* $\langle \nu(P_1), \ldots, \nu(P_n) \rangle$ *van getallen 0 of 1 een getal 0 of 1 toe.*

Zie ook Opgave 1.1: je kunt bij een atomaire propositie P_i aan een lampje denken, dat aan of uit kan staan (resp. $\nu(P) = 1$ of 0) , en aan een uitspraak A die P_1 t/m P_n bevat als een schakeling tussen n lampjes, die aan iedere stand van de lampjes een stand van weer een ander lampje toekent (dat aanstaat als $\nu(A) = 1$ en uitstaat als $\nu(A) = 0$).

Ten slotte gaan we kort in op de verschillen tussen propositielogica en natuurlijke taal.

- De implicatie $\to$ is het meest ongebruikelijk ten opzichte van de natuurlijke taal: $A \to B$ *is altijd waar als* A *onwaar is*, d.w.z. $\nu(A) = 0$ geeft $\nu(A \to B) = 1$, onafhankelijk van $\nu(B)$. Met $A := \bot$ volgt dat $\bot \to B$ waar is voor iedere uitspraak B en valuatie ν, omdat immers altijd geldt $\nu(\bot) = 0$. Zie ook Velleman, §1.5.
- De disjunctie $\vee$ ("of") heeft in de natuurlijke taal vaak een exclusieve betekenis: "de dood of de gladiolen". In de logica is dit niet zo: volgens de waarheidstabel is $A \vee B$ ook waar als A en B beide waar zijn. Zie ook Opgave 1.2.
- De conjunctie $\wedge$ ("en") heeft in gewone taal soms een tijdselement: ik ga naar huis en zet thee. Dat is er in de wiskunde niet: alles heeft eeuwigheidswaarde!

5. Geavanceerde formulering: Stel $\mathscr{A} = \{P_1, P_2, \ldots\}$ is de lijst (verzameling) van atomaire proposities en $\mathscr{P}(\mathscr{A})$ is de lijst (verzameling) van alle mogelijke proposities over $\mathscr{A}$. Dan heeft iedere afbeelding (functie) $\nu : \mathscr{A} \to \{0, 1\}$ een unieke uitbreiding $\nu : \mathscr{P}(\mathscr{A}) \to \{0, 1\}$ die voldoet aan (1.5) t/m (1.9).

1.3 Tautologieën

Voor veel uitspraken A is $\nu(A) = 1$ voor de ene valuatie ν, terwijl $\nu'(A) = 0$ voor een andere valuatie ν'. Een speciaal soort uitspraak A is er een die onder alle valuaties waar is: $\nu(A) = 1$ voor iedere ν. Zo'n uitspraak heet een ***tautologie***. In plaats van "A is een tautologie" schrijven we: $\boxed{\models A}$. Omgekeerd heet een uitspraak die voor alle valuaties ν onwaar is een ***contradictie***. Contradicties geven niets nieuws, want *een uitspraak A is een contradictie desda de negatie $\neg A$ een tautologie is, en omgekeerd* (opgave). Hier is alvast een klein lijstje tautologieën waar slechts één kleinere uitspraak A in voorkomt:

$$\models A \to A; \tag{1.15}$$

$$\models \bot \to A; \tag{1.16}$$

$$\models A \vee (\neg A); \tag{1.17}$$

$$\models \neg A \to (A \to \bot); \qquad \models (A \to \bot) \to \neg A; \tag{1.18}$$

$$\models \neg\neg A \to A; \qquad \models A \to \neg\neg A; \tag{1.19}$$

$$\models (A \wedge \neg A) \to \bot; \qquad \models \bot \to (A \wedge \neg A). \tag{1.20}$$

Hier betekent bijvoorbeeld (1.15) dat $A \to A$ voor *iedere uitspraak* A een tautologie is. Dit volgt uit de tabel bovenaan p. 13: we hebben nu $B = A$ zodat alleen $A = 0$ en $B = 0$ of $A = 1$ en $B = 1$ mogelijk zijn. In beide gevallen geldt $(A \to B) = 1$. Dus $A \to A$ is waar, $\nu(A \to A) = 1$, voor zowel $\nu(A) = 1$ als $\nu(A) = 0$ en daarmee is het een tautologie. Je kunt dit ook zien uit (1.9): deze geeft $\nu(A \to A) = \nu(A) \to \nu(A)$, en dan zien we in (1.4) dat zowel $0 \to 0 = 1$ als $1 \to 1 = 1$. Opnieuw volgt dat wat $\nu(A)$ ook is, nul of een, geldt dat $\nu(A \to A) = 1$. Ga alle andere gevallen (1.16) t/m (1.20) ook na! De laatste zes gelden paarsgewijs beide kanten op (en staan daarom ook op dezelfde regel). De meeste tautologieën zijn van die vorm en daarom is er een speciaal logisch symbool ingevoerd, $\leftrightarrow$, dat feitelijk een afkorting is. Grammaticaal volgt $\leftrightarrow$ regel **iii** uit §1.1, dus: $\boxed{\text{als } A \text{ en } B \text{ uitspraken zijn, dan is } A \leftrightarrow B \text{ dat ook}}$, met als betekenis:

$$A \leftrightarrow B := (A \to B) \wedge (B \to A). \tag{1.21}$$

De al eerder opgeschreven waarheidstabel voor $\leftrightarrow$ is makkelijk na te rekenen, bijv.

$$0 \leftrightarrow 0 = (0 \to 0) \wedge (0 \to 0) = 1 \wedge 1 = 1. \tag{1.22}$$

We kunnen de zes tautologieën (1.18), (1.19) en (1.20) nu in drie regels opschrijven als

$$\models \neg A \leftrightarrow (A \to \bot); \tag{1.23}$$

$$\models \neg\neg A \leftrightarrow A; \tag{1.24}$$

$$\models A \wedge \neg A \leftrightarrow \bot. \tag{1.25}$$

Je kunt narekenen dat dit tautologieën zijn door $\leftrightarrow$ weer te elimineren via (1.21). Doe dat, maar er is een slimmere methode. Uitspraken A, B waarvoor $A \leftrightarrow B$ een tautologie is ($\models A \leftrightarrow B$) heten ***logisch equivalent***. Het blijkt dat dit precies zo is als $\nu(A) = \nu(B)$ voor iedere valuatie ν. Dit is erg handig, omdat je dit vaak uit kunt rekenen, als volgt.

Neem bijvoorbeeld (1.23); als je dat leest als $A \leftrightarrow B$ moet je uiteraard A vervangen door $\neg A$ en B door $A \to \bot$. Zo'n substitutie komt vaak voor en we noteren deze als: $A \rightsquigarrow \neg A$ en $B \rightsquigarrow (A \to \bot)$ (dit is even wennen omdat A twee rollen speelt). We berekenen

$$v(A \to \bot) = v(A) \to v(\bot) = v(A) \to 0 = \neg v(A) = v(\neg A).$$

Hier gebruiken we van (1.4) het deel $0 \to 0 = 1$ en $1 \to 0 = 0$ om dan, met (1.1), te schrijven $v(A) \to 0 = \neg v(A)$. Daarna zetten we (1.6) in om te concluderen dat $\neg v(A) = v(\neg A)$. Dus $v(\neg A) = v(A \to \bot)$, waarmee $\neg A$ en $A \to \bot$ logisch equivalent zijn.

Stelling 1.3 *1. De uitspraak $A \leftrightarrow B$ is een tautologie desda voor iedere valuatie v geldt: $v(A) = v(B)$. Met andere woorden: $\vDash A \leftrightarrow B$ geldt desda A en B altijd (dat wil zeggen voor iedere valuatie v) tegelijk waar of tegelijk onwaar zijn.*

2. Als A en $A \to B$ beide tautologieën zijn, dan is ook B een tautologie.

3. De uitspraak $A \wedge B$ is een tautologie desda A en B dat beide zijn. In het bijzonder geldt vanwege de notatie (1.21) *dat $\vDash A \leftrightarrow B$ desda $\vDash A \to B$ en $\vDash B \to A$.*

Bewijs. 1. De claim $\vDash A \leftrightarrow B$ betekent dat $v(A \leftrightarrow B) = 1$ voor alle valuaties v. Uit de waarheidstabel voor $\leftrightarrow$ zie je dat dit precies zo is als ofwel $v(A) = v(B) = 0$, ofwel $v(A) = v(B) = 1$, oftewel: als A en B logisch equivalent zijn, d.w.z. $A \leftrightarrow B$.

2. De aanname is $v(A) = 1$ en $v(A \to B) = 1$ voor iedere valuatie v. Volgens de waarheidstabel van $\to$ is dit alleen mogelijk als $v(B) = 1$, voor alle v.

3. Analoog uit de waarheidstabel van $\wedge$, ga zelf na. Q.E.D

Hier volgen vele tautologieën, waarvan die met $\leftrightarrow$ volgens Stelling 1.3.3 ook waar zijn als we $\to$ of $\leftarrow$ in plaats van $\leftrightarrow$ nemen (waarbij $A \leftarrow B$ hetzelfde betekent als $B \to A$):

$$\vDash A \wedge B \leftrightarrow B \wedge A; \tag{1.26}$$
$$\vDash A \vee B \leftrightarrow B \vee A; \tag{1.27}$$
$$\vDash \neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B); \tag{1.28}$$
$$\vDash \neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B); \tag{1.29}$$
$$\vDash (A \to B) \leftrightarrow (\neg B \to \neg A); \tag{1.30}$$
$$\vDash (A \to B) \leftrightarrow (\neg A \vee B); \tag{1.31}$$
$$\vDash (A \to B) \leftrightarrow \neg(A \wedge \neg B); \tag{1.32}$$
$$\vDash A \wedge B \leftrightarrow \neg(A \to \neg B); \tag{1.33}$$
$$\vDash A \vee B \leftrightarrow (\neg A \to B); \tag{1.34}$$
$$\vDash \neg A \to (A \to B); \tag{1.35}$$
$$\vDash B \to (A \to B); \tag{1.36}$$
$$\vDash (A \wedge B) \wedge C \leftrightarrow A \wedge (B \wedge C); \tag{1.37}$$
$$\vDash (A \vee B) \vee C \leftrightarrow A \vee (B \vee C); \tag{1.38}$$
$$\vDash (A \vee B) \wedge C \leftrightarrow (A \wedge C) \vee (B \wedge C); \tag{1.39}$$
$$\vDash (A \wedge B) \vee C \leftrightarrow (A \vee C) \wedge (B \vee C); \tag{1.40}$$
$$\vDash A \to (B \wedge C) \leftrightarrow (A \to B) \wedge (A \to C). \tag{1.41}$$

In al deze tautologieën zijn A, B, en vanaf (1.37) ook C willekeurige uitspraken, volgens de regels opgebouwd uit de atomaire proposities P_i, $\bot$, en de logische verbinders $\neg, \wedge, \vee, \rightarrow$. *Een abstracte tautologie als* $A \wedge B \leftrightarrow B \wedge A$ *staat dus eigenlijk voor oneindig veel concrete tautologieën waarin voor* A *en* B *specifieke uitspraken worden ingevuld.*

Vgl. (1.26) en (1.27) zeggen dat $\wedge$ en $\vee$ zich gedragen zoals je van "en" en "of" verwacht, behalve dat $A \wedge B$ niet *gelijk is* aan $B \wedge A$; deze uitspraken zijn slechts *logisch equivalent*.[6] Ook het combineren van drie uitspraken via $\wedge$ en $\vee$ is zoals verwacht, zie (1.37) t/m (1.40). De volgende twee, (1.28) en (1.29), heten de ***wetten van De Morgan***. Vgl. (1.30) is de ***contrapositief*** en de volgende twee zijn daar varianten van. De tautologieën (1.33) en (1.34) stellen ons in staat om de symbolen $\wedge$ en $\vee$, te elimineren. Stel namelijk dat je $\nu(A)$ wilt bepalen via de rekenmethode die uitgaat van (1.1) t/m (1.9). Uit (1.33) en Stelling 1.3 volgt dat overal waar je $\nu(A \wedge B)$ tegenkomt, je hetzelfde (0 of 1) krijgt als er $\neg(A \rightarrow \neg B)$ had gestaan in plaats van $A \wedge B$. Analoog kun je via (1.34) overal $\vee$ vervangen. Voor het berekenen van de (on)waarheid van een uitspraak maakt het dus niets uit of er $A \wedge B$ staat of $\neg(A \rightarrow \neg B)$, en analoog voor $A \vee B$ of $\neg A \rightarrow B$. Je kunt in waarheidsbepalingen $\wedge$ en $\vee$ dus als *afkortingen* beschouwen voor resp.

$$A \wedge B := \neg(A \rightarrow \neg B); \tag{1.42}$$

$$A \vee B := \neg A \rightarrow B, \tag{1.43}$$

en dan in principe alleen met $\rightarrow$, $\neg$ en $\bot$ werken. Hieruit kan $\neg$ ook nog worden vervangen via (1.23), volgens welke we zelfs de negatie $\neg$ als *afkorting* kunnen zien via

$$\neg A := A \rightarrow \bot. \tag{1.44}$$

Dan blijven dus alleen $\rightarrow$ en $\bot$ over! Wat semantiek betreft kun je propositielogica dus bedrijven met slechts deze twee symbolen (en we zullen zien dat dit ook geldt voor bewijzen). Alternatief kun je via (1.31) en (1.32) $\rightarrow$ elimineren ten gunste van $\vee$ en $\wedge$, zodat je in plaats van $\rightarrow$ en $\bot$ ook uitsluitend $\vee$ en $\bot$, ofwel $\wedge$ en $\bot$ kunt gebruiken.

Nos. (1.35), (1.36), en (1.41) komen vaak voor en staan er voor later gebruik. We komen tot slot ook nog even terug op de tautologieën met alleen A. Vgl. (1.16) stelt dat iedere uitspraak uit *falsum* volgt. Vgl. (1.17) is de ***wet van de uitgesloten derde*** of ***tertium non datur***: een van de twee A of $\neg A$ is altijd waar.[7] No. (1.24) zegt dat je een dubbele ontkenning net zo goed weg kan laten.[8] No. (1.25) is de ***wet van de contradictie***, die zegt dat de combinatie van A en haar ontkenning $\neg A$ altijd onwaar is (logisch toch?).

6. Vgl. (1.26) en (1.27) drukken bijna uit dat $\wedge$ en $\vee$ *commutatief* zijn, behalve dat $=$ vervangen is door $\leftrightarrow$ (bijv. friet en mayonaise is logisch equivalent met mayonaise en friet, resp. mayonaise of satésaus is logisch equivalent met satésaus of mayonaise). Vgl. (1.37) en (1.38) drukken evenzo uit dat $\wedge$ en $\vee$ bijna *associatief* zijn (friet met mayonaise, en dan satésaus is logisch equivalent met friet en dan mayonaise met satésaus, enz.). Ten slotte zeggen (1.39) en (1.40) dat $\wedge$ en $\vee$ ten opzichte van elkaar bijna *distributief* zijn (friet met mayonaise of satésaus $\leftrightarrow$ friet met mayonaise of friet met satésaus, enz.).
7. Deze tautologie wordt in de zogenaamde *intuïtionistische wiskunde* van L.E.J. Brouwer afgwezen.
8. Ook dit is in de intuïtionistische wiskunde niet meer juist; de regel is ook equivalent met de vorige.

1.4 Formeel bewijzen

We hebben op p. 9 al opgemerkt dat de wiskunde een soort spel met spelregels is, en daar zijn de regels voor formeel bewijzen onderdeel van. Deze regels zijn echter niet (zoals bij veel andere spellen) willekeurig. We hebben al opgemerkt dat formeel bewijzen geen gebruik mag maken van de betekenis van de symbolen (dit was het grote inzicht van Boole, Hilbert, en anderen). De opzet van een bewijs heeft in principe dus niets te maken met de valuaties v. Maar het volgende moet beslist vermeden worden: Stel dat een uitspraak A bewezen kan worden, genoteerd als $\boxed{\vdash A}$, en dat er een valuatie v is met $v(A) = 0$. Dan zouden we een stelling hebben bewezen die in een bepaalde wereld onwaar is! De wiskunde kan de tent dan wel sluiten, niemand vertrouwt ons nog. Om dit te voorkomen moet een bewijsbare uitspraak A dus onder alle valuaties v waar zijn, oftewel: een tautologie. Omgekeerd zou het natuurlijk mooi zijn om iedere tautologie te kunnen bewijzen, zodat de droom van de (propositie)logica is:

$$\vdash A \text{ desda } \vDash A. \tag{1.45}$$

We geven nu spelregels voor het bewijzen in propositielogica die deze droom waarmaken. Dit is een kwestie van balans: met teveel regels kun je ook onware uitspraken bewijzen, met te weinig regels kun je niet alle tautologieën bewijzen. Hier zijn ze:

1. $\boxed{\dfrac{A}{A}}$ (*herhaling*)

2. $\boxed{\dfrac{\begin{array}{c}[\neg A]\\ \cdots\\ \cdots\\ \bot\end{array}}{A}}$ (*RAA*)

3. $\boxed{\dfrac{A \quad A \to B}{B}}$ ($\to$-*E* = *Modus Ponens*)

4. $\boxed{\dfrac{\begin{array}{c}[A]\\ \cdots\\ \cdots\\ B\end{array}}{A \to B}}$ ($\to$-*I*)

5. $\boxed{\dfrac{\neg A}{A \to \bot}}$ ($\neg$-*E* = $\bot$-*I*)

6. $\boxed{\dfrac{A \to \bot}{\neg A}}$ ($\neg$-*I* = $\bot$-*E*)

7. $\boxed{\dfrac{A \wedge B}{A}}$ en $\boxed{\dfrac{A \wedge B}{B}}$ ($\wedge$-*E*)

8. $\boxed{\dfrac{A \quad B}{A \wedge B}}$ ($\wedge$-*I*)

9. $\boxed{\dfrac{A \vee B \quad A \to C \quad B \to C}{C}}$ ($\vee$-*E*)

10. $\boxed{\dfrac{A}{A \vee B}}$ en $\boxed{\dfrac{B}{A \vee B}}$ ($\vee$-*I*)

Deze bewijsregels moeten als volgt worden gelezen: *uit wat boven de streep staat volgt wat onder de streep staat*. Als bovenaan de streep A staat, betekent dit dus dat we A al hadden bewezen, bijvoorbeeld in een ander (deel van het) bewijs (of A is een axioma van een theorie, zie later). We mogen deze uitspraak dan steeds blijven gebruiken; dit is de inhoud van regel 1. Hierbij betekenen meerdere uitspraken naast elkaar boven de streep, zoals in regel 3, dat deze *allemaal* al bewezen moeten zijn. Typisch en cruciaal voor wiskundig bewijzen is echter het invoeren van onbewezen *aannamen* (te vergelijken met geleend geld), die later in het bewijs weer moeten worden opgeheven (oftewel terugbetaald). We noteren een aanname *op het moment dat deze voor het eerst wordt ingezet* als $[A]$, zoals in regel 4, of als $[\neg A]$ in regel 2. Dit kan dus op twee manieren:

- Regel 4 treedt op als je uit de aanname A de uitspraak B bewijst (de puntjes staan nu voor een bewijs van B uit A). Dan geldt $A \to B$ als bewezen *en moet de aanname A worden opgeheven; daarna mag ook B niet meer worden gebruikt*. De conclusie $A \to B$ kan verder wél steeds in het bewijs worden gebruikt.
  Het eenvoudigste voorbeeld van deze procedure is het volgende bewijs:

$$\dfrac{\dfrac{[A]}{A}}{A \to A.}$$

  Dit bewijs begint met het invoeren van de aanname A. Dan wordt regel 1 gebruikt om A op de volgende regel te schrijven. Daarmee is de situatie van regel 4 ontstaan, met $B \rightsquigarrow A$, en geeft regel 4 dus de conclusie $A \to A$. Daarmee is $A \to A$ een stelling! Je kunt zo bijna uit het niets iets bewijzen (nl. $A \to A$).

  We bewijzen als voorbeeld van regel 4 nu ook de zogenaamde *positive paradox*:

$$\vdash B \to (A \to B). \tag{1.46}$$

$$\dfrac{\dfrac{\dfrac{[A] \quad [B]}{B}}{A \to B}}{B \to (A \to B)}$$

  Stap 1: Invoering van twee aannamen $[A]$ en $[B]$ (dat mag ook!).
  Stap 2: Regel 1 toegepast op B.
  Stap 3: Regel 4 op de aanname $[A]$ (nu opgeheven) en de conclusie B.
  Stap 4: Regel 4 op de aanname $[B]$ (nu opgeheven) en de conclusie $A \to B$.

- Regel 2 (***reductio ad absurdum***,[9] oftewel ***bewijs uit het ongerijmde***, Engels: *proof by contradiction* of *indirect proof*), beschrijft de situatie waarin je $\bot$ bewijst uit de aanname $\neg A$ (de puntjes staan voor een bewijs van $\bot$ uit $\neg A$). In dat geval mag je A concluderen, d.w.z. A is bewezen, *en zodra je dat doet moet de aanname $\neg A$ worden opgeheven* (bijvoorbeeld door deze door te strepen).
  Dan mag de voorlopige conclusie $\bot$ ook niet meer worden gebruikt.
  Hier is een voorbeeld. We gaan bewijzen dat $\vdash (\bot \to A)$, voor willekeurige A:

9. Deze regel werd al door de oude Grieken gebruikt, zie bijvoorbeeld het bewijs van Stelling 5.10. Dat bewijs gebruikt ook de techniek van ***gevalsonderscheiding***, die gerechtvaardigd is door bewijsregel 9.

$$\dfrac{\dfrac{\dfrac{[\bot] \quad [\neg A]}{\bot}}{A}}{\bot \to A}$$

We beginnen met twee aannames. Op de aanname $\bot$ passen we regel 1 toe, waarna we regel 2 toepassen, met conclusie A (en de aanname $\neg A$ opheffen). Daarmee is de situatie van regel 4 ontstaan, met $A \rightsquigarrow \bot$ en $B \rightsquigarrow A$. De conclusie van regel 4 onder de streep, $A \to B$, wordt dus $\bot \to A$. Zodra we dat opschrijven moet de aanname $\bot$ worden opgeheven en zijn we klaar.

Deze voorbeelden geven aan wat wordt bedoeld met een formeel bewijs. Samengevat:

Definitie 1.4 *Een* **bewijs** *van een uitspraak C is een eindige lijst met bovenaan aannamen en/of al bewezen uitspraken en/of axioma's (zie volgende sectie), op iedere volgende rij een of meer uitspraken die volgens bewijsregels 1 t/m 10 (of daaruit afgeleide bewijsregels zoals A t/m H onder) uit de vorige regels volgen, en helemaal onderaan C (aannamen kunnen in ieder stadium worden ingevoerd, als ze uiteindelijk maar weer worden opgeheven). Een aldus bewezen uitspraak heet een* **stelling**.

Een bewijs is pas af als alle aannamen zijn opgeheven! Uit regels 1, 3, en 4 volgt nu dat:

$$\vdash A \to B \text{ feitelijk hetzelfde betekent als } \frac{A}{B}. \tag{1.47}$$

Als je namelijk weet dat $A \to B$ een stelling is, mag je deze in het rechterlid naast A schrijven, en uit regel 3 de conclusie B trekken. Als je omgekeerd weet dat B uit A kan worden bewezen, kun je de aanname $[A]$ invoeren, daaruit B bewijzen, waarna uit regel 4 de conclusie $A \to B$ volgt, onder opheffing van de aanname A. We zullen zo dadelijk zien dat deze observatie een speciaal geval is van de *Deductiestelling* 1.5. Evenzo volgt uit regel 7 en onze manier van formele bewijzen opschrijven, waarin door een spatie worden gescheiden uitspraken op dezelfde regel alle tegelijk gelden, dat:

$A \wedge B$ op een gegeven regel hetzelfde is als A naast B (gescheiden door een spatie).

Regels 3 t/m 10 komen in paren: een ***eliminatieregel*** voor een bepaald logisch symbool met daarnaast een ***introductieregel*** voor datzelfde symbool. Dit wordt aangegeven door bijvoorbeeld $\to$-E voor $\to$-Eliminatie en $\to$-I voor $\to$-Introductie; als je een bewijs uitlegt kun je ofwel de nummers of de namen van de gebruikte bewijsregels vermelden. Regel 3, $\to$-Eliminatie, is de klassieke ***Modus Ponens*** (er is ook een ***Modus Tollens***, zie onder). De daarmee gepaarde $\to$-Introductie, regel 4, reguleert het bewijzen onder onbewezen aannamen, zie boven. Regels 5 en 6 zijn een gevolg van het feit dat we het symbool $\bot$ gebruiken; dit is niet strikt noodzakelijk maar wel erg handig (je kunt ze weglaten als je alleen $\neg$ gebruikt, in welk geval onderaan regel 2 moet staan $B \wedge \neg B$). Regels 7 t/m 10 formaliseren onze intuïtie over "en" en "of".

Er zijn vele nuttige ***afgeleide bewijsregels***, die uit de 10 basisregels volgen, zoals:

A. $\dfrac{\bot}{A}$ (*ex falso sequitur quod libet*) B. $\dfrac{A \to B \quad B \to C}{A \to C}$ (*Transitiviteit* $\to$)

C. $\dfrac{\neg B \quad A \to B}{\neg A}$ (*Modus Tollens*) D. $\dfrac{\neg B \to \neg A}{A \to B}$ (*Contrapositief*)

E. $\dfrac{A \vee B \quad \neg A}{B}$ ($\vee$*-E versie 2*); F. $\dfrac{A \quad \neg A}{\bot}$ ($\neg$*-E =* $\bot$*-I versie 2*)

G. $\dfrac{\neg\neg A}{A}$ (*RAA versie 2*) H. $\dfrac{A \leftrightarrow B \quad B \leftrightarrow C}{A \leftrightarrow C}$ (*Transitiviteit* $\leftrightarrow$)

Hier wordt met "versie 2" bedoeld dat we in plaats van regel 9 voor $\vee$-Eliminatie ook regel E zouden kunnen postuleren (en dan precies dezelfde stellingen kunnen bewijzen), in plaats van regel 5 ook regel F, en in plaats van regel 2 ook regel G. Je mag deze extra bewijsregels altijd gebruiken. Het is leerzaam om deze equivalenties te bewijzen:

A.
$$\dfrac{\dfrac{\bot \quad [\neg A]}{\bot}}{A}$$

B.
$$\dfrac{\dfrac{\dfrac{A \to B \qquad\qquad B \to C}{A \to B \quad [A] \quad B \to C}}{B \qquad\qquad B \to C}}{\dfrac{C}{A \to C}}$$

Geef zelf de uitleg bij het linkerbewijs van A. Voor het rechterbewijs van B:
Stap 1: regel 1 (2x) en invoering aanname $[A]$.
Stap 2: $\to$-Eliminatie op $[A]$ en $A \to B$, geeft dus B, herhaling $B \to C$
Stap 3: $\to$-Eliminatie op B en $B \to C$, geeft dus C.
Stap 4: $\to$-Introductie op de aanname $[A]$ (nu opgeheven) geeft $A \to C$.

C. Het bewijs van de *Modus Tollens* is een speciaal geval van B (opgave).

D. Contrapositief:
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\neg B \to \neg A}{\neg B \to \neg A \quad [\neg B]}}{A \to \bot \quad [A]}}{\bot}}{B}}{A \to B}$$

Stap 1: regel 1 en invoering aanname $[\neg B]$.
Stap 2: $\to$-Eliminatie op $[\neg B]$ en $\neg B \to \neg A$ (N.B. $\neg A := A \to \bot$).
Stap 3: $\to$-Eliminatie op $[A]$ en $A \to \bot$.
Stap 4: RAA op de aanname $[\neg B]$ (nu opgeheven) en $\bot$.
Stap 5: $\to$-Introductie op de aanname $[A]$ (nu opgeheven) en B.

E. Opgave!

F. versie 2 uit versie 1:
$$\dfrac{\dfrac{A \quad \neg A}{\bot}}{\bot}$$
versie 1 uit versie 2:
$$\dfrac{\dfrac{[A] \quad \neg A}{\bot}}{A \to \bot}$$

In het linkerbewijs gebruiken we regel 1 om opnieuw A op te schrijven en dan regel 5 om van $\neg A$ naar $A \to \bot$ te gaan. Dan gebruiken we regel 3 oftewel $\to$-E met $B \rightsquigarrow \bot$. Het rechterbewijs gaat juist met $\to$-I (vul aan!).

G. versie 2 uit versie 1:
$$\dfrac{\dfrac{\neg(\neg A) \quad [\neg A]}{\bot}}{A}$$
(regel F en regel 2). Omgekeerd: opgave!

De bewijstechniek wordt hopelijk duidelijk uit nog meer voorbeelden.

1. $\vdash A \to \neg\neg A$. Bewijs:
$$\dfrac{\dfrac{\dfrac{\dfrac{[A] \quad [\neg A]}{\bot}}{\neg A \to \bot}}{\neg\neg A}}{A \to \neg\neg A}$$

Stap 1: regel F. **Stap 2:** $\to$-I op de aanname $[\neg A]$ (nu opgeheven) en $\bot$;
Stap 3: regel 6 met $A \rightsquigarrow \neg A$; **Stap 4:** $\to$-I op $[A]$ (nu opgeheven).

2. $\vdash \neg A \to (A \to B)$. Dit is een voorbeeld met $\bot$-Eliminatie (geef zelf uitleg):
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A] \; [A \to \bot]}{\bot}}{B}}{A \to B}}{(A \to \bot) \to (A \to B)}}{\neg A \to (A \to \bot) \quad (A \to \bot) \to (A \to B)}}{\neg A \to (A \to B)}$$

3. $\vdash (B \to (C \to D)) \to ((B \to C) \to (B \to D))$. Deze is pittig. *Here we go:*
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[B] \qquad [B \to C]}{C \qquad B \qquad [B \to (C \to D)]}}{C \qquad C \to D}}{D}}{B \to D}}{(B \to C) \to (B \to D)}}{(B \to (C \to D)) \to ((B \to C) \to (B \to D))}$$

Stap 1: $\to$-Eliminatie op B en $B \to C$ en regel 1 (herhaling B).
Stap 2: $\to$-Eliminatie op B en $B \to (C \to D)$.
Stap 3: $\to$-Eliminatie op C en $C \to D$.
Stap 4: $\to$-Introductie op aanname $[B]$ (daarna opgeheven) en D.
Stap 5: $\to$-Introductie op aanname $[B \to C]$ (daarna opgeheven) en $B \to D$.
Stap 6: $\to$-Introductie opaanname $[B \to (C \to D)]$ (...) en $(B \to C) \to (B \to D)$.

4. $\vdash (\neg A \to A) \to A$. Bewijs:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg A \to A] \quad [\neg A]}{A}}{A \quad A \to \bot}}{\bot}}{A}}{(\neg A \to A) \to A}$$

Stap 1: Invoering aannames $\neg A \to A$ en $\neg A$. **Stap 2:** Modus Ponens.
Stap 3: Regel 1 op A en regel 5 op $\neg A$. **Stap 4:** Modus Ponens.
Stap 5: RAA op aanname $\neg A$ met conclusie $\bot$ geeft A (onder opheffing $[\neg A]$).
Stap 6: $\to$-Introductie op aanname $\neg A \to A$ en de conclusie A geeft de laatste regel, waarbij ten slotte ook de aanname $[\neg A \to A]$ wordt opgeheven.

Nu volgen nog een paar voorbeelden met $\wedge$ en $\vee$.

5. $\vdash ((A \to B) \wedge (\neg A \to B)) \to B$. Bewijs (met behulp van de vorige stelling):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[(A \to B) \wedge (\neg A \to B)]}{A \to B \quad \neg A \to B \quad [\neg B]}}{\neg A \to B \quad \neg A}}{B}}{\neg B \to B}}{(\neg B \to B) \to B}}{B}}{((A \to B) \wedge (\neg A \to B)) \to B}$$

Stap 1: Invoering aanname $(A \to B) \wedge (\neg A \to B)$.
Stap 2: Twee keer $\wedge$-Eliminatie (regel 7) en invoering aanname $\neg B$.
Stap 3: Modus Tollens (regel C).
Stap 4: Modus Ponens op $\neg A$ en $\neg A \to B$.
Stap 5: Regel 3 op (nu opgeheven) aanname $[\neg B]$ en net bereikte conclusie B.
Stap 6: Nu gebruiken we de stelling van het vorige onderdeel no. 4 met $A \rightsquigarrow B$ (omdat deze stelling voor alle A geldt, mogen we voor A dus B invullen.
Stap 7: Modus Ponens op de vorige twee regels: $\neg B \to B$ en $(\neg B \to B) \to B$.
Stap 8: Regel 3 op de (nu opgeheven) aanname $[(A \to B) \wedge (\neg A \to B)]$ bovenaan het bewijs en de net bereikte conclusie B. Beide aannamen zijn opgeheven!

6. $\vdash A \vee \neg A$. Bewijs (met behulp van de vorige stelling, geef zelf de uitleg), en de afkorting $B := (A \to (A \vee \neg A)) \wedge (\neg A \to (A \vee \neg A))$,

$$\dfrac{\dfrac{\dfrac{\dfrac{[A] \quad [\neg A]}{A \vee \neg A \quad A \vee \neg A}}{A \to (A \vee \neg A) \quad \neg A \to (A \vee \neg A)}}{B \quad B \to (A \vee \neg A)}}{A \vee \neg A}$$

1.5 Het verband tussen waarheid en bewijsbaarheid

Het formeel bewijzen van een uitspraak is een totaal andere bezigheid dan het bepalen van de (on)waarheid ervan. We hebben echter al de logische droom (1.45) genoemd (geen bedrog): *een uitspraak A is bewijsbaar dan en slechts dan als deze een tautologie is* (d.w.z., waar is onder alle mogelijke valuaties v). We zullen het bewijs van (1.45) slechts één kant op schetsen, maar dan wel algemener. Een wezenlijke uitbreiding is namelijk om stellingen *vanuit axioma's* te bewijzen. ***Axioma's*** (over een gegeven lijst $L = \{P_1, P_2, \ldots\}$ van atomaire proposities) zijn zelf uitspraken en een lijst axioma's heet in de logica een ***theorie***. Een theorie is dus een lijst uitspraken $T := \{A_1, A_2, \ldots\}$.

- De notatie $T \vdash A$ betekent dat een uitspraak A via de bewijsregels uit de vorige sectie in eindig veel stappen te bewijzen is uit de uitspraken in T. Dit houdt in dat overal in het bewijs een willekeurige uitspraak $A_i \in T$ mag worden opgeschreven (niet als aanname: A_i hoeft dus ook nooit te worden opgeheven!).

Als voorbeeld nemen we $T := \{P_1, P_2\}$ en $A := \neg(P_1 \to \neg P_2)$. Dan geldt $T \vdash A$. *Bewijs*:

$$\dfrac{\dfrac{\dfrac{\dfrac{P_1 \qquad P_2 \qquad [P_1 \to \neg P_2]}{\neg P_2}}{\bot}}{(P_1 \to \neg P_2) \to \bot}}{\neg(P_1 \to \neg P_2)}$$

Stelling 1.5 *Voor iedere theorie T en alle uitspraken A en B (over dezelfde A) geldt*

$$T \vdash A \to B \;\; \textit{desda} \;\; T \cup \{A\} \vdash B. \tag{1.48}$$

Dit heet de ***Deductiestelling***.[10] Hier betekent $T \cup \{A\}$ dat A wordt toegevoegd aan de axioma's T, dus als $T := \{A_1, \ldots\}$, dan is $T \cup \{A\} = \{A, A_1, \ldots\}$. Als T leeg is staat er

$$\vdash A \to B \;\; \text{desda} \;\; \{A\} \vdash B. \tag{1.49}$$

Bewijs. Eerst (1.49). Van links naar rechts is *gegeven* dat de uitspraak $A \to B$ een stelling is. De uitdrukking $\{A\} \vdash B$ betekent dat B uit A te bewijzen is. We zetten A naast $A \to B$ en dan volgt B uit $\to$-Eliminatie (regel 3). Van rechts naar links volgt juist uit $\to$-Introductie (regel 4). Het bewijs van (1.48) is een generalisatie van dat van (1.49). Eerst van links naar rechts ($\Rightarrow$). Gegeven $T \vdash A \to B$, hebben we een bewijs

$$\dfrac{\dfrac{A_1 \cdots A_n}{\cdots}}{A \to B}$$

van $A \to B$ uit zeg axioma's A_1 t/m A_n van T (omdat een bewijs eindig veel stappen heeft, gebruikt dit slechts eindig veel axioma's). Voeg nu A toe. Uit A en $A \to B$ volgt B (Modus Ponens); m.a.w. uit het gegeven bewijs van $A \to B$ volgt een bewijs van B:

10. We bewijzen nu, net als in Stelling 1.3, iets *over* propositielogica en niet *binnen* propositielogica. Voor het eerste soort bewijzen hebben we nog geen formele regels gegeven. Die komen nog.

$$\dfrac{\dfrac{\dfrac{A\ A_1 \cdots A_n}{\cdots}}{\cdots}}{\dfrac{A \to B}{B}}$$

Nu van rechts naar links ($\Leftarrow$):

gegeven een bewijs $\dfrac{\dfrac{A_1 \cdots A_n\ A}{\cdots}}{B}$ heb je ook een bewijs $\dfrac{\dfrac{\dfrac{A_1 \cdots A_n\ [A]}{\cdots}}{\cdots}}{\dfrac{B}{A \to B,}}$

waar op het eind $\to$-Introductie is gebruikt (met opheffing van de aanname $[A]$). Q.E.D.

Nu de andere kant: waarheid. Als een valuatie ν voldoet aan $\nu(A_i) = 1$ voor alle axioma's A_i in de theorie T noteren we dat als $\nu(T) = 1$. Een dergelijke valuatie ν heet een ***model*** van T. We voeren in het verlengde daarvan de volgende notatie in:

$$T \vDash A \text{ betekent: } \nu(T) = 1 \Rightarrow \nu(A) = 1. \tag{1.50}$$

In woorden: de notatie $T \vDash A$ betekent dat de uitspraak A waar is in ieder model van de theorie T. Je kunt uit de waarheidstabel voor $\wedge$ bijvoorbeeld makkelijk nagaan dat

$$\{A_1, A_2\} \vDash A_1 \wedge A_2. \tag{1.51}$$

Als $T = \{A\}$ schrijven we in plaats van $\{A\} \vDash B$ en $\{A\} \vdash B$ vaak respectievelijk $A \vDash B$ en $A \vdash B$. Als T leeg is betekent de notatie $\vDash A$ dus dat $\nu(A) = 1$ voor alle valuaties ν. In dat geval is A een tautologie. De definitieve generalisatie van de droom (1.45) is nu:

Stelling 1.6 *Voor iedere theorie T en uitspraak A geldt:* $\boxed{T \vdash A \textit{ desda } T \vDash A}$ *oftewel:*

$$\textit{Als } T \vdash A \textit{ dan } T \vDash A \qquad \textit{(Gezondheid)}; \tag{1.52}$$

$$\textit{Als } T \vDash A \textit{ dan } T \vdash A \qquad \textit{(Volledigheid)}. \tag{1.53}$$

Contrapositief betekent Gezondheid dat $T \nvDash A \Rightarrow T \nvdash A$. Een uitspraak A kan dus geen stelling van T zijn als er ook maar één model van T is waarin A niet waar is:

één tegenvoorbeeld is voldoende om een kandidaat-stelling te weerleggen!

Het bewijs van (1.52) heeft de volgende opzet (die door middel van het principe van volledige inductie kan worden voltooid, zie §5.2): iedere bewijsregel 1 t/m 10 behoudt de waarheid van de vorige regel,[11] zodat de waarheid van de axioma's van T uiteindelijk de waarheid van de conclusie A garandeert (zie opgave 1.13), oftewel $T \vDash A$. Het bewijs van (1.53) is een stuk moeilijker en is onderdeel van het latere vak *Logica*.

11. Regel 4 is een geval apart. De conclusie $\nu(A \to B) = 1$ zou falen als $\nu(A \to B) = 0$, dus als $\nu(A) = 1$ en $\nu(B) = 0$. Dit kan echter niet gebeuren omdat de andere regels de waarheid van A behouden.

1.6 Opgaven bij hoofdstuk 1

Zie ook in Velleman Exercises 1 t/m 7 in §1.1 en 1 t/m 18 in §1.2.
Bij de opgaven onder kun je bij "laat zien" informeel in woorden redeneren. Bij "bewijs formeel" moet je een formeel bewijs geven (en uitleggen) volgens de bewijsregels.

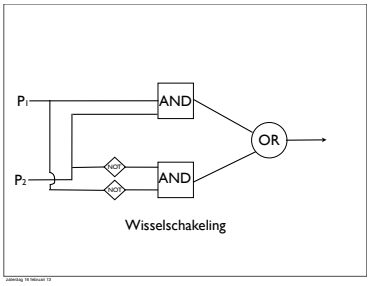
Opgave 1.1

Deze opgave geeft een technologische draai aan de propositielogica. Er bestaat een voor de hand liggend maar interessant verband tussen propositielogica en elektronische circuits, ontdekt door niemand minder dan Claude Shannon (1916–2001), volgens velen de grondlegger van het informatietijdperk. Zo'n circuit heeft ruw gezegd als doel om bij iedere mogelijke stand van n aan/uit schakelaars een lamp wel of niet te doen branden. Het circuit bestaat uit drie soorten poorten, genaamd OR, AND, en NOT, verbonden door draden: de OR en AND poorten hebben twee ingangen en één uitgang, en de NOT part heeft één ingang en één uitgang.[12] Het circuit als geheel heeft n ingangen P_1 t/m P_n, dat zijn de aan/uit schakelaars, en één uitgang, die de lamp voedt. Door alle draden gaat wel of geen stroom, aangegeven met 1 resp. 0; als P_i aan staat geeft die stroom 1, en als hij uit staat stroom 0, aangegeven met $P_i = 0$ of $P_i = 1$.
Een draad kan vertakken (opsplitsen) en bij vertakking houden alle takken dan dezelfde waarde van de stroom. De schakelingen gedragen zich volgens de waarheidstabellen van de bijbehorende logische symbolen: $\vee$ bij OR, $\wedge$ bij AND, en $\neg$ bij NOT (voorbeelden: als 1 in NOT gaat komt er 0 uit, als 1 en 0 in OR gaat komt er 1 uit, enzovoort).
Er zijn nu twee soorten problemen. Het ene is om een circuit te bouwen dat bij iedere mogelijke stand van de schakelaars een gegeven uitgangsstroom heeft. Een klassiek voorbeeld is de wisselschakeling: deze verbindt twee schakelaars ('beneden' en 'boven') met een lamp, die brandt als beide schakelaars aan staan of beide uit staan, maar niet brandt als een van de twee aan staat en de ander uit. Het andere probleem is om bij een gegeven circuit te bepalen of er stroom uit het circuit komt, als functie van de waarden van de P_i. Om dergelijke problemen op te lossen identificeren we iedere schakelaar met een atomaire propositie, iedere poort met het bijbehorende logische symbool (het symbool $\rightarrow$ wordt hier dus niet gebruikt), en het circuit C met een uitspraak C uit de propositielogica. Bij gegeven waarden van de P_i komt er stroom uit C desda $C = 1$. De wisselschakeling correspondeert bijvoorbeeld met de uitspraak

$$C := (\neg P_1 \wedge \neg P_2) \vee (P_1 \wedge P_2), \tag{1.54}$$

en het bijbehorende circuit is

12. In diagrammen kun je de poorten desgewenst met een cirkel, vierkant, e.d. aangeven



a) Geef de waarheidstabel voor de uitspraak (1.54) en ga na dat dit circuit inderdaad de wisselschakeling realiseert.

b) Geef een uitspraak en een circuit dat de volgende schakeling realiseert: er zijn opnieuw twee schakelaars, maar nu brandt de lamp als één van de twee aan is en de andere uit (en brandt niet als ze beide aan of uit staan).

Opgave 1.2

Je kunt een "exclusieve of" invoeren, genaamd $\vee_e$, door middel van

$$A \vee_e B := (A \vee B) \wedge \neg(A \wedge B). \tag{1.55}$$

a) Bereken de waarheidstabel voor $\vee_e$ en concludeer dat dit inderdaad de "exclusieve of" is (informeel: het is het een of het ander, niet beide).

b) Stel nu dat $A := P_1 \to P_2$ en $B := \neg P_1 \to P_2$, waarbij P_1 betekent: "ik heb (tussen mijn kaarten) een koning" en P_2 betekent: "ik heb een aas". Stel dat voor een bepaalde valuatie ν de uitspraak $A \vee_e B$ waar is. Heb ik een aas?

Opgave 1.3

De ***Sheffer stroke*** $|$ (in de computerwereld vaak NAND genoemd) maakt uit twee bestaande uitspraken A en B een nieuwe uitspraak $A|B := \neg(A \wedge B)$.

a) Geef de waarheidstabel van de Sheffer stroke.

b) Laat zien dat de uitspraken $\neg A \leftrightarrow (A|A)$ en $A \vee B \leftrightarrow (A|A)|(B|B)$ voor iedere valuatie ν waar zijn (oftewel: tautologieën zijn, zie §1.3).

Opgave 1.4

Laat zien dat de uitspraken in (1.16) t/m (1.20) en (1.35) en (1.36) voor iedere valuatie ν waar zijn (oftewel: tautologieën).

Opgave 1.5

Laat met behulp van Stelling 1.3. zien dat de uitspraken in (1.26) t/m (1.41) tautologieën zijn.

Opgave 1.6

Reken de waarheidstabel voor $\leftrightarrow$ na.

Opgave 1.7

Laat zien dat een uitspraak A een contradictie is desda de negatie $\neg A$ een tautologie is, en dat $\neg A$ een contradictie is desda A een tautologie is.

Opgave 1.8

Bewijs (formeel) de volgende uitspraken ((1.58) is de inverse *Modus Tollens*):

$$\vdash (A \to B) \to ((B \to C) \to (A \to C)); \tag{1.56}$$
$$\vdash A \to (B \to (\neg A \to \neg B)); \tag{1.57}$$
$$\vdash (A \to B) \to (\neg B \to \neg A). \tag{1.58}$$

Opgave 1.9

Laat zien dat de *Modus Tollens* (afgeleide bewijsregel C) een speciaal geval is van de afgeleide bewijsregel B.

Opgave 1.10

Laat zien dat bewijsregel 9 in aanwezigheid van alle andere bewijsregels equivalent is met de afgeleide bewijsregel E.

Opgave 1.11

Maak het argument in de tekst af dat bewijsregel 2 (RAA) equivalent is met de afgeleide bewijsregel G (geef dus de implicatie: versie 1 uit versie 2).

Opgave 1.12

Leg alle stappen uit in bewijzen no. 2 en 6 op resp. pagina 22 en 23.

Opgave 1.13

Verifieer (met behulp van de waarheidstabellen) voor alle bewijsregels 1 t/m 10 op pagina 19 (behalve regel 2 en regel 4) de volgende eigenschap: voor iedere valuatie v waarvoor alle uitspraken boven de streep waar zijn, is ook de uitspraak onder de streep waar. *Toelichting*: dit is al bijna het bewijs van (1.52).

Opgave 1.14

Ga na dat alle stellingen die in §1.4 bewezen zijn, ook tautologieën zijn (in overeenstemming met Stelling 1.6).

2

Wiskunde met variabelen: Verzamelingen en eerste-orde logica

Verzamelingen geven een basis voor de gehele wiskunde en daarmee ook een context voor variabelen. In het eenvoudigste geval is een verzameling een *eindige* lijst $X = \{X_1, \ldots, X_n\}$, waarbij de X_i de (nader te specificeren) *elementen* van X heten en de typische haakjes $\{\cdots\}$ deze elementen, gescheiden door een komma, samenvoegen. De volgorde van de opsomming binnen de haakjes maakt niet uit, dus $\{X_1, X_2\}$ is hetzelfde als $\{X_2, X_1\}$, enz. Voor eindige verzamelingen voeren we het symbool $\in$ in: als $X = \{X_1, \ldots, X_n\}$ en x is een van deze X_i, dan geldt $\boxed{x \in X}$. Zo niet, dan schrijven we $\boxed{x \notin X}$: dit betekent $\boxed{\neg(x \in X)}$. Zoals we zullen zien is *ieder wiskundig object primair gedefinieerd als een verzameling*. Dat leidt alvast tot een verrassende eerste conclusie:

elementen van verzamelingen zijn zelf ook verzamelingen!

Met eindige verzamelingen–waar we overigens ook de precieze regels en notatie nog voor moeten geven!–kun je echter slechts beperkte wiskunde bedrijven. In de 19e eeuw zetten wiskundigen als Cantor, Dedekind, en Frege daarom een theorie van oneindige verzamelingen op en vroegen zij zich ook af wat een verzameling in haar diepste wezen "is". Hun pogingen om deze absolute essentie te doorgronden liepen echter vast. Dit leidde tot een koerswijziging die typisch is voor de moderne wiskunde als geheel:

- Zeg niet wat een verzameling "is" maar geef *regels* waaraan verzamelingen moeten voldoen en hoe je ze kunt manipuleren. Het blijkt bijvoorbeeld dat het symbool $\in$ via de juiste regels voor *alle* verzamelingen gebruikt kan worden.
- Geef in het bijzonder regels hoe je uit bestaande verzamelingen nieuwe maakt.

We geven deze regels eerst informeel en bouwen al doende de relevante notatie op.

1. *Een verzameling is bepaald door haar elementen: als voor twee verzamelingen X en Y geldt dat een element in X ligt desda het in Y ligt, dan geldt $X = Y$.*
2. *Uit een bestaande verzameling Z kan een nieuwe verzameling X worden gemaakt door een* **predikaat** F *op Z, d.w.z. een eigenschap die de elementen van Z al dan niet kunnen hebben. Deze nieuwe verzameling wordt genoteerd als*

$$X = \{x \in Z \mid F(x)\}. \tag{2.1}$$

Aangezien we nu nog geen enkel voorbeeld van een verzameling hebben en het idee van een "predikaat" ook nog niet precies duidelijk is (komt allemaal later), kunnen we nog geen precies voorbeeld van deze regel geven, maar straks zullen we de getallen 0, 1, 2, enzovoort als verzamelingen definiëren. Hierop vooruitlopend: stel $Z = \{0,1,2,3,4,5,6,7,8,9\}$ en $F(x)$ is de eigenschap "x is even": dan geldt $X = \{0,2,4,6,8\}$.[1]

Voor twee willekeurige verzamelingen X en Y voeren we via regel 2 de notatie in:[2]

$$X \cap Y := \{x \in X \mid x \in Y\} = \{y \in Y \mid y \in X\}, \tag{2.2}$$

en noemen $X \cap Y$ de ***doorsnede*** van X en Y. Er geldt $x \in X \cap Y$ desda $x \in X$ én $x \in Y$, zodat we (2.2) ook informeel–want niet helemaal volgens de regels–schrijven als

$$X \cap Y = \{x \mid (x \in X) \wedge (x \in Y)\}. \tag{2.3}$$

Als $X = \{1,2,3\}$ en $Y = \{3,4,5\}$ dan is $X \cap Y = \{3\}$. Als $Y = \{4,5,6\}$, dan is de doorsnede $X \cap Y$ *leeg*! Je kunt $X \cap Y$ visualiseren als de doorsnede van twee figuren (*Venndiagrammen*) waarbij het ene X voorstelt en het andere Y, zie Velleman, §1.4.

Als X en Y volgens regel 2 zijn gevormd, oftewel

$$X = \{x \in Z \mid F(x)\}; \qquad Y = \{x \in Z \mid G(x)\}, \tag{2.4}$$

dus beide gegeven door een (meestal verschillend) predikaat op Z, dan is de doorsnede

$$X \cap Y = \{x \in Z \mid F(x) \wedge G(x)\}, \tag{2.5}$$

d.w.z. dat $x \in Z$ moet voldoen aan zowel $F(x)$ als $G(x)$. Ook bestaat het ***verschil***

$$Y \setminus X = Y - X := \{x \in Y \mid x \notin X\}. \tag{2.6}$$

Als $X \subset Y$ (zie p. 33) schrijven we ook X^c in plaats van $Y - X$ en noemen X^c het ***complement*** van X in Y (bij de notatie X^c moet dan duidelijk zijn dat $X \subset Y$).

3. *Er bestaat een verzameling zonder elementen, d.w.z. de* **lege verzameling** $\emptyset$.
   Deze verzameling heeft geen enkel element (en is dankzij regel 1 ook uniek met deze eigenschap) en wordt vanaf nu tevens geïdentificeerd met het getal 0. Als $X \cap Y = \emptyset$, en X en Y dus geen element gemeen hebben, dan heten ze ***disjunct***.
4. *Voor alle verzamelingen X en Y bestaat een nieuwe verzameling*

   $$Z = \{X, Y\},$$

   met als elementen X en Y (deze verzameling is volgens de eerste regel uniek).

1. Hier zit een dramatische geschiedenis achter. Frege probeerde (2.1) eerst zonder Z, d.w.z. hij dacht dat ieder predikaat F een verzameling $X = \{x \mid F(x)\}$ definieerde. Russell wees er toen op dat het predikaat $F(x)$ gegeven door $x \notin x$ tot een tegenspraak leidt. Neem de verzameling $R = \{x \mid x \notin x\}$, die volgens Frege moet bestaan. Maar $R \in R$ impliceert $R \notin R$, terwijl $R \notin R$ leidt tot $R \in R$, zodat de uitspraken $R \in R$ en $R \notin R$ logisch equivalent zijn. Ze zijn echter ook met elkaar in tegenspraak, want $R \notin R$ staat voor $\neg(R \in R)$. Volgens de tautologie (1.17) geldt minstens een van deze twee uitspraken, maar dan geldt dus ook de andere uitspraak, waarmee de tautologie (1.25) tot het *falsum* $\perp$ leidt. Dit is de beroemde ***Paradox van Russell***, die door Zermelo werd opgelost door de eis dat X moet ontstaan uit een al bekende verzameling Z.
2. De notatie $A := B$ betekent dat een nieuw iets A per definitie gelijk is aan een bekend iets B.

Als we hierin $Y = X$ nemen en beseffen dat volgens de eerste regel geldt

$$\{X, X\} = \{X\}, \tag{2.7}$$

dan volgt uit regel 4 dat *voor iedere verzameling* X *een nieuwe verzameling* $\{X\}$ *bestaat met als enige element* X. De enige verzameling die we tot nu toe kenden was $\emptyset$, waarmee we tot nul konden tellen, maar nu kunnen al we verder tellen tot twee:[3]

$$0 := \emptyset; \qquad 1 := \{\emptyset\} = \{0\}; \qquad 2 := \{\emptyset, \{\emptyset\}\} = \{0, 1\}. \tag{2.8}$$

Dit is een voorbeeld van het al genoemde idee dat ook de elementen van een verzameling verzamelingen zijn, zodat die elementen zelf ook weer elementen hebben, behalve de lege verzameling $\emptyset$ die géén elementen heeft! Om verder te tellen (en los daarvan meer verzamelingen te kunnen construeren) gebruiken we weer een nieuwe regel:[4]

5. *Voor iedere verzameling* X *bestaat een verzameling* $\cup X$*, genaamd de* **vereniging** *van* X*, met als elementen:* ***de elementen van de elementen van*** X. D.w.z.

$$\cup X = \{x \mid \text{er is een } z \in X \text{ zodat } x \in z\}, \tag{2.9}$$

en dit is de *definitie* van het symbool $\cup$. Als speciaal geval van (2.9) nemen we

$$X \cup Y := \cup\{X, Y\}, \tag{2.10}$$

zodat $x \in X \cup Y$ desda $x \in X$ of $x \in Y$ (of beide, zoals altijd bij "of" in logica).

Opnieuw vooruitlopend op goede definities van getallen, stel dat $X = \{1, 2, 3\}$ en $Y = \{4, 5, 6\}$, dan volgt $X \cup Y = \{1, 2, 3, 4, 5, 6\}$. Als echter $Y = \{2, 3, 4\}$ (met dezelfde X), dan is $X \cup Y = \{1, 2, 3, 4\}$; dat is namelijk dezelfde verzameling als $\{1, 2, 2, 3, 3, 4\}$.

Stel ook weer dat (2.4) geldt, dan is

$$X \cup Y = \{x \in Z \mid F(x) \vee G(x)\}, \tag{2.11}$$

dat wil zeggen dat $x \in Z$ moet voldoen aan ofwel $F(x)$ ofwel $G(x)$. Informeel:

$$X \cup Y = \{x \mid (x \in X) \vee (x \in Y)\}. \tag{2.12}$$

Nu we de *vereniging* $\cup X$ hebben, kunnen we ook de ***doorsnede*** $\cap X$ definiëren door

$$\cap X = \{x \in \cup X \mid \text{ voor alle elementen } Z \in X \text{ geldt } x \in Z\}. \tag{2.13}$$

Net als voor $\cup$ geldt de notatie

$$X \cap Y := \cap\{X, Y\}, \tag{2.14}$$

3. Dit is niet de enige manier om natuurlijke getallen binnen de verzamelingenleer te definiëren. Zermelo schreef bijvoorbeeld $2 = \{\{\emptyset\}\}$ in plaats van (2.8), en dan $3 = \{\{\{\emptyset\}\}\}$, enzovoort, zodat $n + 1 = \{n\}$, in plaats van $n + 1 = \{0, 1, \ldots, n\}$ zoals in (2.18) beneden. Er is ook nog een veel ingewikkeldere definitie van Frege, overgenomen door Russell, waarin het getal n is gedefinieerd als de verzameling van alle verzamelingen met n (verschillende) elementen. Wij volgen von Neumann.

4. In (2.9) moet officieel $\{x \in \text{een verzameling} \mid \cdots\}$ staan, maar regel 5 geeft deze verzameling als $\cup X$. Vaak zegt men $\cup_\lambda x_\lambda$ i.p.v. $\cup X$, waar de x_λ de elementen van X zijn, een 'familie van verzamelingen'.

waarbij we de doorsnede (2.2) terugvinden (ga na). De eigenschap (2.5) volgt dan analoog aan (2.11), ga na, en we zien dus dat de vereniging van twee verzamelingen met het logische "of" te maken heeft, en de doorsnede met het logische "en". Zie ook §2.1. Soms kom je ook het ***symmetrische verschil*** $X\Delta Y$ van X en Y tegen, gedefinieerd als

$$X\Delta Y := (X \cup Y) \setminus (X \cap Y) = (X \setminus Y) \cup (Y \setminus X). \tag{2.15}$$

Een speciaal geval van (2.10), waarmee we de natuurlijke getallen gaan construeren, is

$$X^+ := X \cup \{X\} = \cup\{X, \{X\}\}; \tag{2.16}$$

de elementen van X^+ zijn de elementen van X, én X zelf. Dan is $1 = 0^+$, $2 = 1^+$, en

$$3 := 2^+ = 2 \cup \{2\} = \cup\{2, \{2\}\} = \cup\{\{0, 1\}, \{2\}\} = \{0, 1, 2\}, \tag{2.17}$$

en kunnen we ook alle volgende natuurlijke getallen ***recursief*** definiëren door

$$n + 1 := n^+ = \{0, 1, \ldots, n\}. \tag{2.18}$$

Een recursieve definitie of constructie van een serie wiskundige objecten $O(n)$ die van $n \in \mathbb{N}$ afhangen houdt in dat je bij $O(0)$ begint (boven is dat 0 zelf, gezien als de lege verzameling), en aangeeft hoe je $O(n + 1)$ uit $O(n)$ maakt. Zo maak je deze objecten stap voor stap uit het vorige. Zie ook Stelling 5.6.

Naast $\cap$ en $\cup$ bestaat een net zo belangrijk binair symbool $\subset$, het ***inclusiesymbool***.[5]

$X \subset Y$ betekent: ieder element van X ligt ook in Y, oftewel: $(x \in X) \to (x \in Y)$.

We spreken $X \subset Y$ uit als: "X is een deelverzameling van Y". Merk op:

$X = Y$ desda $X \subset Y$ en $Y \subset X$.

Een simpel voorbeeld waarvoor $X \subset Y$ geldt is $X = \{1\}$ en $Y = \{1, 2\}$. Het geldt niet voor $X = \{3\}$ (met dezelfde Y). Ook hier is weer een onderliggend logisch verhaal: als (2.4) geldt, dan is $X \subset Y$ waar desda voor alle x geldt $F(x) \to G(x)$, oftewel: de eigenschap $F(x)$ impliceert de eigenschap $G(x)$, oftewel: voor iedere x waarvoor $F(x)$ geldt, moet ook $G(x)$ gelden (we maken dit soort notaties later precies).

Stel bijvoorbeeld dat Y uit alle even getallen bestaat en dus binnen alle natuurlijke getallen (die volgens regel 7 een verzameling vormen) ligt via het predikaat "x is even", en X bestaat uit alle veelvouden van vier, dan geldt $X \subset Y$, omdat het predikaat "x is een veelvoud van 4" op een natuurlijk getal impliceert dat x even is. In simpele taal uitgedrukt hebben we hier het volgende gezegd: $\{4, 8, 12, \ldots\} \subset \{0, 2, 4, 6, 8, 10, 12, \ldots\}$.

6. *Voor iedere verzameling* X *bestaat de* **machtsverzameling** $P(X)$ *met als elementen de* **deelverzamelingen** $Y \subset X$ *van* X.

5. $\subset$ wordt ook vaak als $\subseteq$ genoteerd. Soms (*maar niet hier*) betekent $X \subset Y$ dat $X \subseteq Y$ en $Y \neq X$.

Zowel X zelf als de lege verzameling $\emptyset$ zijn elementen van $P(X)$. Het eerste is hopelijk duidelijk, het laatste is zo omdat de implicatie $(x \in \emptyset) \to (x \in X)$ voor alle x waar is omdat het antecedent $x \in \emptyset$ altijd onwaar is, zie de waarheidstabel voor $\to$! Met deze opmerking is het makkelijk om een paar eenvoudige voorbeelden te geven:

$$P(\emptyset) = \{\emptyset\} \qquad \text{oftewel } P(0) = 1; \tag{2.19}$$

$$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}; \qquad \text{oftewel } P(1) = 2; \tag{2.20}$$

$$P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}\}\}; \qquad \text{oftewel } P(2) = 3 \cup \{\{1\}\}. \tag{2.21}$$

Het is jammer dat het patroon van de eerste twee niet doorzet, maar onvermijdelijk:

Stelling 2.1 *Als een verzameling* X *bestaat uit* n *verschillende elementen, dan bestaat de machtsverzameling* $P(X)$ *uit* 2^n *verschillende elementen.*

Deze stelling is handig als check op je antwoord als je $P(X)$ moet opschrijven. Als inleiding op het bewijs geven we eerst, naast (2.19) t/m (2.21), nog een voorbeeld:

$$P(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}. \tag{2.22}$$

Inderdaad heeft het rechterlid $8 = 2^3$ elementen, een aantal dat tot stand komt als $1+3+3+1$, waarbij de eerste 1 de lege verzameling meetelt, de eerste 3 de 3 elementen van $X = \{1, 2, 3\}$ telt die ieder als deelverzameling kunnen optreden (waarbij je er goed op moet letten dat als $x \in X$, het desbetreffende element van $P(x)$ niet x zelf is maar $\{x\}$; dit is het verschil tussen $x \in X$ en $\{x\} \subset X$), de tweede 3 de 3 mogelijkheden telt om deelverzamelingen met 2 elementen te kiezen uit 3 elementen, en de laatste 1 de hele verzameling X meetelt. Als X nu n elementen heeft, wordt deze berekening

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} =: \sum_{k=0}^{n} \binom{n}{k} = 2^n, \tag{2.23}$$

hetgeen een speciaal geval is van het Binomium van Newton (5.27) met $a = b = 1$. Dit bewijst Stelling 2.1, want het linkerlid van (2.23) telt het aantal elementen van $P(X)$:

$\binom{n}{0} = 1$ telt de lege verzameling, $\binom{n}{1} = n$ telt het aantal deelverzamelingen van X met 1 element, $\binom{n}{2}$ telt het aantal deelverzamelingen van X met 2 elementen, ..., en ten slotte telt $\binom{n}{n} = 1$ de verzameling X zelf mee. Daarmee is $P(X)$ dus altijd groter dan X!

7. Ten slotte bestaat *de (oneindige) verzameling van* **natuurlijke getallen**

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}; \tag{2.24}$$

tot nu toe bestond alleen voor iedere n de *eindige* verzameling (2.18).

Er zijn nog twee regels, maar die komen in de wiskundige praktijk zelden voor en worden vooral gebruikt door logici die aan axiomatische verzamelingenleer werken. Van groot belang is wel het zogenaamde *keuzeaxioma*, dat we in §4.6 zullen bespreken.

2.1 Verzamelingen en propositielogica

Eigenschappen van verzamelingen lijken vaak op stellingen (oftewel tautologieën) in de propositielogica (zie ook Velleman, §1.4). Het eenvoudigste voorbeeld is de analogie

$$X \cap Y = Y \cap X \qquad\qquad A \wedge B \leftrightarrow B \wedge A; \tag{2.25}$$

1. De linker gelijkheid betekent (volgens regel 1 van de verzamelingenleer) dat voor alle x geldt: $x \in X \cap Y$ desda $x \in Y \cap X$. Dat willen we nu bewijzen.[6]
2. Uit de vorm (2.3) van het symbool $\cap$ volgt dat $x \in X \cap Y$ desda $x \in X$ en $x \in Y$, terwijl $x \in Y \cap X$ desda $x \in Y$ en $x \in X$. Definieer nu de uitspraken

   $$A := x \in X; \qquad\qquad B := x \in Y. \tag{2.26}$$

   De (bi)implicatie $A \wedge B \leftrightarrow B \wedge A$ rechts in (2.25) wordt met de invulling (2.26):

   $$((x \in X) \wedge (x \in Y)) \leftrightarrow ((x \in Y) \wedge (x \in X)). \tag{2.27}$$

   We hebben net gezien dat we dit ook mogen lezen als:

   $$x \in X \cap Y \leftrightarrow x \in Y \cap X. \tag{2.28}$$

   Het bewijs van $X \cap Y = Y \cap X$ is nu bijna rond: de laatste stap is dat als (2.28), oftewel (2.27), voor een *willekeurige* verzameling x is bewezen, de formule dan ook voor *alle* verzamelingen x geldt. We zullen later zien dat dit inderdaad een bewijsregel is in logica met variabelen (d.w.z. eerste-orde logica). Q.E.D.

We geven nu een lijst van nog veel meer van dergelijke eigenschappen van verzamelingen naast inhoudelijk en optisch gerelateerde stellingen uit de propositielogica:

$X \cap Y = Y \cap X$	$A \wedge B \leftrightarrow B \wedge A;$	(2.29)
$X \cup Y = Y \cup X$	$A \vee B \leftrightarrow B \vee A;$	(2.30)
$(X \cap Y)^c = X^c \cup Y^c$	$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B);$	(2.31)
$(X \cup Y)^c = X^c \cap Y^c$	$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B);$	(2.32)
$X \subset Y$ desda $Y^c \subset X^c$	$(A \to B) \leftrightarrow (\neg B \to \neg A);$	(2.33)
$X \subset Y$ desda $X^c \cup Y = Z$	$(A \to B) \leftrightarrow (\neg A \vee B);$	(2.34)
$X \subset Y$ desda $(X \cap Y^c)^c = Z$	$(A \to B) \leftrightarrow \neg(A \wedge \neg B);$	(2.35)
$(X \cap Y) \cap Z = X \cap (Y \cap Z)$	$(A \wedge B) \wedge C \leftrightarrow A \wedge (B \wedge C);$	(2.36)
$(X \cup Y) \cup Z = X \cup (Y \cup Z)$	$(A \vee B) \vee C \leftrightarrow A \vee (B \vee C);$	(2.37)
$(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$	$(A \vee B) \wedge C \leftrightarrow (A \wedge C) \vee (B \wedge C);$	(2.38)
$(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$	$(A \wedge B) \vee C \leftrightarrow (A \vee C) \wedge (B \vee C);$	(2.39)
$\emptyset \subset X$	$\bot \to A;$	(2.40)
$X \cup X^c = Z$	$A \vee (\neg A);$	(2.41)
$X \cap X^c = \emptyset$	$A \wedge \neg A \leftrightarrow \bot;$	(2.42)
$X^{cc} = X$	$\neg\neg A \leftrightarrow A.$	(2.43)

6. We doen dit informeel. De benodigde formele bewijsregels komen pas later aan bod, zie §2.3.

De rechterkolom is het setje tautologieën (1.26) t/m (1.32), en dan (1.37) t/m (1.40), en dan (1.16), (1.17), (1.25), en (1.24).[7] Ten slotte geven we (1.41) en een variant daarop:

$X \subset (Y \cap Z)$ desda $X \subset Y$ en $X \subset Z$ $\quad (A \to (B \wedge C)) \leftrightarrow ((A \to B) \wedge (A \to C))$; (2.44)
$(X \cup Y) \subset Z$ desda $X \subset Z$ en $Y \subset Z$ $\quad ((A \vee B) \to C) \leftrightarrow ((A \to C) \wedge (B \to C))$. (2.45)

We nemen als ingewikkelder voorbeeld dan (2.25) nu (2.38): we bewijzen (informeel)

$$(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z). \tag{2.46}$$

1. In de stelling $(A \vee B) \wedge C \leftrightarrow (A \wedge C) \vee (B \wedge C)$ rechts in (2.38) nemen we:

   $$A := x \in X; \qquad B := x \in Y \qquad C := x \in Z. \tag{2.47}$$

   Met deze invulling is de stelling $(A \vee B) \wedge C \leftrightarrow (A \wedge C) \vee (B \wedge C)$ geworden tot

   $$(x \in X \vee x \in Y) \wedge (x \in Z) \leftrightarrow (x \in X \wedge x \in Z) \vee (x \in Y \wedge x \in Z). \tag{2.48}$$

2. Dankzij (2.12) herkennen we nu $x \in X \vee x \in Y$ als $x \in X \cup Y$ en via (2.3) volgt, net als in het eerste voorbeeld, dat $x \in X \wedge x \in Z$ en $x \in Y \wedge x \in Z$ staan voor respectievelijk $x \in X \cap Z$ en $x \in Y \cap Z$. Dan is (2.48) dus:

   $$(x \in X \cup Y) \wedge (x \in Z) \leftrightarrow (x \in X \cap Z) \vee (x \in Y \cap Z). \tag{2.49}$$

   Nu gebruiken we opnieuw (2.3) in het linkerlid en (2.12) in het rechterlid, zodat

   $$x \in ((X \cup Y) \cap Z) \leftrightarrow x \in ((X \cap Z) \cup (Y \cap Z)). \tag{2.50}$$

3. De laatste stap van het bewijs is hetzelfde als in het eerste voorbeeld: omdat (2.50) is bewezen voor een *willekeurige* verzameling x, geldt de formule voor *alle* verzamelingen x. Uit regel 1 voor verzamelingen volgt dan (2.46). Q.E.D.

Als derde voorbeeld bewijzen we de "De Morgan" eigenschap (2.31) , d.w.z.

$$(X \cap Y)^c = X^c \cup Y^c. \tag{2.51}$$

Dit lijkt eenvoudiger dan het vorige voorbeeld, maar in werkelijkheid moeten we steeds beseffen dat $X \subset Z$ en $Y \subset Z$ voor een zekere verzameling Z, zodat $X^c = Z \setminus X$, het complement van X *in* Z, en $Y^c = Z \setminus Y$ (*idem*), zie de uitleg na (2.6).

1. Er geldt: $x \in (X \cap Y)^c$ desda $x \notin (X \cap Y)$ én $x \in Z$, oftewel $\neg(x \in X \cap Y)$ én $x \in Z$ oftewel $\neg(x \in X \wedge x \in Y) \wedge (x \in Z)$.
2. Neem nu net als in het vorige bewijs (2.47), dan hebben we dus

   $$x \in (X \cap Y)^c \qquad \text{desda} \qquad \neg(A \wedge B) \wedge C. \tag{2.52}$$

7. Om X^c en Y^c te definiëren nemen we aan dat $X \subset Z$ en $Y \subset Z$, voor een zekere verzameling Z.

3. Met soortgelijke argumenten (geef deze zelf) volgt dat

$$x \in (X^c \cup Y^c) \qquad \text{desda} \qquad (\neg A \vee \neg B) \wedge C. \tag{2.53}$$

Om verder te komen moeten we van $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$ in (2.31) naar

$$\neg(A \wedge B) \wedge C \leftrightarrow (\neg A \vee \neg B) \wedge C. \tag{2.54}$$

Dat dit ook een stelling van de propositielogica is kun je zelf bewijzen. Algemener: als $A \leftrightarrow B$ een stelling is, dan is $A \wedge C \leftrightarrow B \wedge C$ dat ook.

4. Vgl. (2.52), (2.53), en (2.54) geven samen $x \in (X \cap Y)^c$ desda $x \in (X^c \cup Y^c)$. Het slot van het bewijs van (2.51) is dan zoals in de vorige twee gevallen. Q.E.D.

Je kunt het linkerlid in (2.29) t/m (2.45) steeds bewijzen met behulp van het rechterlid.[8] Daarbij merk je dat er een woordenboek is tussen verzamelingen en propositielogica:

Verzamelingen	Logische uitspraken
$\cap$	$\wedge$
$\cup$	$\vee$
$\setminus$	$\neg$
$\subset$	$\rightarrow$
$=$	$\leftrightarrow$
$\emptyset$	$\bot$,

waarbij in het geval dat de negatie optreedt de 'verzamelingen' moeten worden beschouwd als deelverzamelingen van een verzameling Z. Ook zien we dat de bi-implicatie $\leftrightarrow$ soms als desda in plaats van $=$ moet worden vertaald, namelijk wanneer aan weerszijden van de vertaling geen verzamelingen komen te staan maar eigenschappen van verzamelingen, zoals $X \subset Y$; zie bijvoorbeeld (2.33) - (2.35).
Merk op dat de machtsverzameling $P(X)$ in dit woordenboek ontbreekt! Om te laten zien dat het bewijzen van eigenschappen daarvan toch ook lijkt op het type bewijs dat we boven van (2.29) hebben gegeven, bewijzen we nu als voorbeeld de eigenschap

$$\cup P(X) = X. \tag{2.55}$$

Volgens regel 1 moeten we bewijzen dat $x \in \cup P(X)$ desda $x \in X$. We bewijzen eerst van links naar rechts, dus de implicatie $x \in \cup P(X) \rightarrow (x \in X)$. Per definitie van $\cup$, zie (2.9), geldt $x \in \cup Y$ desda er een $y \in Y$ is zodat $x \in y$, dus met $Y = P(X)$ is dit: $x \in \cup P(X)$ desda er een $y \in P(X)$ is zodat $x \in y$, oftewel $x \in \cup P(X)$ desda er een $y \subset X$ is zodat $x \in y$. Maar $x \in y$ en $y \subset X$ geeft $x \in X$ per definitie van het $\subset$ symbool.

Omgekeerd: stel $x \in X$ en neem in de vorige regel $y = X$. Deze y voldoet aan $y \subset X$ (want $X \subset X$, zoals we zagen) en tevens aan $x \in y$, de aanname is immers $x \in X$. Dit geeft direct de implicatie $x \in X \rightarrow x \in \cup P(X)$. Daarmee is (2.55) bewezen. Q.E.D.

Analoog kun je als opgave zelf bewijzen dat

$$\cap P(X) = \emptyset. \tag{2.56}$$

8. Je kunt de meeste eigenschappen in de linkerkolom ook visueel begrijpen via Venn-diagrammen, zie Velleman §1.4, maar een echt bewijs moet toch worden geleverd op de bovenstaande manier.

2.2 Eerste-orde logica en verzamelingenleer

Om variabelen te definiëren (als "willekeurige verzamelingen") hebben we een uitgebreidere logische taal nodig. Dit is de *eerste-orde logica* (= *predikaatlogica*). Hierin worden alle symbolen $\neg$, $\wedge$, $\vee$, $\rightarrow$, en $\bot$ van de propositielogica gebruikt, met dezelfde betekenis,[9] evenals haakjes. Daar komen de volgende symbolen bij:[10]

- ***gelijkteken*** $=$.
- ***variabelen***, genaamd $x_1, x_2, \ldots, x, y, z, \ldots$ (altijd kleine letters in deze syllabus);
- ***kwantoren*** $\forall$ ('voor alle') en $\exists$ ('er is/bestaat'), waar *altijd* een variabele aan moet worden gehangen, dus $\forall_x$ ('voor alle x') of $\exists_x$ ('er is/bestaat een x').

In klassieke logica geldt $\boxed{\exists_x = \neg\forall_x\neg}$ zodat we in principe alleen $\forall$ kunnen gebruiken (wat echter niet zo inzichtelijk is). Een bepaalde wiskundige theorie heeft daarnaast nog eigen symbolen, zoals $P_1, P_2, \ldots$ in propositielogica, $+$, $\times$ in rekenkunde, en $\in$ in verzamelingenleer. We kijken nu alleen naar dat laatste. Ofschoon verzamelingenleer in principe alle andere wiskundige theorieën omvat, heeft de verzamelingenleer maar één eigen symbool, namelijk $\boxed{\in \text{ voor 'element van'.}}$ Alle bestaande wiskunde kan dus worden uitgedrukt als: *een verzameling is (niet) gelijk aan een andere verzameling, of is daar (g)een element van!* Daarnaast gebruiken we voor het gemak:

- Namen van *specifieke* verzamelingen, zoals $\emptyset$, $0, 1, 2, \pi, \ldots$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, enz., en X, Y, Z, voor zowel concrete als "vaste maar willekeurige" verzamelingen.

Nu treedt nog een verschil op met propositielogica (PL). Daar had je voor een combinatie C van symbolen twee mogelijkheden: C is zinloos, of C is een ***uitspraak***. In de eerste-orde logica komen hier twee zinvolle combinaties bij: ***termen*** en ***formules***. De eerste bestaan niet in PL, de laatste vallen in PL samen met uitspraken. Per definitie:

0. Een ***term*** t is ofwel een variabele ofwel een naam (zoals $\emptyset$ of $\mathbb{N}$, zie boven).

1. Als t_1 en t_2 termen zijn, zijn $t_1 = t_2$ en $t_1 \in t_2$ ***formules***. Ook $\bot$ is een formule.

2. Nu maken we nog meer formules m.b.v. de andere zuiver logische symbolen:
   1. Als F en G formules zijn, dan zijn $\neg F$, $F \vee G$, $F \wedge G$, en $F \rightarrow G$ dat ook.
   2. Ook $\exists_x F$ en $\forall_x F$ zijn formules, voor een willekeurige variabele x.
   3. Dit proces is iteratief: je kunt de stappen **2**.1 en **2**.2 eindig vaak herhalen.

3. Een ***uitspraak*** is een formule waarin alle variabelen *gebonden* zijn.

Dit laatste betekent dat direct voor de deelformule F waar een variabele x in voorkomt, een kwantor $\forall_x$ of $\exists_x$ staat. Een variabele heet *vrij* als deze niet gebonden is en een uitspraak is dus een formule zonder vrije variabelen. Let op: de constructie van termen is specifiek voor verzamelingenleer en is anders in bijv. rekenkunde of PL. In regel **2**.2 hoeft de variabele x niet eens in F voor te komen om $\exists_x F$ en $\forall_x F$ te kunnen opschrijven.

9. De eliminatie van $\vee$, $\wedge$ en $\neg$ is hetzelfde als voorheen; we kunnen ook in eerste-orde logica slechts $\rightarrow$ en $\bot$ gebruiken. De symbolen voor atomaire proposities komen in eerste-orde logica niet voor.
10. Ook in eerste-orde logica gebruiken we voor het gemak het symbool $:=$ in de metataal.

Net als in PL kun je een uitspraak bewijzen of weerleggen. Je kunt bijvoorbeeld niet eisen dat $x = 1$ wel of niet bewijsbaar is; dat is dan ook 'slechts' een formule. Dat kun je wel eisen van bijv. $\exists_x(x = 1)$ of $\forall_x(x = 1)$, en dat zijn dan ook uitspraken (de eerste is een stelling en de tweede niet!). Soms kan een formule met een vrije variabele echter wel worden bewezen, zoals $x = x$, zie onder. Als een hygiënische extra maatregel (die bovenop de formatieregels komt) spreken we af dat variabelen ofwel *gebonden* ofwel *vrij* zijn ofwel *niet voorkomen* in een formule, en dus niet zowel vrij als gebonden. Om aan te geven dat een formule F *tenminste* de variabele x vrij bevat schrijven we $F(x)$.

Volgens regel 1 zijn $X = Y$, $x = \emptyset$, $x \in X$, en $x \in y$ formules. Hoe zit het met uitdrukkingen als $X \cap Y$ of $\{x, y\}$? Hiervoor geldt de volgende *afgeleide formatieregel*:

1. *extra*: Als t een term is, dan zijn $\cup t$, $\cap t$, $P(t)$, en $\{t\}$ termen. Als t_1 en t_2 termen zijn, dan zijn $\{t_1, t_2\}$, $t_1 \cup t_2$, $t_1 \cap t_2$, en $t_1 \setminus t_2$ termen, en is $t_1 \subset t_2$ een formule.
Als t een term is en $F(x)$ een formule (zie boven), dan is $\{x \in t \mid F(x)\}$ een term.

Uitdrukkingen als $X \cap Y = Y \cap X$ of $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$, zie (2.25) en (2.38), zijn dus *formules*, waarbij X, Y en Z namen van vaste maar willekeurige verzamelingen zijn. Inhoudelijk hetzelfde (zie onder) maar grammaticaal anders kun je ook schrijven:

$$\forall_x \forall_y (x \cap y = y \cap x); \tag{2.57}$$
$$\forall_x \forall_y \forall_z ((x \cup y) \cap z = (x \cap z) \cup (y \cap z)); \tag{2.58}$$

waar (2.25) - (2.38) uit volgen (zie §2.3). Als derde voorbeeld luidt (2.31) met variabelen:

$$\forall_x \forall_y \forall_z (((x \subset z) \wedge (y \subset z)) \to (z \setminus (x \cap y) = (z \setminus x) \cup (z \setminus y)). \tag{2.59}$$

De afgeleide symbolen $\cup$, $\cap$, $\subset$ en $\setminus$ kunnen in principe in het symbool $\in$ en de zuiver logische symbolen $\to$ etc. worden uitgedrukt, maar we kunnen ze gebruiken alsof ze primair zijn. Hun syntactische status is dan als boven, hetgeen we nu in een paar gevallen uitleggen. Termen hebben uitsluitend als doel om in formules terecht te komen!

- Grammaticaal is $t_1 \cup t_2$ een *term*, want voor gegeven verzamelingen t_1 en t_2 is $t_1 \cup t_2$ de verzameling waarvoor geldt: $(x \in t_1 \cup t_2) \leftrightarrow (x \in t_1 \vee x \in t_2)$. Volgens regel 1 kun je dus uit een andere term t de formules $t = t_1 \cup t_2$ en $t \in t_1 \cup t_2$ maken. Dan zijn $t \in t_1 \cup t_2$ en $t = t_1 \cup t_2$ respectievelijk afkortingen voor:[11]

$$t \in t_1 \cup t_2 := t \in t_1 \vee t \in t_2; \tag{2.60}$$
$$t = t_1 \cup t_2 := \forall_x ((x \in t) \leftrightarrow (x \in t_1 \vee x \in t_2)). \tag{2.61}$$

- Analoog is de doorsnede $t_1 \cap t_2$ van t_1 en t_2 een *term*, waarbij je vergeleken met de vereniging $t_1 \cup t_2$ alleen $\vee$ voor $\wedge$ moet verwisselen, zodat er komt te staan:

$$t \in t_1 \cap t_2 := t \in t_1 \wedge t \in t_2; \tag{2.62}$$
$$t = t_1 \cap t_2 := \forall_x ((x \in t) \leftrightarrow (x \in t_1 \wedge x \in t_2)). \tag{2.63}$$

11. We zouden haakjes kunnen plaatsen, bijv. $t \in (t_1 \cup t_2) := (t \in t_1) \vee (t \in t_2)$, maar dergelijke formules zijn maar op één manier correct te lezen. Ga na: $(t \in t_1) \cup t_2$ is alvast ongedefinieerd ($t \in t_1$ is geen term).

- Voor gegeven term t zijn ook de vereniging $\cup t$ en de doorsnede $\cap t$ *termen* (de voorgaande analyse is daar een speciaal geval van, zie (2.10) en (2.14)). Eerst is $\cup t$ volgens (2.9) de verzameling die voldoet aan

$$x \in \cup t \leftrightarrow \exists_{z\in t}(x \in z), \tag{2.64}$$

waarbij we een uiterst belangrijke nieuwe logische afkorting invoeren:

$$\exists_{z\in t}F(z) := \exists_z(z \in t \wedge F(z)), \tag{2.65}$$

d.w.z.: **"er is een element z van t waarvoor de formule $F(z)$ geldt"**. In (2.64) is $F(z)$ dus de formule $x \in z$; de notatie $F(z)$ houdt in dat F *tenminste* z bevat (maar in principe ook andere variabelen kan bevatten). Er geldt dus:

$$t_1 \in \cup t := \exists_{z\in t}(t_1 \in z); \tag{2.66}$$
$$t_1 = \cup t := \forall_x((x \in t_1) \leftrightarrow \exists_{z\in t}(x \in z)). \tag{2.67}$$

Voor later: een verscherping van $\exists_{z\in t}$ is de notatie $\exists!_{z\in t}$, gedefinieerd door

$$\exists!_{z\in t}F(z) := \exists_{z\in t}(\forall_{y\in t}(F(y) \leftrightarrow z = y)), \tag{2.68}$$

oftewel: **"er is een *unieke* z in t waarvoor de formule $F(z)$ geldt."**

- Ook de doorsnede $\cap t$ is een *term*, namelijk de verzameling met

$$x \in \cap t \leftrightarrow \forall_{z\in t}(x \in z), \tag{2.69}$$

waarbij we opnieuw een hele belangrijke nieuwe logische afkorting invoeren:[12]

$$\forall_{z\in t}F(z) := \forall_z(z \in t \to F(z)), \tag{2.70}$$

te lezen als: **"voor iedere z in t geldt de formule $F(z)$"**. Dan hebben we:

$$t_1 \in \cap t := \forall_{z\in t}(t_1 \in z); \tag{2.71}$$
$$t_1 = \cap t := \forall_x((x \in t_1) \leftrightarrow \forall_{z\in t}(x \in z)). \tag{2.72}$$

- Ook $t_2 \setminus t_1$ is voor gegeven t_1 en t_2 een *term*, met als definiërende eigenschappen

$$t \in t_2 \setminus t_1 := t \in t_2 \wedge t \notin t_1; \tag{2.73}$$
$$t = t_2 \setminus t_1 := \forall_x((x \in t) \leftrightarrow (x \in t_2 \wedge x \notin t_1)). \tag{2.74}$$

- De inclusie $t_1 \subset t_2$ is echter geen term maar een *formule*, gedefinieerd door

$$t_1 \subset t_2 := \forall_x(x \in t_1 \to x \in t_2), \tag{2.75}$$

hetgeen met de notatie (2.70), met $F(x) := x \in t_2$, kan worden geschreven als

$$t_1 \subset t_2 := \forall_{x\in t_1}(x \in t_2). \tag{2.76}$$

Definieer zelf op soortgelijke wijze de andere gevallen uit regel 1 *extra*!

12. De notatie $\exists_{z\in t}F(z)$ geeft een nadere *specificatie* van z, namelijk dat de z waarvoor $F(z)$ geldt een element van t is, terwijl $\forall_{z\in t}F(z)$ een *beperking* op z geeft, namelijk dat $F(z)$ alleen wordt beweerd voor elementen z van t en niet voor alle z.

2.3 Axioma's en bewijsregels voor verzamelingenleer

We kunnen nu ook onze eerdere zeven regels van de verzamelingenleer als uitspraken in eerste-orde logica opschrijven. In deze vorm heten ze de *ZF-axioma's*, of **ZF**:[13]

ZF1	$\forall_x \forall_y ((\forall_z(z \in x \leftrightarrow z \in y)) \leftrightarrow x = y)$	(*Extensionaliteitsaxioma*);
ZF2	$\forall_x \exists_y \forall_z (((z \in x) \wedge F(z)) \leftrightarrow z \in y)$	(*Scheidingssaxioma*);
ZF3	$\neg \exists_x x \in \emptyset$	(*Axioma van de lege verzameling*);
ZF4	$\forall_v \forall_w \exists_y \forall_z (z \in y \leftrightarrow (z = v) \vee (z = w))$	(*Paringsaxioma*);
ZF5	$\forall_x \exists_y \forall_z (z \in y \leftrightarrow \exists_{w \in x} z \in w)$	(*Verenigingsaxioma*);
ZF6	$\forall_x \exists_y \forall_z (z \in y \leftrightarrow z \subset x)$	(*Machtsverzamelingsaxioma*);
ZF7	$\exists_y (\emptyset \in y \wedge \forall_z (z \in y \rightarrow z^+ \in y))$	(*Oneindigheidsaxioma*).

ZF3 is grammaticaal het eenvoudigste axioma: omdat x een variabele is en $\emptyset$ een naam, is het deel $x \in \emptyset$ volgens regel 1 een formule, waarin x vrij is, daaruit geeft regel 2 (b) een nieuwe formule $\exists_x x \in \emptyset$, waarin x gebonden is, en ten slotte maakt $\neg$ daar volgens regel 2 (a) weer een formule van (waarin x nog steeds gebonden is). De enige variabele, x, is gebonden door $\exists_x$ en daarmee is **ZF3** een uitspraak (alle axioma's van alle wiskundige theorieën zijn *uitspraken* in de logische taal waarin ze zijn geformuleerd). **ZF1** is hopelijk duidelijk. **ZF2** hangt samen met regel 2 als we (2.1) met andere variabelen schrijven als $y = \{z \in x \mid F(z)\}$, zodat **ZF2** zegt dat deze verzameling bestaat. Hiermee is ook de notatie $\{z \in x \mid F(z)\}$, gedefinieerd: het is de verzameling y die in **ZF2** wordt beschreven (en die volgens **ZF1** uniek is).[14] Analoog definieert **ZF4** de notatie $\{v, w\}$: dit is de verzameling y die volgens dat axioma bestaat. **ZF5** definieert dan de notatie $y = \cup x$, **ZF6** zegt dat $y = P(x)$ bestaat, en ten slotte definieert **ZF7** $y = \mathbb{N}$.[15]

11. $\dfrac{F(x)}{\forall_x F(x)}$ (∀-Introductie): 12. $\dfrac{\forall_x F(x)}{F(t)}$ (∀-*Eliminatie*);

13. $\dfrac{F(t)}{\exists_x F(x)}$ (∃-*Introductie*); 14. $\dfrac{F(x) \rightarrow G \qquad \exists_x F(x)}{G}$ (∃-*Eliminatie*).

15. $\dfrac{\cdots}{x = x}$ $\dfrac{x = y \qquad y = z}{x = z}$ $\dfrac{x = y}{y = x}$

16. $\dfrac{F(x) \qquad x = y}{F(y)}$ 17. $\dfrac{x = y}{t(x) = t(y)}$

13. Naar Zermelo, die ze voor het eerst informeel opschreef, en Abraham Fraenkel (1891–1965). De laatste twee axioma's van ZF luiden: [ZF8] $\forall_u((\forall_{x \in u} \exists!_z F(x,z)) \rightarrow \exists_y \forall_z (z \in y \leftrightarrow \exists_{x \in u} F(x,z)))$, het *Substitutieaxioma*, en ten slotte [ZF9] $\forall_{v \neq \emptyset} \exists_{x \in v} \forall_y (y \in x \rightarrow y \notin v)$, genaamd het *Regulariteitsaxioma*. Hieruit volgt (moeilijke opgave!) dat $x \notin x$, hetgeen de paradox van Russell definitief oplost (hoe?).
14. In axioma **ZF2** mag de variabele x niet in F voorkomen, ga na waarom!
15. In **ZF7** is z^+ gedefinieerd door (2.16), onderzoek daar ook de grammaticale structuur van!

Ook de eerste-orde logica kent bewijsregels. Naast de bewijsregels voor propositielogica (die nu gelden voor *formules* $A, B, C, \ldots$) komen regels 11 t/m 17 boven erbij. Hierin is $F(x)$ een formule met *tenminste* vrije variabele x (meer variabelen mogen ook). In regels 12 en 13 is t een willekeurige *term*, die de vrije variabele x in $F(x)$ vervangt. Aan deze regels zijn voorwaarden verbonden om rare situaties uit te sluiten:

1. In regel 11 en 14 mogen eerder in het bewijs geen aannamen op x zijn gedaan;
2. In regel 12 en 13 mogen vrije variabelen in t niet gebonden raken in $F(t)$;
3. In regel 14 mag x niet vrij voorkomen in G (dit sluit bijvoorbeeld $G := F(x)$ uit).

- Regel 11 zegt dat als je een formule $F(x)$ voor *willekeurige* "vaste" x bewijst, deze dan voor *alle* x geldt, *zolang er in de afleiding geen aannamen op de variabele* x *zijn gedaan*. Er is in bewijzen dus nauwelijks verschil tussen $F(x)$ en $\forall_x F(x)$ (behalve dat het eerste een formule is en het tweede een uitspraak).
- Voor de term $t := x$ is regel 12 het omgekeerde van regel 11; in de algemene vorm kun je zo van een stelling over *variabele* verzamelingen dezelfde uitspraak over *concrete* verzamelingen afleiden. We zullen dit straks bij (2.80) zien.
- Regel 13 luidt voor de term $t := x$: als $F(x)$ voor *willekeurige* x geldt, dan *bestaat* er ook een x waarvoor $F(x)$ geldt. Deze regel is verre van triviaal! Nuttige speciale gevallen van regels 12 en 13 zijn in iedere wiskundige theorie:

$$\boxed{\frac{\forall_x F(x)}{F(x)}} \qquad\qquad \boxed{\frac{F(x)}{\exists_x F(x)}} \tag{2.77}$$

- Regel 14 is een *Modus Ponens* voor formules met variabelen: als rechts boven de streep $F(x)$ stond in plaats van $\exists_x F(x)$ was het letterlijk de MP geweest.
- Regels 15 t/m 17 liggen zo voor de hand dat je ze zonder nadenken correct gebruikt; ze zeggen in feite dat het symbool = ook het gebruikelijke = teken is.[16]

Je kunt een gebonden variabele een andere naam geven (die niet al voorkomt):

$$\boxed{\frac{\forall_x F(x)}{\forall_y F(y)}} \qquad\qquad \boxed{\frac{\exists_x F(x)}{\exists_y F(y)}} \tag{2.78}$$

Het maakt in bijvoorbeeld regel 11 niet uit of je onder streep $\forall_x F(x)$ of $\forall_y F(y)$ schrijft, en evenzo boven de streep in regel 12. We herhalen dat dezelfde variabele liefst niet zowel vrij als gebonden in een formule voorkomt. Dit herlabelen gebeurt dan ook vaak om dat te voorkomen. ***Bij herhaalde*** $\forall$ ***of*** $\exists$ ***maakt de volgorde niet uit***: er geldt dus

$$\boxed{\frac{\forall_x \forall_y F(x,y)}{\forall_y \forall_x F(x,y)}} \qquad\qquad \boxed{\frac{\exists_x \exists_y F(x,y)}{\exists_y \exists_x F(x,y)}} \tag{2.79}$$

16. Het beperkte aantal mogelijke termen in verzamelingenleer maakt regel 17 daar overbodig.

In principe zijn de regels voor $\forall$ afdoende, als we $\exists$ elimineren via $\exists_x := \neg\forall_x\neg$, maar voor de volledigheid geven we boven ook de regels voor $\exists$ (die volgen uit die voor $\forall$).

Aangezien *formeel* bewijzen in eerste-orde logica iets voor specialisten is, zullen we deze regels redelijk informeel gebruiken (*het formele bewijzen is in dit vak dus beperkt tot de propositielogica*). Het is voldoende als je in informeel opgeschreven bewijzen beseft dat je deze regels voortdurend gebruikt en weet dat een compleet stelsel bewijsregels voor de wiskunde überhaupt bestaat (wat pas sinds ~ 1920 het geval is!).

Laten we bijvoorbeeld nog eens kijken naar de eigenschap

$$X \cap Y = Y \cap X, \tag{2.80}$$

waarin we de hoofdletters X en Y voor zowel namen van concrete verzamelingen als variabelen kunnen staan. Merk eerst op dat (2.80) voor concrete verzamelingen X en Y volgt uit (2.57), waarin de kleine letters x en y variabelen aangeven (zoals altijd in deze syllabus). Het idee van het bewijs van (2.57), waar (2.80) dus uit volgt, is al gegeven onder (2.25). Het kan nu, met handige variabelen, veel preciezer worden opgeschreven:

1. In de stelling $A \wedge B \leftrightarrow B \wedge A$, zie (2.29), kies je $A := z \in v$ en $B := z \in w$, d.w.z.

   $$(z \in v \wedge z \in w) \leftrightarrow (z \in w \wedge z \in v). \tag{2.81}$$

2. Volgens (2.62) staat er $(z \in v \cap w) \leftrightarrow (z \in w \cap v)$, en $\forall_z$ ervoor (regel 11) geeft

   $$\forall_z((z \in v \cap w) \leftrightarrow (z \in w \cap v)). \tag{2.82}$$

3. Hieruit willen we met **ZF1** afleiden dat $v \cap w = w \cap v$. In dit axioma staat echter $x = y$ en niet $v \cap w = w \cap v$. We passen daarom regel 12 eerst toe op **ZF1** met

   $$F(x) := \forall_y\,((\forall_z(z \in x \leftrightarrow z \in y)) \leftrightarrow x = y); \qquad t := v \cap w, \tag{2.83}$$

   zodat er komt $\forall_y\,((\forall_z(z \in v \cap w \leftrightarrow z \in y)) \leftrightarrow (v \cap w) = y)$. Nu passen we nog een keer regel 12 toe, met net als boven $\forall_y F(y)$ boven de streep, deze keer met

   $$F(y) := (\forall_z(z \in v \cap w \leftrightarrow z \in y)) \leftrightarrow v \cap w = y; \qquad t := w \cap v, \tag{2.84}$$

   zodat volgt $\forall_z(z \in v \cap w \leftrightarrow z \in w \cap v) \leftrightarrow v \cap w = w \cap v$. Hiervan hebben we alleen de implicatie $\rightarrow$ van de tweede dubbele implicatie $\leftrightarrow$ nodig,[17] oftewel:

   $$\forall_z(z \in v \cap w \leftrightarrow z \in w \cap v) \rightarrow v \cap w = w \cap v; \tag{2.85}$$

4. *Modus Ponens* (= bewijsregel 3) op (2.85) en (2.82), en vervolgens regel 11 geeft

   $$v \cap w = w \cap v; \qquad \forall_v\forall_w(v \cap w = w \cap v). \tag{2.86}$$

5. Regel 12 met $x \rightsquigarrow v$ en $F(v) := \forall_w(v \cap w = w \cap v)$ en $t := X$ geeft $\forall_w(X \cap w = w \cap X)$. Nu passen we opnieuw regel 12 toe, met $x \rightsquigarrow w$ en $F(w) := (X \cap w = w \cap X)$, en $t = Y$. Dan volgt (2.80), voor willekeurige "concrete" verzamelingen X en Y.

17. Een axioma of stelling van de vorm $A \leftrightarrow B$ impliceert de zwakkere uitspraak $A \rightarrow B$.

Als opgave kun je nu de bewijzen van (2.46) en (2.51) op deze manier preciseren; de te bewijzen uitspraken zijn dan, in de taal van eerste-orde logica,

$$\forall_x \forall_y \forall_z ((x \cup y) \cap z = (x \cap z) \cup (y \cap z)); \tag{2.87}$$

$$\forall_x \forall_y \forall_z ((x \subset z \wedge y \subset z) \to (z \setminus (x \cap y) = (z \setminus x) \cup (z \setminus y))). \tag{2.88}$$

Je hoeft daarbij het gebruik van axioma **ZF1** niet zo uitvoerig te behandelen als boven; het voldoet om te zeggen dat wegens dit axioma bijvoorbeeld (2.87) volgt uit

$$w \in (x \cup y) \cap z \leftrightarrow w \in ((x \cap z) \cup (y \cap z)). \tag{2.89}$$

Met de volgorde van kwantoren moet je erg oppassen: er geldt weliswaar (2.79), maar je kunt de volgorde $\forall_x \exists_y$ niet zomaar verwisselen, omdat de gezochte y mogelijk van x afhangt, terwijl dat in $\exists_y \forall_x$ juist niet mag. Dus **zeker niet** $\forall_x \exists_y F(x, y) \leftrightarrow \exists_y \forall_x F(x, y)$!

Tussen $\forall$, $\exists$, en de symbolen $\wedge$, $\vee$, en $\to$ gelden de volgende (afgeleide) bewijsregels, die we voor nu en je hele toekomst geven (bewaar deze syllabus dus goed!):

$$\frac{\forall_x (F(x) \to G(x))}{(\forall_x F(x)) \to (\forall_y G(y))} \qquad \frac{\forall_x (F(x) \leftrightarrow G(x))}{(\forall_x F(x)) \leftrightarrow (\forall_y G(y))} \tag{2.90}$$

$$\frac{(\exists_x F(x)) \to (\forall_y G(y))}{\forall_x (F(x) \to G(x))} \qquad \frac{\forall_x (F(x) \to G(x))}{(\exists_x F(x)) \to (\exists_y G(y))} \tag{2.91}$$

$$\frac{(\forall_x F(x)) \vee (\forall_y G(y))}{\forall_x (F(x) \vee G(x))} \qquad \frac{\exists_x (F(x) \vee G(x))}{(\exists_x F(x)) \vee (\exists_y G(y))} \tag{2.92}$$

$$\frac{\forall_z (F(z) \wedge G(z))}{(\forall_x F(x)) \wedge (\forall_y G(y))} \qquad \frac{(\forall_x F(x)) \wedge (\forall_y G(y))}{\forall_z (F(z) \wedge G(z))} \tag{2.93}$$

Als voorbeeld bewijzen we de linkerhelft van (2.44), die in eerste-orde logica luidt:[18]

$$\forall_x \forall_y \forall_z ((x \subset (y \cap z)) \leftrightarrow (x \subset y) \wedge (x \subset z)). \tag{2.94}$$

Als we de $\forall_x \forall_y \forall_z$ kwantoren zoals gebruikelijk weglaten is (2.94) hetzelfde als

$$(\forall_u (u \in x \to (u \in y \wedge u \in z))) \leftrightarrow (\forall_v (v \in x \to v \in y) \wedge \forall_w (w \in x \to w \in z)). \tag{2.95}$$

Het doel is nu om dit te bewijzen uit de stelling/tautologie rechts in (2.44), nl.

$$(A \to (B \wedge C)) \leftrightarrow ((A \to B) \wedge (A \to C)), \tag{2.96}$$

uit de propositielogica, waarin de uitspraken A, B en C bijna worden gegeven door (2.47), maar nu met andere namen voor de variabelen, die je uit (2.95) kunt aflezen als

$$A := u \in x; \qquad B := u \in y \qquad C := u \in z. \tag{2.97}$$

18. Het is nu nog niet de bedoeling dat je zo'n bewijs zelf kunt *bedenken*, wel dat je het kunt *volgen*.

Met die keuze luidt (2.96) dus

$$(u \in x \to (u \in y \wedge u \in z)) \leftrightarrow ((u \in x \to u \in y) \wedge (u \in x \to u \in z)). \tag{2.98}$$

Volgens regel 11 mogen we hier $\forall_u$ voorzetten. Volgens de regel rechts in (2.90) volgt

$$(\forall_u(u \in x \to (u \in y \wedge u \in z))) \leftrightarrow (\forall_s((s \in x \to s \in y) \wedge (s \in x \to s \in z))), \tag{2.99}$$

waarbij we de namen van gebonden variabelen steeds veranderen om doublures te voorkomen. Volgens (1.47) kunnen we de bewijsregels (2.93) ook schrijven als

$$\forall_s(F(s) \wedge G(s)) \leftrightarrow \forall_v F(v) \wedge \forall_w G(w), \tag{2.100}$$

met $F(v) := (v \in x \to v \in y)$ en $G(w) := (w \in x \to w \in z)$. Dit geeft dus

$$(\forall_s((s \in x \to s \in y) \wedge (s \in x \to s \in z))) \leftrightarrow (\forall_v(v \in x \to v \in y) \wedge \forall_w(w \in x \to w \in z)). \tag{2.101}$$

We schrijven nu (2.95) als $D \leftrightarrow E$ en de bewezen uitspraken (2.99) en (2.101) als resp. $D \leftrightarrow F$ en $F \leftrightarrow E$ (schrijf D, E, F zelf uit!). Volgens de afgeleide bewijsregel H uit de propositielogica (transitiviteit van $\leftrightarrow$) impliceren $D \leftrightarrow F$ en $F \leftrightarrow E$ samen $D \leftrightarrow E$. Dit is dus (2.95), waaruit met drie keer regel 11 uiteindelijk (2.94) volgt. Q.E.D.

Net als voor (2.80) volgt uit (2.94) dat voor alle *concrete* verzamelingen X, Y, Z geldt

$$X \subset (Y \cap Z) \leftrightarrow (X \subset Y) \wedge (X \subset Z). \tag{2.102}$$

Dit volgt uit (2.94) door herhaaldelijk toepassen van bewijsregel 12 (opgave). Als toepassing van (2.94) bewijzen we tevens dat voor alle concrete verzamelingen Y, Z geldt

$$P(Y \cap Z) = P(Y) \cap P(Z). \tag{2.103}$$

Eerst informeel: Volgens regel 1 van de verzamelingenleer staat hier $X \in P(Y \cap Z)$ desda $X \in P(Y) \cap P(Z)$. Volgens de definitie van de machtsverzameling (regel 6 van de verzamelingenleer) is dit hetzelfde als $X \subset Y \cap Z$ desda $X \subset Y$ en $X \subset Z$, hetgeen hetzelfde is als (2.102). Nu iets formeler: de uitspraak, waar (2.103) uit volgt is

$$\forall_y \forall_z(P(y \cap z) = P(y) \cap P(z)). \tag{2.104}$$

Volgens bewijsregel 11 volgt dit uit $P(y \cap z) = P(y) \cap P(z)$. Volgens axioma **ZF1** en opnieuw regel 11 volgt dit uit $x \in P(y \cap z) \leftrightarrow x \in P(y) \cap P(z)$. De y in axioma **ZF6** is precies $P(x)$, zodat, met andere namen van de variabelen, het voorgaande equivalent is met $x \subset (y \cap z)) \leftrightarrow (x \subset y) \wedge (x \subset z)$, wat via regel 11 feitelijk hetzelfde is als (2.94).

Je ziet dat er eigenlijk niet zo'n groot verschil is tussen het informeel en formeel opschrijven van een bewijs, als de stappen maar correct zijn en steeds naar de gebruikte axioms's en bewijsregels wordt verwezen. Het informele bewijs bevat altijd het idee van het formele bewijs en als je dat idee correct opschrijft haal je al een voldoende!

2.4 Opgaven bij hoofdstuk 2

Zie ook de exercises in Velleman, §1.4, 2.2, 2.3, 3.4, 3.5.

Opgave 2.1

Schrijf voor $X = \{1, 2, 3, 4\}$ en $Y = \{4, 5\}$ de verzamelingen op: $X \cup Y$, $X \cap Y$, $X \setminus Y$, $X \Delta Y$, $P(X)$, en X^+.

Opgave 2.2

Maak met behulp van Venn-diagrammen zo veel mogelijk van de eigenschappen in de linkerkolom van (2.29) t/m (2.45) plausibel (zie Velleman §1.4).

Opgave 2.3

Bewijs in de stijl van het bewijs onder (2.25) dat $X \cup Y = Y \cup X$, zie (2.30).

Opgave 2.4

Bewijs in de stijl van het bewijs van (2.38) onder (2.46) de eigenschap (2.39).

Opgave 2.5

Bewijs in de stijl van het bewijs van (2.31) onder (2.51) de eigenschap (2.32).

Opgave 2.6

Bewijs in de stijl van het bewijs van (2.55) dat $\cap P(X) = \emptyset$, zie (2.56).

Opgave 2.7

Bewijs in dezelfde informele stijl dat $X = Y$ desda $X \subset Y$ en $Y \subset X$.

Opgave 2.8

Bewijs in dezelfde informele stijl dat $(X \cap Y) \subset X \subset (X \cup Y)$.

Opgave 2.9

Bewijs in dezelfde stijl dat $(X \cup Y) \subset Z$ desda $X \subset Z$ en $Y \subset Z$, zie (2.45).

Opgave 2.10

Schrijf, zoals voor axioma **ZF3** in de tekst, voor ieder van de andere axioma's **ZF1** t/m **ZF7** uit hoe en waarom het een grammaticaal correcte uitspraak is.

Opgave 2.11

Geef precieze versies van de informele bewijzen van (2.46) en (2.51) in §2.1, nu dus op de manier van §2.3, zoals voorgedaan onder (2.80) en onder (2.94).

Opgave 2.12

Maak ook je bewijzen uit de opgaven 2.3 t/m 2.9 nu precies in de stijl van §2.3.

3

Cartesisch product en relaties

Met verzamelingenleer achter de kiezen kunnen we nu het raadselachtige feit ophelderen dat de halve wiskunde op het begrip functie berust, terwijl dat in de taal van de verzamelingenleer niet voorkomt! Hiertoe moeten we eerst het zogenaamde *cartesisch product* van twee (of meer) verzamelingen invoeren.[1] Dit is een van de meest gebruikte constructies in de hele wiskunde! Het doel is *geordende* paren te krijgen, dus paren $\langle x, y\rangle$ (vaak genoteerd als (x, y), maar we hebben al genoeg haakjes), *waarin de volgorde uitmaakt*. We zagen al dat in $\{x, y\}$ de volgorde juist *niet* uitmaakt, aangezien $\{x, y\} = \{y, x\}$. We lossen dit op met een trucje (dat je direct weer mag vergeten):[2]

$$\langle x, y\rangle := \{\{x\}, \{x, y\}\}. \tag{3.1}$$

Definitie 3.1 *Het* **cartesisch product** *van de verzamelingen* X *en* Y *is de verzameling*

$$X \times Y = \{\langle x, y\rangle \mid x \in X, y \in Y\}. \tag{3.2}$$

Hier is $x \in X, y \in Y$ hetzelfde als $(x \in X) \wedge (y \in Y)$; deze komma-notatie komt vaak voor in lijsten van voorwaarden. We gebruiken regel 2 (d.w.z. axioma **ZF2**) om te rechtvaardigen dat het cartesisch product van twee verzamelingen ook echt bestaat: de verzameling Z in (2.1) is dan $\mathcal{P}(\mathcal{P}(X \cup Y))$, zie opgave.[3] Uit Velleman, Theorem 4.1.3:

Stelling 3.2 *Voor alle verzamelingen* X, Y, Z, W *geldt:*

$$X \times (Y \cap Z) = (X \times Y) \cap (X \times Z); \tag{3.3}$$
$$X \times (Y \cup Z) = (X \times Y) \cup (X \times Z); \tag{3.4}$$
$$(X \times Y) \cap (Z \times W) = (X \cap Z) \times (Y \cap W); \tag{3.5}$$
$$(X \times Y) \cup (Z \times W) \subset (X \cup Z) \times (Y \cup W); \tag{3.6}$$
$$X \times \emptyset = \emptyset \times X = \emptyset. \tag{3.7}$$

Let op dat in (3.6) *geen gelijkheid maar een inclusie staat!* Zie Velleman voor het bewijs, met als zeer nuttige opgave om dit voor jezelf uit te schrijven zoals in hoofdstuk 2.

1. Het cartesisch product werd oorspronkelijk door René Descartes (1596–1650) ingevoerd om het platte vlak te beschrijven (waarin $X = Y = \mathbb{R}$, de reële getallen, die we nog moeten invoeren).
2. Deze definitie is van Kuratowski uit 1921. In 1914 stelde Wiener nog voor $\langle x, y\rangle := \{\{x\}, \{y, \emptyset\}\}$.
3. Je kunt deze constructie ook herhalen: aangezien $X \times Y$ een verzameling is, kun je ook $(X \times Y) \times Z$ maken, enzovoort. Het is helaas echter niet zo dat $(X \times Y) \times Z = X \times (Y \times Z)$. Er is wel een *bijectie* tussen deze twee verzamelingen, zie volgend hoofdstuk en met name opgave 4.1. Deze complicatie is echter irrelevant omdat we later langere cartesische producten als functies zullen definiëren.

3.1 Relaties

In de moderne wiskunde is het cartesisch product vooral bedoeld om *relaties* te definiëren, waar *functies* weer een speciaal geval van zijn (zie volgend hoofdstuk).

Definitie 3.3 *Een* **relatie** R *tussen twee verzamelingen* X *en* Y *is een deelverzameling* $R \subset X \times Y$ *van* $X \times Y$. *Een relatie op* X *is een deelverzameling* $R \subset X \times X$ *(d.w.z.* $Y = X$*).*

Laten we met het speciale geval $R \subset X \times X$ beginnen. Een flauw voorbeeld is $R = \mathrm{id}_X$, waarbij $\langle x, y\rangle \in R$ desda $x = y$, d.w.z.

$$\mathrm{id}_X = \{\langle x, x\rangle \mid x \in X\}. \tag{3.8}$$

Deze relatie heet de ***diagonaal*** of ***identiteit*** op X en wordt ook wel Δ_X of $\mathfrak{i}_X$ genoemd. Stel nu $X = \mathbb{N} = \{0, 1, 2, \ldots\}$, de natuurlijke getallen. We definiëren een relatie op $\mathbb{N}$, oftewel een deelverzameling $R \subset \mathbb{N} \times \mathbb{N}$ door: $\langle m, n\rangle \in R$ desda $m \leqslant n$, d.w.z., m is kleiner dan of gelijk aan n. Vaak noteert men xRy in plaats van $\langle x, y\rangle \in R$. In het voorbeeld van zojuist zou je dus $\leqslant$ zelf de relatie R kunnen noemen, en dan betekent $m \leqslant n$ hetzelfde als $\langle m, n\rangle \in \leqslant$. Die laatste notatie wordt echter zelden gebruikt.

- Het ***domein*** van een relatie R tussen X en Y is de deelverzameling

$$\mathrm{dom}(R) = \{x \in X \mid \exists_{y \in Y} \langle x, y\rangle \in R\} \subset X, \tag{3.9}$$

  bestaande uit alle $x \in X$ waarvoor een $y \in Y$ bestaat die in relatie R staat tot x.
- Het ***bereik (range)*** van een relatie R tussen X en Y is de deelverzameling

$$\mathrm{ran}(R) = \{y \in Y \mid \exists_{x \in X} \langle x, y\rangle \in R\} \subset Y, \tag{3.10}$$

  oftewel: alle $y \in Y$ waarvoor een $x \in X$ bestaat die in relatie R staat tot y.

Als oefening kun je bijvoorbeeld eenvoudig nagaan dat $\mathrm{dom}(\mathrm{id}_X) = \mathrm{ran}(\mathrm{id}_X) = X$.

Je kunt relaties *inverteren* en je kunt twee relaties *samenstellen*:

- De ***inverse*** van een relatie R tussen X en Y is deze relatie R^{-1} tussen Y en X:

$$R^{-1} = \{\langle y, x\rangle \in Y \times X \mid \langle x, y\rangle \in R\}. \tag{3.11}$$

  Hier is opnieuw een simpel voorbeeld $(\mathrm{id}_X)^{-1} = (\mathrm{id}_X)$.
- Als R een relatie tussen X en Y is en S een relatie tussen Y en Z, dan is de ***samenstelling*** $S \circ R$ (uitgesproken "S na R") de volgende relatie tussen X en Z:

$$S \circ R = \{\langle x, z\rangle \in X \times Z \mid \exists_{y \in Y}(\langle x, y\rangle \in R) \wedge (\langle y, z\rangle \in S)\}. \tag{3.12}$$

Bewijs als oefening nu zelf de volgende eigenschappen (Velleman, Theorem 4.2.5):

$$(R^{-1})^{-1} = R; \tag{3.13}$$
$$\mathrm{dom}(R^{-1}) = \mathrm{ran}(R); \tag{3.14}$$
$$\mathrm{ran}(R^{-1}) = \mathrm{dom}(R); \tag{3.15}$$
$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}. \tag{3.16}$$

Bovendien is de samenstelling van relaties ***associatief***, d.w.z., als er nog een derde relatie T tussen Z en W is, geldt een eigenschap die je overal in de wiskunde tegenkomt:

$$T \circ (S \circ R) = (T \circ S) \circ R. \tag{3.17}$$

Zie Velleman, §4.2 voor vele voorbeelden en opgaven. Het begrip 'relatie' is zeer algemeen en wordt pas interessant als de relatie speciale eigenschappen heeft. Als X bestaat uit alle volwassenen in de wereld en $\langle x, y\rangle \in R$ desda x verliefd is op y, dan hoeft niet te gelden dat tevens $\langle y, x\rangle \in R$. Maar als $\langle x, y\rangle \in R$ desda x getrouwd is met y, dan geldt ook $\langle y, x\rangle \in R$. In dat geval heet R *symmetrisch*. Hier zijn nog meer eigenschappen:[4]

Definitie 3.4 *Een relatie $R \subset X \times X$ op een verzameling X heet:*

- **reflexief** *als* xRx *voor alle* $x \in X$*;*
- **transitief** *als voor alle* $x, y, z \in X$ *geldt:* xRy *en* $yRz \Rightarrow xRz$*;*
- **symmetrisch** *als voor alle* $x, y \in X$ *geldt:* $xRy \Rightarrow yRx$*.*
- **antisymmetrisch** *als voor alle* $x, y \in X$ *geldt:* xRy *en* $yRx \Rightarrow x = y$*.*
- *een* **preordening** *als* R *reflexief en transitief is.*
- *een* **equivalentierelatie** *als* R *reflexief, transitief, en symmetrisch is.*
- *een* **partiële ordening** *als* R *reflexief, transitief, en antisymmetrisch is.*

Een nuttige test voor de eerste drie basiseigenschappen is Theorem 4.3.4. in Velleman:

Stelling 3.5 *Stel dat R een relatie op X is. Dan is R:*

- *reflexief desda* $\mathrm{id}_X \subset R$*;*
- *transitief desda* $R \circ R \subset R$*.*
- *symmetrisch desda* $R^{-1} = R$*.*

Velleman (Chapter 4) staat bol van de voorbeelden! We behandelen nu twee belangrijke gevallen: partiële ordeningen en equivalentierelaties. Zie ook hoofdstuk 4.

3.2 Partiële ordeningen

Een partiële ordening wordt meestal genoteerd als $\leqslant$. Een verzameling met een partiële ordening heet een ***poset*** (*partially ordered set*). Een poset P heet ***totaal*** geordend als voor iedere $x, y \in P$ geldt: $x \leqslant y$ of $y \leqslant x$. De gebruikelijke relatie $\leqslant$ op $\mathbb{N}$ is een partiële ordening: ga na. Dit voorbeeld is uit te breiden tot $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$, zodra we deze verzamelingen hebben gedefinieerd. Deze ordeningen zijn allemaal totaal. Een heel ander voorbeeld levert de machtsverzameling $X = P(Z)$ van een verzameling Z. Definieer een relatie $\leqslant$ op $P(Z)$ door $\boxed{x \leqslant y \text{ desda } x \subset y}$ (waarin dus $x \subset Z$ en $y \subset Z$). Dit is een partiële ordening (ga na), die *niet* totaal is (tenzij Z leeg is of één element heeft). Merk op dat $\emptyset \leqslant x$ en $x \leqslant Z$ (kort: $\emptyset \leqslant x \leqslant Z$) voor alle $x \in P(Z)$.

4. We zullen geen voorbeelden tegenkomen van een preordening die niet ofwel een partiële ordening ofwel een equivalentierelatie is, dus die definitie staat er alleen voor de volledigheid.

Het volgende begrip is van groot belang in de hele wiskunde, maar vooral in Analyse en Logica. Al in dit college speelt het straks een sleutelrol bij de reële getallen.

Definitie 3.6 *Stel X is een verzameling met een partiële ordening $\leqslant$, en $S \subset X$.*

1. *$y \in X$ heet een* **bovengrens** *van S als $x \leqslant y$ voor alle $x \in S$.*
2. *$z \in X$ heet een* **kleinste bovengrens** *(Engels: lowest upper bound, l.u.b.) of* **supremum** *van S, notatie $z = \bigvee S$ of $z = \sup S$, als z een bovengrens van S is en bovendien voor iedere (andere) bovengrens y van S geldt: $z \leqslant y$.*
3. *Analoog heet $y \in X$ heet een* **ondergrens** *van S als $y \leqslant x$ voor alle $x \in S$.*
4. *$z \in X$ heet een* **grootste ondergrens** *(Engels: greatest lower bound, g.l.b.) of* **infimum** *van S, notatie $z = \bigwedge S$ of $z = \inf S$, als z een ondergrens van S is en bovendien voor iedere (andere) ondergrens y van S geldt: $y \leqslant z$.*

Als een kleinste bovengrens of een grootste ondergrens bestaat, is deze uniek (opgave). In het algemeen hoeven bovengrenzen en kleinste bovengrenzen (of ondergrenzen) van S niet te bestaan, en als ze wel bestaan kunnen ze wel of niet in de verzameling S zelf liggen. Later zullen we bijvoorbeeld zien dat de opmerkelijke deelverzameling

$$S = \{q \in \mathbb{Q} \mid (q < 0) \vee (q^2 < 2)\} \tag{3.18}$$

van $X = \mathbb{Q}$ geen kleinste bovengrens heeft, maar dat wel heeft als deelverzameling van $X = \mathbb{R}$, namelijk $\sqrt{2}$, en die ligt niet in S. Met $q^2 \leqslant 2$ zou dat in $\mathbb{R}$ wel zo zijn, in $\mathbb{Q}$ niet.

We kijken weer naar de poset $P(Z)$ onderaan de vorige pagina. Uit de zojuist genoemde eigenschap $\emptyset \leqslant x \leqslant Z$ voor alle $x \in P(Z)$ volgt dat iedere niet-lege deelverzameling $S \subset P(Z)$ een bovengrens heeft, namelijk Z (ga na). Sterker nog:

Stelling 3.7 *Stel $Z \neq \emptyset$. Bekijk de poset $P(Z)$ met partiële ordening $\leqslant$ gegeven door inclusie $\subset$. Iedere niet-lege deelverzameling $S \subset P(Z)$ heeft een kleinste bovengrens*

$$\sup S = \cup S. \tag{3.19}$$

Toelichting: per definitie is $\cup S \in P(Z)$ en dus $\cup S \subset Z$, en $\cup S$ bevat simpelweg alle elementen van alle deelverzamelingen $x \subset Z$ die in S zitten (d.w.z. $x \in S \subset Z$). Steeds moet je beseffen dat S *een verzameling van deelverzamelingen van Z is!*

Bewijs: We gaan eerst na dat $\cup S$ überhaupt een bovengrens van S is. Als $x \in S$, met $x \subset Z$, moet dus gelden $x \leqslant \cup S$, oftewel $x \subset \cup S$. Dat klopt, zie toelichting boven. Nu moet $\cup S$ ook de *kleinste* bovengrens van S zijn, dus: als $x \leqslant z$ voor alle $x \in S$ moet $\cup S \leqslant z$, hetgeen in onze situatie betekent: als voor alle $x \in S$ geldt $x \subset z$, dan moet gelden $\cup S \subset z$. Vouw dit laatste volgens de definitie van $\subset$ uit als $w \in \cup S \to w \in z$, en besef dat $w \in \cup S$ per definitie van $\cup$ betekent dat er een $x \in S$ is met $w \in x$. Dus: als $w \in x \in S$ voor zekere $x \in S$, dan moet $w \in z$. Maar op $x \in S$ gold de aanname $x \subset z$, zie box, zodat geldt $w \in x \subset z$, en daarmee $w \in z$. Wat een gepriegel! Q.E.D.

3.3 Equivalentierelaties

We geven nu voorbeelden van *equivalentierelaties*, meestal genoteerd als $\sim$.

1. Voor alle X is de relatie id_X een equivalentierelatie (met $x \sim y$ desda $x = y$).
2. Een leuke equivalentierelatie op $\mathbb{N}$ is: $m \sim n$ desda $m + n$ even is (ga na).

Bij iedere equivalentierelatie $\sim$ op een verzameling X hoort een verzameling $X/\sim$, genaamd het ***quotiënt*** van X naar $\sim$. Formeel is $X/\sim$ een deelverzameling van de machtsverzameling $P(X)$; *elementen* $[x]$ van $X/\sim$ zijn dus *deelverzamelingen* van X, met

$$X/\sim := \{[x] \in P(X) \mid x \in X\}; \qquad [x] := \{z \in X \mid z \sim x\}. \tag{3.20}$$

De deelverzameling $[x] \subset X$ heet de ***equivalentieklasse*** (of ***baan***) van x in X (ten opzichten van de equivalentierelatie $\sim$). Ga de volgende cruciale eigenschap na:

$$[x_1] = [x_2] \text{ desda } x_1 \sim x_2, \tag{3.21}$$

en check dat ieder element $x \in X$ in precies één equivalentieklasse zit, namelijk $[x]$.

De verzameling $X/\sim$ is een voorbeeld van een *partitie* van X, in de volgende zin:[5]

Definitie 3.8 *Een* **partitie** *van $X \neq \emptyset$ is een verzameling $\emptyset \notin \pi \subset P(X)$ (de elementen van π zijn dus niet-lege deelverzamelingen van X) met de volgende eigenschappen:*

1. *als $a \in \pi$ en $b \in \pi$ met $a \neq b$ dan is $a \cap b = \emptyset$ (d.w.z. a en b zijn disjunct);*
2. *$X = \cup\pi$, met andere woorden, iedere $x \in X$ zit in een zekere $a \in \pi$ (en deze a is vanwege de eis in het vorige punt uniek).*

Gegeven een equivalentierelatie $\sim$ op X krijgen we een partitie $\boxed{\pi = X/\sim}$; ga na dat de eigenschappen van een equivalentierelatie garanderen dat π inderdaad een partitie is! Omgekeerd geeft een partitie π van X een equivalentierelatie $\sim$ op X: neem namelijk: $\boxed{x \sim y \text{ desda } x \text{ en } y \text{ in hetzelfde element van } \pi \text{ zitten.}}$ Een equivalentierelatie op X is dus min of meer hetzelfde als een partitie van X: de eerste is weliswaar een willekeurige deelverzameling van $X \times X$ en de tweede is een speciaal soort deelverzameling van $P(X)$, maar je kunt het ene begrip op de bovengenoemde manier in het andere vertalen. Als we de bovenstaande twee voorbeelden van equivalentierelaties aflopen zien we:

1. De equivalentieklassen zijn singletons, $[x] = \{x\}$, en de bijbehorende partitie π van X bestaat uit de elementen $\{x\}$ van X. Let op: $\pi \neq X$ (waarom niet?).
2. Er zijn twee equivalentieklassen: de even getallen en de oneven getallen. Die geven dus ook de bijbehorende partitie van de natuurlijke getallen $\mathbb{N}$.

5. Let op: in getaltheorie betekent het begrip 'partitie' vaak iets anders dan hier. Een partitie van een geheel getal $n \in \mathbb{N}$ is een manier om n te schrijven als een som van gehele getallen, bijvoorbeeld: $1 = 1$ (dus 1 heeft 1 partitie), $2 = 2$ en $2 = 1 + 1$ (dus 2 heeft 2 partities), $3 = 3$ of $3 = 2 + 1$ of $3 = 1 + 1 + 1$ (dus 3 heeft 3 partities). Een dergelijke partitie van n is niet hetzelfde als een partitie van n gezien als verzameling. Zo heeft $3 = \{0, 1, 2\}$ gezien als verzameling de volgende partities: $\pi_1 = \{\{0, 1, 2\}\}$, $\pi_2 = \{\{0, 1\}, \{2\}\}$, $\pi_3 = \{\{0, 2\}, \{1\}\}$, $\pi_4 = \{\{1, 2\}, \{0\}\}$, $\pi_5 = \{\{0\}, \{1\}, \{2\}\}$.

3.4 Opgaven bij hoofdstuk 3

Zie ook de exercises in Velleman, §4.1, 4.2, 4.4, 4.6.

Opgave 3.1

Toon aan dat $\langle x, y\rangle \in P(P(X \cup Y))$.

Opgave 3.2

Toon aan dat $X \times Y = \emptyset$ desda $X = \emptyset$ of $Y = \emptyset$.

Opgave 3.3

Stel in (3.12) dat $X = Y = Z = X$. Bewijs dat voor iedere relatie R op X geldt $(\mathrm{id}_X) \circ R = R \circ (\mathrm{id}_X) = R$.

Opgave 3.4

Bewijs zelf de eigenschappen (3.13) t/m (3.17).

Opgave 3.5

Bewijs (3.21).

Opgave 3.6

Hoeveel relaties zijn er op een verzameling met n elementen?

Opgave 3.7

Bewijs dat een kleinste bovengrens uniek is als deze bestaat.

Opgave 3.8

Ga na dat: $m \sim n$ desda $m + n$ even is, een equivalentierelatie op $\mathbb{N}$ is.

Opgave 3.9

Laat zien dat $\pi = X/\sim$ een partitie is (als $\sim$ een equivalentierelatie is), en omgekeerd dat de relatie $\sim$ gedefinieerd door $x \sim y$ desda x en y in hetzelfde element van een partitie π van X zitten, een equivalentierelatie is.

Opgave 3.10

Bewijs zelf Stellingen 3.2 en 3.5.

Opgave 3.11

Definieer $x \sim y$ op $X = \mathbb{R}^2$ desda $\sqrt{x_1^2 + x_2^2} = \sqrt{y_1^2 + y_2^2}$, met $x = \langle x_1, x_2\rangle$ en $y = \langle y_1, y_2\rangle$. Laat zien dat dit een equivalentierelatie op $\mathbb{R}^2$ geeft. Teken de equivalentieklassen! Wat is het quotiënt $\mathbb{R}^2/\sim$?

4

Functies

Je bent gewend een functie te zien als een 'afbeelding' $f : X \to Y$ van X naar Y (met $X = Y = \mathbb{R}$), met het idee: "f stuurt iedere $x \in X$ naar een zekere $y = f(x) \in Y$". Maar wat betekent dat precies? Een voorschrift? Een formule? Een regel? Te vaag. Bovendien willen we ieder wiskundige object als verzameling zien en dat is f zo te zien niet. De oplossing is om niet de functie zelf maar haar *grafiek* als uitgangspunt te nemen. Informeel: als we een functie $f : X \to Y$ hebben, is de ***grafiek*** van f gedefinieerd als

$$G_f = \{\langle x, y\rangle \in X \times Y \mid y = f(x)\} \subset X \times Y. \tag{4.1}$$

Gezien als relatie tussen X en Y heeft deze grafiek duidelijk de eigenschap dat er voor iedere $x \in X$ een unieke $y \in Y$ is zodanig dat $\langle x, y\rangle$ in de grafiek G_f ligt. Formeel:

$$\forall_{x\in X}\exists!_{y\in Y}(\langle x, y\rangle \in G_f), \tag{4.2}$$

waarbij de notatie (2.68) is gebruikt: voor iedere x in X bestaat een unieke y in Y zodat het geordende paar $\langle x, y\rangle$ in de grafiek $G_f \subset X \times Y$ ligt. *Dit is een conditie op* G_f. Dus:

Definitie 4.1 *Een* **functie** $f : X \longrightarrow Y$ *is een relatie* $G_f \subset X \times Y$ *waarvoor* (4.2) *geldt.*

In verzamelingenleer is een functie dus een speciale relatie, net als een partële ordening en een equivalentierelatie, maar nu met als axioma (4.2). De functie "is" haar grafiek:[1] de relatie $G_f \subset X \times Y$ is het uitgangspunt en de notatie $f : X \longrightarrow Y$ is daarvan afgeleid. Bij die notatie is $y = f(x)$ het unieke element $y \in Y$ dat volgens (4.2) voor een gegeven G_f bij x hoort via $\langle x, y\rangle \in G_f$. Vaak gebeurt dat inderdaad volgens een "voorschrift" of "regel". Functies $f : \mathbb{R} \to \mathbb{R}$ in de zin van wiskunde B definiëren via hun grafiek in $\mathbb{R}^2$ ook functies in de nieuwe zin. De eenheidscirkel in $\mathbb{R}^2$ is geen functie: aan geen van de eisen in (4.2) is voldaan. De y-as is ook geen functie, maar de x-as is dat weer wel!

Voor een ander voorbeeld: stel dat X weer de verzameling van alle volwassenen op de wereld is, met ook weer de relatie $R \subset X \times X$ gedefinieerd door: $\langle x, y\rangle \in R$ desda x met y is getrouwd. Is deze relatie een *functie*? Kijk zelf maar: dit is het geval desda

1. ieder persoon in de wereld getrouwd is: dit is de $\forall_{x\in X}$ in (4.2);
2. personen die getrouwd zijn precies één partner hebben: dit is de $\exists!_{y\in Y}$ in (4.2).

1. Daarmee is de historische cirkel rond. In de 17e eeuw dacht Newton niet aan functies maar aan hun grafieken (die hij zag als krommen in de ruimte en interpreteerde als de beweging van een deeltje). Euler begon in de 18e eeuw met de toekenning van een functiewaarde $f(x) \in Y$ aan $x \in X$ (vaak via een formule). Nu beginnen we met de grafiek G_f en zijn we dus weer terug bij Newton!

4.1 Terminologie rond functies

De volgende definities zul je vrijwel dagelijks gebruiken! Zie ook Velleman, Ch. 5.

Definitie 4.2 *Stel* $f : X \to Y$ *is een functie (eigenlijk dus een grafiek* $G_f \subset X \times Y$*).*

- *De notatie* $y = f(x)$ *met* $y \in Y$ *en* $x \in X$ *betekent hetzelfde als* $\langle x, y\rangle \in G_f$.
- *De notatie* $x \mapsto f(x)$ *wordt ook vaak gebruikt als naam van de functie, vooral als* f *(zoals op school) door een concreet voorschrift wordt gegeven (de functie* $f(x) = \sin(x)$ *van* $X = \mathbb{R}$ *naar* $Y = \mathbb{R}$ *wordt dus ook genoteerd als* $x \mapsto \sin(x)$*).*
- *De verzameling* X *heet het* **domein** *van* f*, dus* $X = \mathrm{dom}(f)$*, zie ook* (3.9).
- *De verzameling* Y *heet het* **codomein** *van* f*, dus* $Y = \mathrm{codom}(f)$.
- *Als* $W \subset X$ *staat* $f(W)$ *voor het* **beeld** *van* W *onder* f*, gedefinieerd door*

$$f(W) := \{y \in Y \mid \exists_{x \in W}\, (y = f(x))\}. \tag{4.3}$$

  Dus $f(W) \subset Y$*. Het geval* $W = \{x\}$ *geeft* $f(\{x\}) = \{f(x)\}$*. Officieel is* $\{y\} = \{f(x)\}$ *dus het beeld van* $\{x\}$ *(onder* f*), maar we zeggen dat* $f(x)$ *het beeld van* x *is.*
- *Het* **beeld** *(***range***) van* f *is de verzameling* $\mathrm{ran}(f) = f(X)$*, zie ook* (3.10)*, d.w.z.*

$$\mathrm{ran}(f) := \{y \in Y \mid \exists_{x \in X}\, (y = f(x))\}. \tag{4.4}$$

- *Als* $U \subset Y$ *is het* **volledig origineel** $f^{-1}(U) \subset X$ *van* U *onder* f *gedefinieerd door*

$$f^{-1}(U) := \{x \in X \mid f(x) \in U\}. \tag{4.5}$$

- f *heet* **injectief/een injectie (one-to-one)** *als iedere* $y \in \mathrm{ran}(f)$ *1 origineel heeft:*

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2, \tag{4.6}$$

  of contrapositief: verschillende originelen verschillende beelden hebben, d.w.z.

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2). \tag{4.7}$$

- f *heet* **surjectief/een surjectie (onto)** *als* f *het hele codomein bereikt, d.w.z.*

$$\mathrm{ran}(f) = Y, \tag{4.8}$$

  met andere woorden, als voor iedere $y \in Y$ *een* $x \in X$ *bestaat met* $y = f(x)$*. Codomein en beeld van de functie vallen in dat geval samen.*
- f *heet* **bijectief/een bijectie** *als* f *injectief én surjectief is. Naast* (4.2) *geldt dan*

$$\forall_{y \in Y} \exists!_{x \in X} \langle x, y\rangle \in G_f, \tag{4.9}$$

  d.w.z. bij iedere $y \in Y$ *hoort precies één* $x \in X$ *zodat* $y = f(x)$*.*
- *Voor* $f_1 : X \to Y$ *en* $f_2 : X \to Y$ *schrijven we* $f_1 = f_2$ *desda* $G_{f_1} = G_{f_2}$*, en dit is het geval desda* $f_1(x) = f_2(x)$ *voor alle* $x \in X$ *(zie Velleman, Theorem 5.1.4).*

4.2 Bijecties en inverses

De eenvoudigste bijectie op een willekeurige verzameling X is $\mathrm{id}_X : X \to X$ uit §3.1, met grafiek $G = \{\langle x, y\rangle \in X \times X \mid y = x\}$ en voorschrift $\mathrm{id}_X(x) = x$. Het belangrijkste punt is dit. Iedere relatie heeft een inverse, zie (3.11). Maar een bijectie $f : X \to Y$ heeft een *inverse* $f^{-1} : Y \to X$ *die ook weer een functie is*, en zelfs een bijectie, met inverse $(f^{-1})^{-1} = f$. Als we (3.11) toepassen op de grafiek $R = G_f$ van een functie f, volgt

$$G_f^{-1} = \{\langle y, x\rangle \in Y \times X \mid y = f(x)\} \subset Y \times X. \tag{4.10}$$

Als f een *bijectie* is, dan is vanwege (4.9) de inverse relatie G_f^{-1} de grafiek $G_{f^{-1}}$ van een zekere functie $f^{-1} : Y \to X$ (ga na), genaamd de ***inverse*** van f, zodat

$$G_f^{-1} = G_{f^{-1}}. \tag{4.11}$$

Let op! Voor *iedere* functie $f : X \to Y$ en $U \subset Y$ is $f^{-1}(U)$ gedefineerd door (4.5). Als f een *bijectie* is, kunnen we $f^{-1}(U)$ echter ook zien als het beeld van U under $f^{-1} : Y \to X$, zoals in (4.3) met f^{-1} in plaats van f, d.w.z. $f^{-1}(U) = \{x \in X \mid \exists_{y\in U}(x = f^{-1}(y)\}$. Gelukkig geldt voor bijecties dat $f^{-1}(U)$ volgens (4.5) gelijk is aan $f^{-1}(U)$ volgens (4.3).

Als $f : X \to Y$ en $g : Y \to Z$, of, in een diagram, $X \xrightarrow{f} Y \xrightarrow{g} Z$, dan kunnen we de bijbehorende grafieken G_f en G_g volgens (3.12) samenstellen tot een relatie

$$G_g \circ G_f = \{\langle x, z\rangle \in X \times Z \mid (y = f(x)) \wedge (z = g(y))\} \subset X \times Z. \tag{4.12}$$

Dit is de grafiek van een functie genaamd $g \circ f : X \to Z$, zodat $G_g \circ G_f = G_{g\circ f}$. Merk op dat $G_g \circ G_f$ de grafiek van een functie is omdat de $y \in Y$ in (4.12) wegens (4.2) toegepast op f uniek is en bij die y vanwege (4.2) toegepast op g een unieke z hoort (zie Velleman, Theorem 5.1.5). Als $\langle x, z\rangle \in G_{g\circ f}$, dan schrijven we $z = g(f(x))$ of $z = (g \circ f)(x)$. Dit geldt voor willekeurige functies f en g. Als f een bijectie is, met inverse f^{-1}, dan volgt

$$f^{-1} \circ f = \mathrm{id}_X; \qquad\qquad f \circ f^{-1} = \mathrm{id}_Y. \tag{4.13}$$

Stelling 4.3 *Een functie $f : X \to Y$ is een bijectie desda er een functie $g : Y \to X$ bestaat met $g \circ f = \mathrm{id}_X$ en $f \circ g = \mathrm{id}_Y$. De functie g is uniek en gelijk aan de inverse f^{-1}.*

De eerste claim volgt van links naar rechts uit (4.13) en de opmerking daarboven. Van rechts naar links gebruik je het volgende resultaat (Velleman, Theorem 5.3.3):

Stelling 4.4 *Stel $f : X \to Y$ is een functie.*

1. *Als er een functie $g : Y \to X$ bestaat met $g \circ f = \mathrm{id}_X$, dan is f injectief.*
2. *Als er een functie $h : Y \to X$ bestaat met $f \circ h = \mathrm{id}_Y$, dan is f surjectief.*
3. *Als beide voorwaarden gelden is f een bijectie en geldt $g = h = f^{-1}$.*

Bewijs. Voor no. 1 pas je g toe op $f(x_1) = f(x_2)$ en vindt $x_1 = x_2$, zie (4.6). Voor no. 2 neem je $x = h(y)$ en pas je f toe, zodat $y = f(x)$. Voor no. 3 laat je f^{-1} van rechts los op $g \circ f = \mathrm{id}_X$ en gebruikt dan de linkerkant van (4.13) alsmede $\mathrm{id}_X \circ f^{-1} = f^{-1}$ (ga na); dit geeft $g = f^{-1}$. Vervolgens laat je f van links los op $f \circ h = \mathrm{id}_Y$ en gebruikt de rechterkant van (4.13) alsmede $f \circ \mathrm{id}_Y = f$ (ga ook dit na); dit geeft $h = f^{-1}$. Q.E.D.

4.3 Gelijkmachtigheid

Bijecties geven een antwoord op de vraag wanneer verzamelingen "even groot" zijn.

Definitie 4.5 (Cantor) *Voor twee verzamelingen X en Y schrijven we $X \cong Y$ desda er een bijectie $f : X \to Y$ bestaat, en zeggen in dat geval dat X en Y* gelijkmachtig *zijn.*

We zien $\cong$ als een equivalentierelatie op de 'klasse' van alle verzamelingen.[2] Ga na:

- $\cong$ is *reflexief*: $\mathrm{id}_X : X \to X$, d.w.z. $\mathrm{id}_X(x) = x$, is een bijectie, zodat $X \cong X$.
- $\cong$ is *transitief*: stel $X \cong Y$ en $Y \cong Z$, dan hebben we bijecties $f : X \to Y$ en $h : Y \to Z$. Dan is ook $h \circ f : X \to Z$ een bijectie (ga na), zodat $X \cong Z$.
- $\cong$ is *symmetrisch*: dit volgt uit Stelling 4.3 (waarom?).

Als $X \cong n$ voor zekere $n \in \mathbb{N}$, dan heeft X precies n elementen. Wegens symmetrie van $\cong$ bestaat er namelijk een bijectie $g : n \to X$ en kunnen we X dus opsommen:

$$X = \{g(0), \ldots, g(n-1)\} = \{x_0, \ldots, x_{n-1}\}. \tag{4.14}$$

Definitie 4.6 *Een verzameling X heet:*
- **eindig** *als er een $n \in \mathbb{N}$ bestaat zodat $X \cong n$ (notatie: $|X| = n$);*
- **oneindig** *als dit niet het geval is (d.w.z. X niet eindig is);*
- **aftelbaar oneindig** *(of* **aftelbaar***) als $X \cong \mathbb{N}$;*
- **overaftelbaar** *als X eindig noch aftelbaar oneindig is.*

Stelling 4.7 *Als X eindig is, dan geldt $X \cong Y$ desda Y ook eindig is en Y precies evenveel elementen heeft als X (dus als $X \cong n$ dan $X \cong Y$ desda $Y \cong n$).*

Dit volgt uit hetzelfde soort argumenten dat aantoont dat $\cong$ een equivalentierelatie is:

- Van links naar rechts: X eindig $\Rightarrow$ er is een $n \in \mathbb{N}$ en een bijectie $g : n \to X$ (zie boven); $X \cong Y \Rightarrow$ er is een bijectie $f : X \to Y \Rightarrow$ er is een bijectie $f \circ g : n \to Y$.
- Van rechts naar links: uit bijecties $h : X \to n$ en $i : n \to Y$ halen we een bijectie $i \circ h : X \to Y$. Q.E.D.

Als twee *eindige* verzamelingen X en Y evenveel elementen hebben, zeg $n \in \mathbb{N}$, dan krijg je in de praktijk simpelweg een bijectie door hun elementen op een willekeurige manier te nummeren, als in (4.14), en analoog $Y = \{y_0, \ldots, y_{n-1}\}$. Dan is de volgende functie $f : X \to Y$ een bijectie: kies $f(x_i) = y_i$ voor $i = 0, \ldots, n-1$ (als $Y = X$ krijg je zo een permutatie van X). Hoe zit het met oneindige verzamelingen als $\mathbb{N}$? Zelfs in het aftelbare geval sta je meteen al voor een verrassing. Laat de verzameling $E = \{2n \mid n \in \mathbb{N}\}$ even getallen zijn. Ofschoon E een echte deelverzameling is van $\mathbb{N}$ en $\mathbb{N} - E$ zelfs oneindig is, geldt $E \cong \mathbb{N}$, omdat de functie $f : \mathbb{N} \to E$ gegeven door $f(n) = 2n$ een bijectie is (ga na volgens de definitie). Zelfs geldt

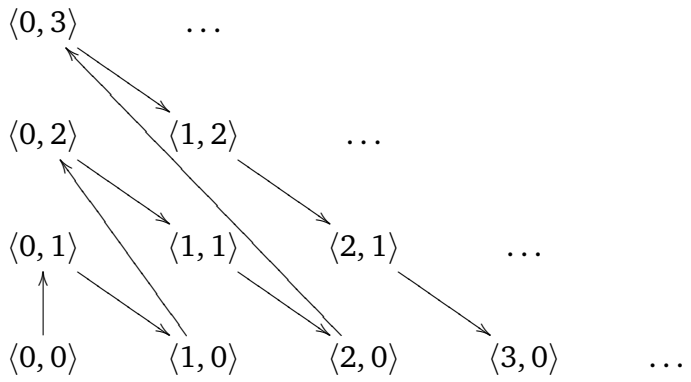
$$\mathbb{N} \times \mathbb{N} \cong \mathbb{N}. \tag{4.15}$$

2. In **ZF** bestaat er geen verzameling van alle verzamelingen, maar voor dit doel mag het wel even.

Bewijs: 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 $\mathbb{N}$. We maken echter als volgt een verrassende bijectie van $\mathbb{N}$ naar $\mathbb{N} \times \mathbb{N}$ (zie ook opgave 4.7):

$$0 \mapsto \langle 0,0\rangle, 1 \mapsto \langle 0,1\rangle, 2 \mapsto \langle 1,0\rangle, 3 \mapsto \langle 0,2\rangle, \ldots$$

of veel instructiever in een diagram:



Q.E.D.

Definitie 4.8 *We schrijven $X \leqslant Y$ als er een injectie $X \to Y$ bestaat (ook als $X \cong Y$) en $X < Y$ als $X \leqslant Y$ en $X \ncong Y$, d.w.z. er is wel een injectie $X \to Y$ maar geen bijectie.*

Stelling 4.9 (Cantor) *Voor iedere verzameling X geldt $X < P(X)$.*

Bewijs (diagonaalargument). De afbeelding $x \mapsto \{x\}$ laat zien dat $X \leqslant P(X)$; ga na dat dit een injectie is! Stel nu dat er een bijectie $f : X \to P(X)$ bestaat. Definieer

$$D = \{z \in X \mid z \notin f(z)\}.$$

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

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

Dit is een tegenspraak, zodat een bijectie f zoals boven niet kan bestaan. Q.E.D.

Als je alleen maar wilt bewijzen dat $X \to Y$ zonder een expliciete bijectie te geven, kun je de volgende *Stelling van Cantor-Schröder-Bernstein-Dedekind* gebruiken:[3]

Stelling 4.10 *Als zowel geldt $X \leqslant Y$ als $Y \leqslant X$, dan is $X \cong Y$ (en omgekeerd).*

Je kunt $\leqslant$ dus zien als een partiële ordening op de klasse van alle verzamelingen (echter met $\cong$ in de rol van $=$), zoals $\cong$ een equivalentierelatie op dezelfde klasse is. Het bewijs van Stelling 4.10 is een bonusopgave, gebaseerd op het volgende speciale geval:

Lemma 4.11 *Als $Z \subset X$ en $f : X \to Z$ is een injectie, dan is $X \cong Z$.*

3. Zie ook Velleman, Theorem 8.3.2 in §8.3 voor een uitvoerige discussie.

4.4 Karakteristieke functies en deelverzamelingen

Om te bewijzen dat $X \cong Y$ kun je vaak expliciet een bijectie $f : X \to Y$ opschrijven. Zodra je een kandidaat voor f hebt zijn daar dankzij Stelling 4.3 twee strategieën voor:

1. Toon apart aan dat f een injectie is en dat f een surjectie is.
2. Vind een functie g die voldoet aan $g \circ f = \mathrm{id}_X$ en $f \circ g = \mathrm{id}_Y$ (dan is $g = f^{-1}$).

In het voorbeeld na Stelling 4.7 zie je het eerste direct. Voor de tweede strategie is de functie $g : Y \to X$ gegeven door $g(y_i) = x_i$ voor $i = 0, \ldots, n-1$ een/de inverse van f.

We geven nu een ander voorbeeld van deze strategieën dat ook op zich informatief is. Naast $\mathrm{id}_X : X \to X$ is er nog een heel algemeen soort functie die je vaak tegenkomt. Voor iedere verzameling X nemen we $Y = 2 = \{0, 1\}$ en dan definiëren we voor iedere deelverzameling $W \subset X$ de ***karakteristieke functie*** $1_W : X \to 2$ door middel van:

$$1_W(x) = 1 \text{ als } x \in W; \tag{4.16}$$

$$1_W(x) = 0 \text{ als } x \notin W. \tag{4.17}$$

Als speciale gevallen hebben we $1_X(x) = 1$ en $1_\emptyset(x) = 0$ voor alle $x \in X$. Omgekeerd hoort bij iedere functie $h : X \to 2 = \{0, 1\}$ een deelverzameling W_h van X, namelijk

$$W_h = \{x \in X \mid h(x) = 1\} = h^{-1}(\{1\}). \tag{4.18}$$

De deelverzameling W bevat dus dezelfde informatie als de karakteristieke functie 1_W. We schrijven 2^X voor de verzameling van alle functies $h : X \to 2$. Algemener noteren we de verzameling van alle functies $h : X \to Y$ als Y^X (deze verzameling bestaat volgens **ZF**). De notatie Y^X komt uit ons voorbeeld: als $Y = 2 = \{0, 1\}$ en X heeft n elementen, dan heeft 2^X volgens Stellingen 2.1 en 4.12 precies 2^n elementen.

Stelling 4.12 *Voor iedere verzameling X is de functie $f : P(X) \to 2^X$ gedefinieerd door $f(W) = 1_W$ (preciezer: door de grafiek $G_f = \{\langle W, 1_W\rangle \mid W \subset X\}$) een bijectie.*

Bewijsstrategie 1: we bewijzen apart dat de functie f zowel injectief als surjectief is.

- f is *injectief:* als $f(W) = f(Z)$, oftewel $1_W = 1_Z$, dan is $1_W(x) = 1$ desda $1_Z(x) = 1$ en is dus volgens (4.16) ook $x \in W$ desda $x \in Z$. Regel 1 in voor verzamelingenleer in §2 (of formeler axioma **ZF1**) geeft dus $W = Z$.
- f is *surjectief:* voor $h \in 2^X$ definiëren we $W_h \in P(X)$ door (4.18), zodat $h = 1_{W_h}$. Daarmee geldt $h = f(W_h)$, zodat iedere h in het beeld van f ligt.

Bewijsstrategie 2: De functie $g : 2^X \to P(X)$ gedefinieerd door $g(h) = W_h$, zie (4.18), voldoet aan $g \circ f = \mathrm{id}_{P(X)}$ en $f \circ g = \mathrm{id}_{2^X}$. Dit volgt uit respectievelijk

$$W_{1_W} = W; \qquad 1_{W_h} = h, \tag{4.19}$$

voor alle $W \subset X$ en $h : X \to 2$, zoals je makkelijk uit de definities na kunt gaan. Links staat $g(1_W) = W$ oftewel $g(f(W)) = W$ oftewel $g \circ f = \mathrm{id}_{P(X)}$, en analoog staat rechts $f(W_h) = h$ oftewel $f(g(h)) = h$ oftewel $f \circ g = \mathrm{id}_{2^X}$. Q.E.D.

4.5 Equivalentierelaties en projecties

De volgende constructie komt vaak voor, om te beginnen in het volgende hoofdstuk.

Stelling 4.13 *Stel* $f : X \to Y$ *is een functie. Dan is de relatie* $\sim$ *op* X *gedefinieerd door*

$$x_1 \sim x_2 \text{ desda } f(x_1) = f(x_2) \tag{4.20}$$

een equivalentierelatie. Voor het bijbehorende quotient geldt

$$X/\sim \;\cong\; f(X), \tag{4.21}$$

waarbij een (mogelijke) bijectie de functie $g : X/\sim \to f(X)$ *is, gedefinieerd door*

$$g([x]) = f(x). \tag{4.22}$$

Als f *surjectief is (d.w.z.* $f(X) = Y$*), geldt dus, met als bijectie dezelfde functie* (4.22)*,*

$$X/\sim \;\cong\; Y. \tag{4.23}$$

De definitie van de functie (4.22) van $X/\sim$ naar $f(X) \subset Y$ lijkt riskant, omdat het argument van g de equivalentieklasse $[x]$ is, terwijl rechts x zelf staat. Toch is g welgedefinieerd, want als $[x_1] = [x_2]$, dan geldt vanwege (3.21) en (4.20) ook $f(x_1) = f(x_2)$. Dit argument vatten we samen in een algemeen principe dat nog vaak voor zal komen:

Stelling 4.14 *Als* $\sim$ *een equivalentierelatie is op* X *en* $f : X \to Y$ *een functie zodat*

$$x_1 \sim x_2 \to f(x_1) = f(x_2), \tag{4.24}$$

dan is $g : (X/\sim) \to Y$ *gegeven door* (4.22) *welgedefinieerd, in de zin dat* $g([x])$ *uitsluitend afhangt van de equivalentieklasse* $[x]$ *(en niet de keuze van het element* $x \in [x]$*).*

Bewijs van Stelling 4.13. Om te bewijzen dat $\sim$ een equivalentierelatie is gaan we de drie eisen daarop na: *reflexief* (xRx), *transitief* (xRy en $yRz \Rightarrow xRz$), en *symmetrisch* ($xRy \Rightarrow yRx$). Die volgen, in deze volgorde, alle drie uit bewijsregel(s) 15 onder (2.68). Om te bewijzen dat g een bijectie is volgen we strategie 1 uit de vorige sectie en bewijzen dus apart dat g injectief en surjectief is (probeer strategie 2 zelf).

- *Injectief*: stel $g(y_1) = g(y_2)$, met $y_1 = [x_1]$ en $y_2 = [x_2]$. Dan volgt uit de definitie van g dat $f(x_1) = f(x_2)$, daaruit volgens (4.20) dat $x_1 \sim x_2$, daaruit volgens (3.21) dat $[x_1] = [x_2]$, en daaruit $y_1 = y_2$. Klaar, zie (4.6).
- *Surjectief*: je moet voor iedere $z = f(x) \in f(X)$ een $y \in X/\sim$ vinden met $g(y) = z$. Neem $y = [x]$ en gebruik (4.22): $g(y) = g([x]) = f(x) = z$. Q.E.D.

Stelling (4.13) gaat van een functie f naar een equivalentierelatie, met het mooiste resultaat (4.23) als f surjectief is. Omgekeerd hoort bij een willekeurige equivalentierelatie $\sim$ op X een surjectieve functie naar $Y = X/\sim$, genaamd de ***canonieke projectie***:

$$p : X \to X/\sim; \qquad p(x) = [x]. \tag{4.25}$$

4.6 Het keuzeaxioma

Het bovenstaande materiaal heeft een belangrijke toepassing in de vorm van een nieuw axioma voor de verzamelingenleer, bovenop axioma's **ZF1** t/m **ZF9**. Dit zogenaamde ***keuzeaxioma*** werd in 1904 ingevoerd door Zermelo, met name om bepaalde bewijzen in de Analyse en Topologie mogelijk te maken. Het stelsel **ZF** samen met het keuzeaxioma heet **ZFC**, waar C staat voor *Choice*.[4] De *constructieve wiskunde* wijst het keuzeaxioma af, evenals de daarmee nauw gerelateerde *intuïtionistische wiskunde*.

Keuzeaxioma (versie 1): Voor iedere equivalentierelatie $\sim$ op een verzameling X bestaat een deelverzameling $W \subset X$ zodat $[x] \cap W$ voor iedere $x \in X$ precies één element heeft (equivalent: zodat $W \cong X/\sim$ via de functie $x \mapsto [x]$, met $x \in X$).

Je kunt dus voor iedere equivalentieklasse $[x]$ in $X/\sim$ een *representant* $[x] \cap W$ in X "kiezen". Hieruit volgt $X/\sim \leqslant X$. Een gangbare equivalente vorm van het keuzeaxioma is als volgt. Eerst definiëren we een ***rechts-inverse*** van een functie $f : X \to Y$ als een functie $s : Y \to X$ die voldoet aan $f \circ s = \mathrm{id}_Y$ oftewel $f(s(y)) = y$ voor alle $y \in Y$. Zo'n rechts-inverse hoeft niet te bestaan! Het keuzeaxioma zegt hier juist iets over.

Keuzeaxioma (versie 2): voor iedere equivalentierelatie $\sim$ op een verzameling X heeft de functie $p : X \to X/\sim$ in (4.25) een rechts-inverse $s : X/\sim \to X$.

Via het tweede deel van Stelling 4.13, met name (4.23), is deze versie equivalent met:

Keuzeaxioma (versie 3): Iedere surjectie $f : X \to Y$ heeft een *rechts-inverse* $s : Y \to X$.

Hiermee bedoelen we dat versie 2 versie 3 impliceert en andersom. De equivalentie van versies 2 en 3 met versie 1 volgt uit Stelling 4.13 en de constructie daarna:

- versie 1 $\Rightarrow$ versie 3: gegeven een surjectie $f : X \to Y$ neem je in versie 1 de equivalentierelatie uit Stelling 4.13. Die stelling en versie 1 geven samen $W \cong Y$ via de bijectie $x \mapsto f(x)$, met $x \in W$. Voor $y \in Y$ is er dus een unieke $x \in W \subset X$ met $y = f(x)$. Kies nu $s(y) = x$ (equivalent: kies $s(y) = f^{-1}(y) \cap W$).
- versie 2 $\Rightarrow$ versie 1: gegeven $\sim$, kies een rechts-inverse $s : X/\sim \to X$ van de projectie $p : X \to X/\sim$ (versie 2), en definieer $W = s(X/\sim)$ als het beeld van s.

Keuzeaxioma (versie 4): Voor iedere niet-lege verzameling X bestaat een ***keuzefunctie*** $f : P(X) \to X$ met $f(W) \in W$ voor alle niet-lege deelverzamelingen $W \subset X$.

Dit is equivalent met, en tevens een speciaal geval (hoe?) van de volgende versie:

Keuzeaxioma (versie 5): Voor iedere niet-lege verzameling X bestaat een ***keuzefunctie*** $f : X \to \cup X$ met $f(x) \in x$ voor alle niet-lege elementen $x \in X$.

4. Zie Wikipedia, Axiom of choice, voor meer informatie. Er zijn hele boeken over het keuzeaxioma!

4.7 Opgaven bij hoofdstuk 4

Zie ook de exercises in Velleman, §5.1, 5.2, 5.3.

Opgave 4.1

Bewijs dat er voor alle verzamelingen X, Y, en Z een bijectie bestaat tussen de verzamelingen $(X \times Y) \times Z$ en $X \times (Y \times Z)$, d.w.z. $(X \times Y) \times Z \cong X \times (Y \times Z)$

Opgave 4.2

Laat zien dat $\mathrm{id}_X : X \to X$ de enige relatie op X is die zowel een functie als een equivalentierelatie is.

Opgave 4.3

Bewijs dat als f en g *beide* injectief/surjectief zijn, dan ook $g \circ f$ injectief/surjectief is. Geef tegenvoorbeelden waarbij slechts één van de twee injectief/surjectief is.

Opgave 4.4

Bewijs Stelling 4.4 (het eerste deel staat in Velleman, Theorem 5.3.3).

Opgave 4.5

Stel dat X een *eindige* verzameling is en dat $f : X \to X$. Bewijs dat f injectief is desda f surjectief is (in Lineaire Algebra zul je een soortgelijke stelling tegenkomen over lineaire functies tussen lineaire ruimtes = vector-ruimtes).

Opgave 4.6

Stel dat $f : X \to Y$, $g : Y \to Z$, en $h : Z \to W$ alle drie functies zijn. Bewijs dat

$$h \circ (g \circ f) = (h \circ g) \circ f. \tag{4.26}$$

Opgave 4.7

Laat zien dat de volgende functie van $\mathbb{N} \times \mathbb{N}$ naar $\mathbb{N}$ een bijectie is:

$$f(x, y) = \tfrac{1}{2}\big((x + y + 1)^2 - (x + y + 1)\big) + x. \tag{4.27}$$

Opgave 4.8

Stel dat $f : X \to Y$ en $g : Y \to Z$ functies zijn. Bewijs dat voor elke $W \subset Z$ geldt

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

Opgave 4.9

Met de notatie (4.3), laat zien dat, voor willekeurige $V \subset X$ en $W \subset X$,

$$f(V \cup W) = f(V) \cup f(W). \tag{4.28}$$

Bewijs dat dezelfde formule met $\cap$ in plaats van $\cup$ geldt desda f injectief is.

Opgave 4.10

Met de notatie (4.5), laat zien dat, voor willekeurige $U \subset Y$ en $Z \subset Y$,

$$f^{-1}(U \cup Z) = f^{-1}(U) \cup f^{-1}(Z). \tag{4.29}$$

Is dezelfde formule met $\cap$ in plaats van $\cup$ waar? Geef bewijs of tegenvoorbeeld.

Opgave 4.11

Gegeven een functie $f : X \to Y$ en een deelverzameling $Z \subset X$ definiëren we de ***beperking*** $f_{|Z} : Z \to Y$ van f tot Z via de grafiek

$$G_{f_{|Z}} := G_f \cap (Z \times Y).$$

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

a) Laat zien dat $f_{|Z} = f \circ i_{Z \hookrightarrow X}$, waar $i_{Z \hookrightarrow X} : Z \to X$ (soms minder nauwkeurig ook als i_Z genoteerd) de functie $x \mapsto x$ is.

b) Stel dat $W \subset Z \subset X$. Bewijs dat $(f_{|Z})_{|W} = f_{|W}$.

c) Stel dat $V \subset Y$. Bewijs dat $f^{-1}_{|Z}(V) = Z \cap f^{-1}(V)$.

Opgave 4.12

Bewijs Stelling 4.10 vanuit Lemma 4.11 (dat je zonder bewijs aan mag nemen).

Opgave 4.13

a) Laat zien dat de functie (4.25) inderdaad surjectief is, en voldoet, met de notatie (4.5), aan

$$p^{-1}([x]) = [x]. \tag{4.30}$$

N.B. Let op notatie en context: in het linkerlid is $[x] \in X/\sim$, terwijl in het rechterlid $[x] \subset X$.

b) Laat zien dat de cirkel nu rond is, in de zin dat als we in Stelling 4.13 nemen $Y = X/\sim$ en $f = p$, dan de equivalentierelatie (4.20) weer de oorspronkelijke is die aan de basis van (4.25) ligt.

Opgave 4.14

Bewijs de equivalentie van versie 4 van het keuzeaxioma met, naar keuze (!) één van de andere drie. Bewijs vervolgens dat versie 4 (en daarmee alle versies) al in **ZF** geldt indien X eindig is (in welk geval het dus overbodig is als extra axioma).

5

Getallen

We gaan nu vrijwel alle abstractie die tot nu toe is opgebouwd inzetten om de jullie bekende wiskunde (en daarna nieuwe!) van de grond af op te bouwen. Dit begint met getalsystemen, waarvan er in de loop van de geschiedenis verschillende soorten zijn geïntroduceerd. Daarbij hebben vooral twee zaken een belangrijke rol gespeeld:

1. het kunnen oplossen van vergelijkingen (zoals $x^2 = 2$ al in de oudheid);
2. het rigoreus onderbouwen van de Analyse via de reële getallen $\mathbb{R}$ (19e eeuw).

In dit hoofdstuk bespreken we de eenvoudigste en meest voorkomende getalsystemen

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}, \tag{5.1}$$

met als uitgangspunt de ***natuurlijke getallen*** $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, waaruit (tenminste in de moderne wiskunde) alle andere getalsystemen in (5.1) worden geconstrueerd.

5.1 De natuurlijke getallen $\mathbb{N}$

Er zijn minstens vier manieren om tegen de natuurlijke getallen aan te kijken:

1. "*Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.*" (Leopold Kronecker, 1823–1891).
2. "*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.*" (Bertrand Russell, 1872–1970).
3. Identificatie met de verzameling $\mathbb{N}$ in verzamelingenleer à la **ZF** (zie regel 7).[1]
4. Impliciete beschrijving van $\mathbb{N}$ door middel van de Dedekind–Peano axioma's.

Ofschoon de standpunten van Kronecker en Russell wellicht zeer wijs zijn, gooien ze de handdoek feitelijk in de ring. We gaan in deze inleiding daarom uit van het derde en vierde standpunt. Het derde heeft als nadeel dat men een relatief elementair begrip ($\mathbb{N}$) ophangt aan een veel ingewikkelder bouwwerk (**ZF**). Het vierde is veel directer.[2] De Dedekind–Peano axioma's beschrijven eerst $\mathbb{N}$ als verzameling, uitgaande van de (helemaal in stijl ongedefinieerde) begrippen 0 en "opvolger", en luiden als volgt:

1. In die context wordt $\mathbb{N}$ door verzamelingstheoretici en logici meestal als ω aangeduid.
2. De Dedekind–Peano axioma's worden vaak alleen genoemd naar de laatste, die ze 1889 opschreef met een logische precisie die nu als ontoereikend wordt ervaren maar in die tijd voorbeeldig was. De bijdrage van Dedekind staat in zijn beroemde boek *Was sind und was sollen die Zahlen?* uit 1888.

1. 0 is een natuurlijk getal.
2. Ieder natuurlijk getal n heeft als zodanig een opvolger $S(n)$.
3. 0 is niet de opvolger van enig natuurlijk getal.
4. Als twee natuurlijke getallen dezelfde opvolger hebben zijn ze identiek.
5. Als $P(n)$ een eigenschap van natuurlijke getallen n is zodanig dat:
   (a) $P(0)$ geldt; (b) Als $P(n)$ geldt, dan geldt ook $P(S(n))$,
   dan geldt $P(n)$ voor alle natuurlijke getallen n (***inductie-axioma***).

No. 5 is equivalent met: als $P \subset \mathbb{N}$ een deelverzameling van $\mathbb{N}$ is zodat $0 \in P$ en de implicatie $(n \in P) \to (S(n) \in P)$ geldt, dan is $P = \mathbb{N}$. Dit volgt uit no. 5 via $P(n) := (n \in P)$. Omgekeerd volgt no. 5 uit de equivalente versie via $P = \{n \in \mathbb{N} \mid P(n)\}$.
Vanuit deze axioma's zijn al een paar eenvoudige stellingen te bewijzen, zoals

$$\forall_{n\in\mathbb{N}}(S(n) \neq n). \tag{5.2}$$

Bewijs. We noemen de eigenschap $S(n) \neq n$ verder $P(n)$. Uit axioma's 1 en 3 volgt dat $P(0)$ waar is, want (bewijs uit het ongerijmde) als $S(0) \neq 0$ *niet* waar is, zodat $S(0) = 0$, dan zou 0 wel degelijk de opvolger zijn van een natuurlijk getal, namelijk 0. Neem nu aan dat $P(n)$ geldt. Uit axioma's 2 en 4 volgt dat $P(S(n))$ geldt, met opnieuw een bewijs uit het ongerijmde: uit $S(S(n)) = S(n)$ volgt immers via axioma 4 dat $S(n) = n$, in tegenspraak met de aanname $P(n)$. Ten slotte volgt de claim uit axioma 5. Q.E.D.

Sectie 5.2 gaat nader in op bewijzen via het inductie-axioma. Intussen definiëren we

$$1 := S(0), \qquad 2 := S(1), \qquad 3 := S(2), \qquad 4 := S(3), \ldots \tag{5.3}$$

Deze getallen willen we optellen en vermenigvuldigen. Dat lukt via nieuwe axioma's:

6. $m + 1 = S(m)$.
7. $m + S(n) = S(m + n)$.
8. $m \times 0 = 0$.
9. $m \times S(n) = (m \times n) + m$.

Hier zou je in de eerste-orde logica kwantoren voor moeten zetten (zoals $\forall_{m\in\mathbb{N}}$ bij axioma 6), maar omdat het stelsel sowieso niet in die taal is opgeschreven laten we die weg (axioma 6 is in feite een notatie en alles loopt door elkaar). Latere wiskundigen hebben de Dedekind-Peano axioma's omgeschreven in de taal van eerste-orde logica, die in deze toepassing ten opzichte van **ZF** in §2.2 de volgende wijzigingen ondergaat:

- In plaats van de naam $\emptyset$ in **ZF** hebben we in **PA** de namen 0 en 1, en de daarvan afgeleide namen $2 := S(1) = 1 + 1$, $3 = S(2) = 2 + 1$, $4 := S(3) = 3 + 1$, enz.
- In plaats van het symbool $\in$ in **ZF** hebben we in **PA** de symbolen $+$ en $\times$.
- **PA** heeft meer soorten termen dan **ZF** (waarin alleen regel 1 hieronder geldt):
  1. **Variabelen of namen zijn termen.**
  2. **Als t_1 en t_2 termen zijn, dan zijn $t_1 + t_2$ en $t_1 \times t_2$ termen.**
- **Als t_1 en t_2 termen zijn, dan is $t_1 = t_2$ een formule** (evenals in **ZF**).

Formatieregel 2 op p. 38 in §2.2 geldt ook hier, waarbij de kwantoren $\forall_x$ en $\exists_x$ in **PA** over alle natuurlijke getallen lopen. De Dedekind-Peano axioma's zien er als volgt uit:[3]

$$\textbf{PA1} : \neg\exists_x(x+1=0); \tag{5.4}$$
$$\textbf{PA2} : \forall_x\forall_y(x+1=y+1\to x=y); \tag{5.5}$$
$$\textbf{PA3} : \forall_x(x+0=x); \tag{5.6}$$
$$\textbf{PA4} : \forall_x\forall_y(x+(y+1)=(x+y)+1); \tag{5.7}$$
$$\textbf{PA5} : \forall_x(x\times 0=0); \tag{5.8}$$
$$\textbf{PA6} : \forall_x\forall_y(x\times(y+1)=(x\times y)+x); \tag{5.9}$$
$$\textbf{PA7} : (F(0)\wedge\forall_x(F(x)\to F(x+1)))\to\forall_x F(x). \tag{5.10}$$

We gebruiken hier S niet meer wegens axioma/definitie 6 boven (het is echter ook in eerste-orde logica mogelijk om S aan te houden). De oude axioma's 1, 2, en 6 zijn nu in de notatie terechtgekomen, axioma 3 is nu **PA1**, axioma 4 is **PA2**, het inductie-axioma 5 is nu **PA7**;[4] dit axioma geldt voor alle formules $F(x)$ met vrije variabele (tenminste) x. Axioma's 7, 8, en 9 zijn respectievelijk **PA4**, **PA5**, en **PA6**. Axioma **PA3** volgde in de oude opzet uit de axioma's, maar nu S is weggevallen moet het apart worden genoemd. Axioma's **PA1** t/m **PA6** zijn waar vanuit je kennis over optellen en vermenigvuldigen, maar het punt is dat ze deze kennis coderen en dat een computer die slechts deze axioma's kent (en de notatie begrijpt) alle mogelijke sommen correct kan maken en in principe bovendien stellingen over de rekenkunde zou kunnen bewijzen. De eenvoudigste stelling uit **PA** is bijvoorbeeld

$$\textbf{PA}\vdash 0+0=0. \tag{5.11}$$

Deze volgt uit **PA3** door bewijsregel 12 met $t\rightsquigarrow 0$. Probeer zelf $\vdash 1\times 1=1$ (opgave). Lastiger te bewijzen (vanuit **PA1** t/m **PA7**) zijn de volgende stellingen in **PA**:[5]

$$\textbf{R1} : \forall_x\forall_y\forall_z\,(x+(y+z)=(x+y)+z)); \tag{5.12}$$
$$\textbf{R2} : \forall_x\forall_y(x+y=y+x); \tag{5.13}$$
$$\textbf{R3} : \forall_x\,(x+0=x); \tag{5.14}$$
$$\textbf{R4} : \forall_x\forall_y\forall_z\,(x\times(y\times z)=(x\times y)\times z)); \tag{5.15}$$
$$\textbf{R5} : \forall_x\forall_y(x\times y=y\times x); \tag{5.16}$$
$$\textbf{R6} : \forall_x\,(x\times 1=x); \tag{5.17}$$
$$\textbf{R7} : \forall_x\forall_y\forall_z\,(x\times(y+z)=x\times y+x\times z). \tag{5.18}$$

3. Ze heten standaard **PA** voor *Peano Arithemtic*, in plaats van het historisch meer correcte **DP**.
4. **PA7** is een *axioma-schema*, niet één axioma. Het is één axioma voor iedere formule $F(x)$.
5. Het volgende is voor later in je studie. Stellingen **R1** en **R2** zeggen dat optelling resp. *associatief* en *commutatief* zijn, en stellingen **R4** en **R5** zeggen dit over vermenigvuldiging. Stelling **R3** (= axioma **PA3**) zegt dat 0 een *neutraal element* is voor optelling, terwijl Stelling **R6** hetzelfde zegt over 1 ten opzichte van vermenigvuldiging. Stelling **R7** zegt dat vermenigvuldiging *distributief* is over optelling. Stelling **R1** maakt van $\mathbb{N}$ een *semigroep* onder optelling, evenzo maakt Stelling **R4** van $\mathbb{N}$ een semigroep onder vermenigvuldiging. Stellingen **R2** resp. **R5** maken daar *commutatieve* semigroepen van, en de eigenschappen **R3** resp. **R6** versterken een semigroep tot een *monoïde* (d.w.z. een semigroep met eenheid).

5.2 Intermezzo: inductie

Stel dat je het volgende wilt bewijzen: Voor alle $n \in \mathbb{N}$ geldt

$$\sum_{k=0}^{n} k = \tfrac{1}{2}n(n+1). \tag{5.19}$$

Hier betekent, voor $m \leqslant n \in \mathbb{N}$ en $f : \mathbb{N} \to \mathbb{N}$ (later: $f : \mathbb{N} \to \mathbb{R}$ of $\mathbb{C}$), de notatie:

$$\sum_{k=m}^{n} f(k) := f(m) + \cdots + f(n). \tag{5.20}$$

In (5.19) is $f(k) = k$ en staat er dus $\sum_{k=0}^{n} k = 0 + 1 + \cdots + n$ (voor $n = 0$ is $\sum_{k=0}^{0} = 0$).

Methode 1: Omdat $n = \{0, 1, 2, 3, \ldots\}$ bewijs je de uitspraak achtereenvolgens voor alle waarden van n apart. Dit proces duurt echter oneindig lang en werkt niet.

Methode 2: Op grond van bewijsregel 11 (uit $F(x)$ volgt $\forall_x F(x)$) bewijs je de uitspraak voor willekeurige $n \in \mathbb{N}$. Dat kan toevallig in dit geval, omdat het een "pedagogisch voorbeeld" is, maar meestal werkt alleen de volgende methode:

Methode 3: Bewijs (5.19) eerst voor $n = 0$. Dan staat er $0 = 0$, dus dat klopt. Bewijs vervolgens dat uit (de vooralsnog onbewezen) uitspraak (5.19) voor willekeurige n diezelfde uitspraak voor $n + 1$ volgt, dus $\sum_{k=0}^{n+1} k = \frac{1}{2}(n+1)(n+2)$. Inderdaad:

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + (n+1) = \tfrac{1}{2}n(n+1) + (n+1) = \tfrac{1}{2}(n+1)(n+2). \tag{5.21}$$

Hier volgt het tweede = teken uit de aanname (5.19).

Deze derde bewijsmethode is gebaseerd op het *principe van volledige inductie*. Stel dat we een uitspraak $\forall_{n\in\mathbb{N}} F(n)$ willen bewijzen, waarbij $F(n)$ een formule is met vrije variabele n. In het voorbeeld boven is $F(n)$ de formule (5.19). Dan is het volgens het vijfde Dedekind–Peano axioma in §5.1, of axioma **PA7**, voldoende om te bewijzen dat:

1. $F(0)$ waar is, of algemener: $F(m)$ waar is voor willekeurige $m \in \mathbb{N}$;
2. voor iedere $n \in \mathbb{N}$ de implicatie $F(n) \to F(n+1)$ waar is.

Stap 1 heet de ***basis*** van de inductie, stap 2 de ***inductiestap***, en $F(n)$ de ***inductiehypothese***. Als we stap 1 en stap 2 hebben bewezen, volgt de uitspraak voor alle $n \geqslant m$:

Uit $F(m)$ en $\forall_{n\geqslant m}(F(n) \to F(n+1))$ volgt $\forall_{n\geqslant m} F(n)$.

Hier is een voorbeeld met $m = 1$. Voor elke $n \in \mathbb{N}$ is $n!$ ("n ***faculteit***") gedefinieerd als

$$n! := n(n-1)! = 1 \cdot 2 \cdot \ldots \cdot n \quad (n > 0); \qquad 0! = 1. \tag{5.22}$$

Een ***permutatie*** van n objecten is een bijectie $p : n \to n$, waarbij we de verzameling n als gedefinieerd in (2.18) in dit geval meestal (her)schrijven als $\{1, \ldots, n\}$, waarbij de laatste n de "gewone" n uit het dagelijks leven is, zodat $p : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Voor een gegeven n geven we de verzameling permutaties van $\{1, \ldots, n\}$ aan met S_n.

Stelling 5.1 *Voor elke* $n \geqslant 1$ *geldt* $|S_n| = n!$.

Hierbij is $|X|$ het aantal elementen van een eindige verzameling X. Dit zegt algemener dat $|S_n| = n!$ het aantal bijecties is tussen elke twee verzamelingen met n elementen.

Bewijs. We bewijzen dit met inductie naar n vanaf $n = 1$. Voor $n = 1$ geldt de bewering, want $1! = 1$. Stel nu dat $|S_n| = n!$; we bewijzen dat $|S_{n+1}| = (n+1)!$. Als p een permutatie is van $\{1, \ldots, n+1\}$, dan zijn er $n+1$ mogelijkheden voor $p(n+1)$. Voor elke keuze van $p(n+1)$ is de beperking van p tot $\{1, \ldots, n\}$ een bijectie tussen twee verzamelingen met n elementen. Wegens de inductiehypothese zijn er hiervan $n!$, dus in totaal zijn er $(n+1)n! = (n+1)!$ mogelijkheden voor p, zie (5.22). Q.E.D.

Laat nu n en k getallen zijn in $\mathbb{N}$ met $n \geqslant k$. We definiëren de ***binomiaalcoëfficiënten***

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{5.23}$$

We spreken $\binom{n}{k}$ uit als "n boven k" (Engels: "n choose k"); dit is het aantal manieren om k elementen uit een verzameling van n elementen te kiezen (zie Propositie 5.3).

Stelling 5.2 (Regel van Pascal) *Voor elke* $n \geqslant k > 0$ *geldt*

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}. \tag{5.24}$$

Bewijs. Uitschrijven van de definitie geeft

$$\begin{aligned} \frac{n!}{(k-1)!(n+1-k)!} + \frac{n!}{k!(n-k)!} &= \frac{k \cdot n! + (n+1-k)n!}{k!(n+1-k)!} \\ &= \frac{(n+1)!}{k!(n+1-k)!} \end{aligned}$$ Q.E.D.

Dit geeft het volgende plaatje van de binomiaalcoëfficiënten, de *driehoek van Pascal*:[6]

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

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 (5.24).

6. De driehoek was reeds ver voor Pascal (1623–1662) 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). In dit boek wordt ook het principe van inductie voor het eerst expliciet beschreven.

Dit geeft tevens een snelle recursieve procedure om deze coëfficiënten te berekenen. Ook volgt dat $\binom{n}{k}$ altijd een geheel getal is (wat van tevoren allerminst duidelijk was).

Stelling 5.3 *Zij $n \in \mathbb{N}$, en laat X een verzameling zijn met n elementen. Dan geldt voor alle $0 \leqslant k \leqslant n$,*

$$\binom{n}{k} = \big|\{A \subset X : |A| = k\}\big|. \tag{5.25}$$

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, en zij X een verzameling met $n+1$ elementen. We bewijzen dat de uitspraak geldt voor X. Neem $x \in X$ vast. Dan zijn er voor elke $A \subset X$ 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 $\binom{n}{k-1}$ 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 $\binom{n}{k}$. Samen geeft dit, gebruik makend van Propositie 5.2, het aantal

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \tag{5.26}$$

verzamelingen A met k elementen. Q.E.D.

Stelling 5.4 (Binomium van Newton) *Voor alle $a, b \in \mathbb{R}$ en $n \in \mathbb{N}$ geldt*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{5.27}$$

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 hebben we de volgende eigenschappen gebruikt:

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \binom{n+1}{k}; \\ \binom{n}{0} &= \binom{n+1}{0}; \\ \binom{n}{n} &= \binom{n+1}{n+1}.\end{aligned}$$

Q.E.D.

Een tweede variatie op inductie (equivalent met het oorspronkelijke principe) is:

Uit $\forall_{n\in\mathbb{N}}((\forall_{m<n} F(m)) \to F(n))$ volgt $\forall_{n\in\mathbb{N}} F(n)$, waarin $\forall_{m<n} := \forall_{m\in\{0,\ldots,n-1\}}$.

Dit heet ***sterke inductie***. Zie ook Velleman, §6.4. Voor $n = 0$ betekent $\forall_{m<0} F(m)$ per definitie (2.70) dat $\forall_m((m < 0) \to F(m))$. Dit is voor alle formules $F(m)$ waar omdat $m < 0$ in $\mathbb{N}$ onwaar is en $\bot$ alles impliceert. Daarmee is de implicatie $\forall_{m<0} F(m) \to F(0)$ waar desda $F(0)$ waar is. Je kunt $\forall_{n\in\mathbb{N}}(\forall_{m<n} F(m) \to F(n))$ dus opsplitsen in het geval $n = 0$, dus $F(0)$, en $\forall_{n>0}((\forall_{m\leqslant n} F(m)) \to F(n+1))$, die je dus beide moet bewijzen.

Als voorbeeld van sterke inductie bewijzen we eindelijk (losjes) Stelling 1.2 uit hoofdstuk 1 met inductie naar het aantal symbolen n dat in de uitspraak A voorkomt. Voor $n = 1$ moet A zijn $\bot$ of een van de atomaire proposities P_i en is de claim waar, omdat $\nu(P_i)$ en $\nu(\bot)$ gegeven zijn, zie (1.5) voor $\bot$. Als $n > 1$ gebruiken we de regels (1.6) t/m (1.9) om A te laten werken op deelformules van kortere lengte, waarvoor de claim volgens de inductiehypothese waar is. Q.E.D.

Een andere toepassingen van inductie is *recursie*. Een functie $f : \mathbb{N} \to \mathbb{N}$ is ***recursief*** gedefinieerd als de waarde $f(n+1)$ gedefinieerd is in termen van $f(n)$ (een generalisatie volgt straks). Een voorbeeld is de functie $f(n) = n!$, die wordt gedefinieerd door

$$f(0) = 1; \tag{5.28}$$
$$f(n+1) = f(n)(n+1). \tag{5.29}$$

Hier uit volgt de al bekende definitie (5.22), die we nu precies maken.

Stelling 5.5 *Gegeven een natuurlijk getal $g \in \mathbb{N}$ en een functie $h : \mathbb{N}^2 \to \mathbb{N}$ bestaat er een unieke functie $f : \mathbb{N} \to \mathbb{N}$ zodat*

$$f(0) = g \tag{5.30}$$
$$f(n+1) = h(f(n), n). \tag{5.31}$$

Voorbeeld: om uit dit schema $n!$ te krijgen nemen we dus

$$g = 1; \tag{5.32}$$
$$h(m, n) = m(n+1). \tag{5.33}$$

Bewijs. In zo'n geval moet je apart bestaan en uniciteit (van f) bewijzen.

- *Bestaan.* Bewijs met volledige inductie naar n. De inductiehypothese $F(n)$ is: *er bestaat een functie $f : \mathbb{N} \to \mathbb{N}$ die voor alle $m \leqslant n$ voldoet aan* (5.30) *en aan*

$$f(m+1) = h(f(m), m). \tag{5.34}$$

  Dan is $F(0)$ dus: er bestaat een functie $f : \mathbb{N} \to \mathbb{N}$ die voldoet aan (5.30) en aan $f(1) = h(g, 0)$. Inderdaad: kies f zodat $f(0) = g$ en $f(1) = h(g, 0)$. De waarden $f(n)$ voor $n > 1$ zijn (nu nog) willekeurig. Stel nu dat $F(n)$ geldt, zodat $f(0)$ t/m $f(n+1)$ zijn vastgelegd. Uit $F(n)$ moeten we $F(n+1)$ bewijzen, en dat kan door f die volgens de inductiehypothese aan $F(n)$ voldoet, uit te breiden door te kiezen

$$f(n+2) = h(f(n+1), n+1). \tag{5.35}$$

Door deze keuze geldt de uitspraak $F(n+1)$ per definitie. Nu is bewezen

$$F(n) \to F(n+1),$$

en uit het principe van volledige inductie volgt nu $\forall_n F(n)$, oftewel: er bestaat een functie $f : \mathbb{N} \to \mathbb{N}$ die voor alle $m \leqslant n$ voldoet aan (5.30) en (5.31).

- *Uniciteit.* Uit het ongerijmde. Stel dat f_0 en f_1 beide voldoen aan (5.30) en (5.31), en stel dat $n_0 \in \mathbb{N}$ het kleinste getal is zodat $f_0(n_0) \neq f_1(n_0)$. Dan moet vanwege (5.30) gelden $n_0 > 0$, want voor $n_0 = 0$ is $f_0(0) = f_1(0) = g$. Dus is $n_0 = m_0 + 1$ voor zekere $m_0 \geqslant 0$. Maar dan volgt een tegenspraak met $f_0(m_0{+}1) \neq f_1(m_0{+}1)$:

$$f_0(m_0+1) = h(f_0(m_0), m_0) = h(f_1(m_0), m_0) = f_1(m_0+1).$$

Zo'n n_0 kan dus niet bestaan, zodat $f_0(n) = f_1(n)$ voor alle $n \in \mathbb{N}$. Q.E.D.

Hieruit volgt dat axioma's **PA3** en **PA4** optelling in $\mathbb{N}$, oftewel $m+n$, volledig vastleggen, waarbij $m+1$ al gedefinieerd is via $0+1=1$ (dit volgt via stelling **R2** uit **PA3**), en $1+1=:2$, $2+1=:3$, enz. Ten eerste volgt uit **PA3** en **PA4** m.b.v. bewijsregel 12

$$m+0=m; \qquad m+(n+1)=(m+n)+1. \tag{PA3,4}$$

Neem nu in Stelling 5.5: $g = m$ en $h(k,n) = k{+}1$ (deze functie hangt niet af van n). Dan luiden (5.30) en (5.31): $f(0) = m$ en $f(n{+}1) = f(n){+}1$. Als we hier provisorisch invullen $f(n) = m+n$ zijn deze twee gelijkheden precies (PA3,4), en is f welgedefinieerd als de unieke "oplossing" van het recursieschema (5.30) - (5.31). Analoog definiëren Axioma's **PA5** en **PA6** en Stelling 5.5 vermenigvuldiging. Kies nu namelijk $g = 0$ en $h(k,n) = k+m$, zodat (5.30) - (5.31) luiden: $f(0) = 0$ en $f(n+1) = f(n) + m$. Met $f(n) = m \times n$ volgen deze uit **PA5** en **PA6** en is f dus de unieke oplossing van het recursieschema!

In het algemeen hebben we de volgende uitbreiding van Stelling 5.5:

Stelling 5.6 (primitieve recursie) *Stel* $p \in \mathbb{N}$. *Gegeven functies*

$$g : \mathbb{N}^p \to \mathbb{N}; \tag{5.36}$$
$$h : \mathbb{N}^{p+2} \to \mathbb{N} \tag{5.37}$$

bestaat er een unieke functie $f : \mathbb{N}^{p+1} \to \mathbb{N}$ *zodat voor alle* $x \in \mathbb{N}$ *en* $\vec{y} \in \mathbb{N}^p$ *geldt:*

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

Het bewijs is vrijwel hetzelfde als van het speciale geval Stelling 5.5 (waarin $p = 0$). Een andere soort algemener voorbeeld van recursie is de beroemde ***rij van Fibonacci***:[7]

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

Elk getal in de Fibonacci-rij is de som van de *twee* voorafgaande getallen, oftewel: $F(n+2) = F(n+1) + F(n)$, met beginwaarden $F(0) = F(1) = 1$. Dit legt F geheel en uniek vast, hetgeen kan worden bewezen met sterke inductie (zie p. 67 bovenaan).

7. Naar de Italiaanse wiskundige Leonardo van Pisa (ca.1170 – ca.1250), ook bekend als Fibonacci. De rij van Fibonacci komt in de natuur veelvuldig voor, en is ook gerelateerd aan de zgn. gulden snede.

5.3 De gehele getallen $\mathbb{Z}$

Het probleem met de definitie van $\mathbb{Z}$ vanuit verzamelingenleer is dat $n = \{0, \ldots, n-1\}$ de verzameling is met n (specifieke) elementen, maar $-n$ moeilijk kan worden gedefinieerd als de verzameling met $-n$ elementen. Een oplossing is om paren $\langle m, n\rangle$ in $\mathbb{N} \times \mathbb{N}$ te nemen en $k \in \mathbb{Z}$ te definiëren als het verschil $m - n$. Het eerste probleem is echter dat we het minteken nog niet hebben (we hebben via de Peano-axioma's alleen optelling en vermenigvuldiging in $\mathbb{N}$ gedefinieerd) en het tweede probleem is dat er talloze paren $\langle m, n\rangle$ in $\mathbb{N} \times \mathbb{N}$ zijn met hetzelfde verschil. Gelukkig hebben we equivalentierelaties! Informeel willen we dus $\langle a, b\rangle \sim \langle c, d\rangle$ desda $a - b = c - d$.

Definitie 5.7 *Definieer een relatie $\sim$ op $\mathbb{N} \times \mathbb{N}$ door:*

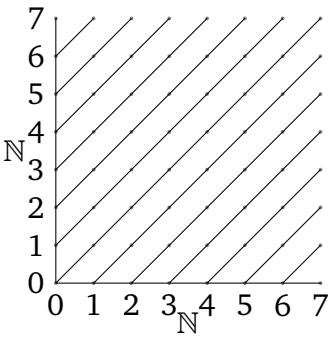
$$\langle a, b\rangle \sim \langle c, d\rangle \quad \textit{desda} \quad a + d = b + c. \tag{5.38}$$

Dit is een equivalentierelatie, en de gehele getallen zijn het bijbehorende quotiënt:

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim . \tag{5.39}$$

We geven de equivalentieklasse van het paar $\langle a, b\rangle \in \mathbb{N} \times \mathbb{N}$ in $(\mathbb{N} \times \mathbb{N})/\sim$ aan met $[a, b]$.

De bijbehorende equivalentieklassen zijn de diagonale lijnen in het onderstaande plaatje:



De equivalentieklassen zijn dus allemaal van een van de twee volgende vormen:

- Als $m \geqslant n$, dan geldt $[m, n] = \{\langle m - n + k, k\rangle \mid k = 0, 1, 2, \ldots\}$;
- Als $m < n$, dan geldt $[m, n] = \{\langle k, n - m + k\rangle \mid k = 1, 2, \ldots\}$;

We definiëren nu de optelling $+$ op $\mathbb{Z}$, gedefinieerd via (5.39), door middel van

$$[a, b] + [c, d] := [a + c, b + d]. \tag{5.40}$$

We moeten nagaan dat deze definitie op de equivalentieklassen $[a, b]$ niet afhangt van de keuze van de representanten $\langle a, b\rangle$, vgl. Stelling 4.14. Met andere woorden, stel dat $\langle a, b\rangle \sim \langle a', b'\rangle$, zodat $[a, b] = [a', b']$, en analoog $\langle c, d\rangle \sim \langle c', d'\rangle$, zodat $[c, d] = [c', d']$, dan moet gelden $\langle a+c, b+d\rangle \sim \langle a'+c', b'+d'\rangle$, oftewel $[a+c, b+d] = [a'+c', b'+d']$. Dit is een eenvoudige verificatie vanuit de definitie van $\sim$: uit $a + b' = b + a'$ en $c + d' = d + c'$ volgt immers direct $a + c + b' + d' = b + d + a' + c'$.

Om de $\mathbb{Z}$ uit Definitie 5.7 meer te laten lijken op de vertrouwde verzameling

$$\text{“}\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}\text{”} \tag{5.41}$$

geven we een verzameling $S \subset \mathbb{N}\times\mathbb{N}$ met de eigenschap dat S iedere equivalentieklasse precies één keer snijdt, zodat $S \cong (\mathbb{N} \times \mathbb{N})/\sim$. Uit het plaatje volgt een voor de hand liggen keuze, namelijk, met de notatie $\mathbb{N}_* = \mathbb{N} \setminus \{0\} = \{1, 2, 3, \ldots\}$,

$$S := \{\langle n, 0\rangle \mid n \in \mathbb{N}\} \cup \{\langle 0, n\rangle \mid n \in \mathbb{N}_*\}. \tag{5.42}$$

Als $m \geqslant n$, dan geldt $[m, n] \cap S = \langle m - n, 0\rangle$ op de horizontale as, en als $m < n$, dan hebben we $[m, n] \cap S = \langle 0, n - m\rangle$ op de verticale as. Met de identificaties

$$k := \langle k, 0\rangle; \qquad\qquad -k := \langle 0, k\rangle \tag{5.43}$$

hebben we dus

$$S = \{k \mid k \in \mathbb{N}\} \cup \{-k \mid k \in \mathbb{N}_*\} \cong \mathbb{Z}. \tag{5.44}$$

We hebben een injectie ι van $\mathbb{N}$ naar $\mathbb{Z}$, genoteerd $\mathbb{N} \overset{\iota}{\hookrightarrow} \mathbb{Z}$ en gegeven door $\iota(n) = [n, 0]$. Van $\mathbb{N}$ naar S is dit simpelweg $\iota(n) = \langle n, 0\rangle$. Dan is eenvoudig na te gaan dat

$$\iota(n) + \iota(m) = \iota(n + m). \tag{5.45}$$

We kunnen $\mathbb{N}$ dus opvatten als een deelverzameling van $\mathbb{Z}$, hoewel dat volgens de constructie van $\mathbb{Z}$ in Definitie 5.7 strikt genomen niet zo is. Toch schrijven we $\mathbb{N} \subset \mathbb{Z}$.

Voor $\mathbb{Q}$ hebben we ook vermenigvuldiging in $\mathbb{Z}$ nodig: met “$\langle a, b\rangle = a - b$” is deze

$$[a, b] \times [c, d] := [ac + bd, ad + bc]. \tag{5.46}$$

Ook hier geldt dat deze welgedefinieerd is en overeenkomt met de bekende op $\mathbb{N} \subset \mathbb{Z}$.

Ook $\mathbb{Z}$ met de boven gedefinieerde optelling en vermenigvuldiging voldoet aan de eigenschappen **R1** t/m **R7**, waarbij 0 de equivalentieklasse $[a, a] = [0, 0]$ is en 1 de equivalentieklasse $[1, 0]$. Maar $\mathbb{Z}$ heeft nog een extra eigenschap, namelijk

$$\textbf{R8}: \ \forall_x \exists_y (x + y = 0). \tag{5.47}$$

Als $x = [a, b]$ nemen we $y = [b, a]$ en schrijven $y = -x$. Uit (5.40) volgt immers

$$[a, b] + [b, a] = [a + b, b + a] = [a + b, a + b] = [0, 0] = 0,$$

waar **R2** en (5.38) zijn gebruikt. Merk op dat de y in **R8** uniek is: als $x + y = 0$ én $x + z = 0$, dan volgt uit de eerste $x + y + z = z$, daaruit $x + z + y = z$, en dan uit de tweede $0 + y = z$ en dus $y = z$. De eerste stap gebruikt de eigenschap $\forall_z((x = y) \to (x + z = y + z))$, die je weer kunt afleiden uit de extra afleidingsregel in §5.1 met $t(x) \rightsquigarrow x + z$. Nu dit duidelijk is,[8] kunnen we het verschil $x_1 - x_2$ in $\mathbb{Z}$ definiëren als

$$x_1 - x_2 := x_1 + (-x_2). \tag{5.48}$$

8. Voor later: de eigenschappen **R1** t/m **R8** maken $(\mathbb{Z}, +, \times)$ een ***commutatieve ring***, en het fragment $(\mathbb{Z}, +)$ is dankzij **R1** t/m **R3** en **R8** een ***abelse*** (of ***commutatieve***) ***groep***.

5.4 De rationale getallen $\mathbb{Q}$

De constructie van de rationale getallen $\mathbb{Q}$ zal nu geen verrassing meer zijn: we stellen breuken k/l (met $k \in \mathbb{Z}$ en $l \in \mathbb{Z}_*$) voor als equivalentieklassen$[k, l]$ in $\mathbb{Z} \times \mathbb{Z}_*$, waarbij

$$\mathbb{Z}_* := \mathbb{Z} \setminus \{0\}. \tag{5.49}$$

Definitie 5.8 *Definieer een relatie $\sim'$ op $\mathbb{Z} \times \mathbb{Z}_*$ door:*

$$\langle k, l\rangle \sim' \langle m, n\rangle \quad \textit{desda} \quad kn = lm. \tag{5.50}$$

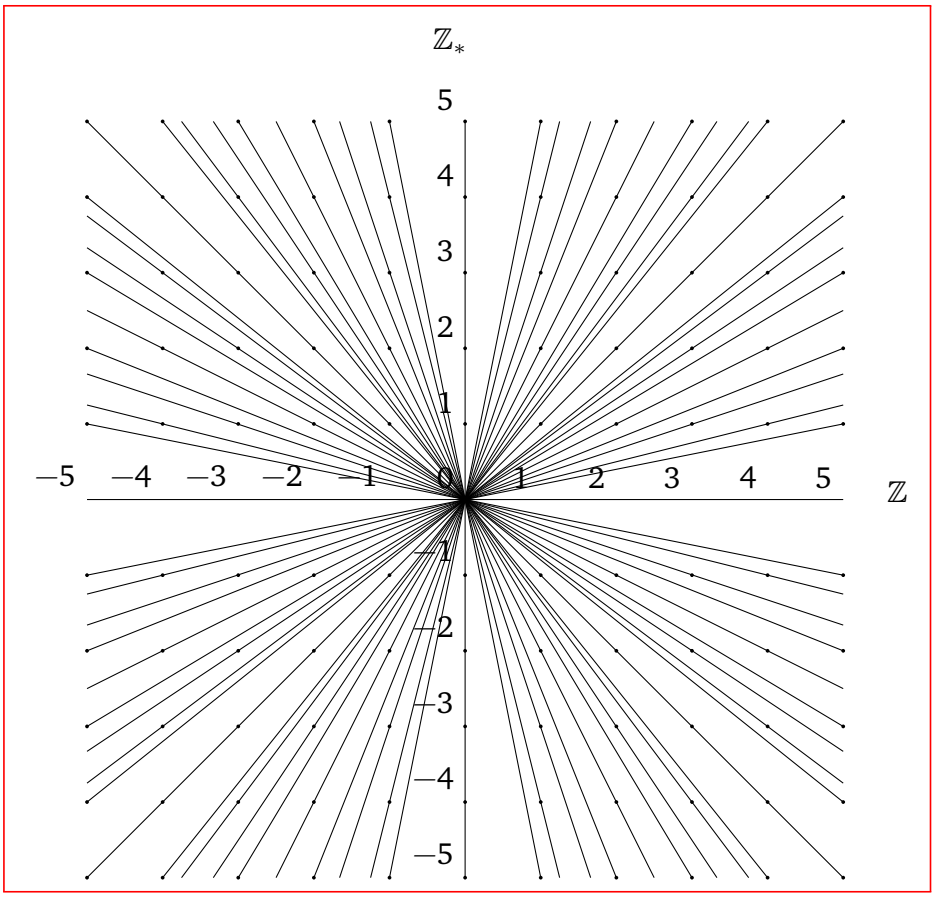
Dit is een equivalentierelatie. De rationale getallen zijn nu het bijbehorende quotiënt

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}_*)/\sim' . \tag{5.51}$$

We geven de equivalentieklasse ten opzichte van $\sim'$ aan met $[k, l]'$, enzovoort. De operaties optelling en vermenigvuldiging op $\mathbb{Q}$ zijn dan gedefinieerd door

$$[k, l]' + [m, n]' := [kn + lm, ln]'; \tag{5.52}$$
$$[k, l]' \times [m, n]' := [km, ln]'. \tag{5.53}$$

De $k \in \mathbb{Z}$ binnen het paar $[k, l]' \in \mathbb{Q}$ is zelf een paar $k = [a, b]$, en zo ook l, enzovoort. De equivalentieklassen van de equivalentierelatie $\sim'$ op $\mathbb{Z} \times \mathbb{Z}_*$ zien er als volgt uit:[9]



9. Plaatje gemaakt door Menzo van Kessel met behulp van het tikz package.

Wat is er gewonnen door de uitbreiding van $\mathbb{Z}$ naar $\mathbb{Q}$? Antwoord: de vergelijking

$$mx = n, \tag{5.54}$$

met $m, n \in \mathbb{Z}$ en $m \neq 0$, die zelden oplosbaar is in $\mathbb{Z}$ (namelijk alleen als n een veelvoud is van m), is altijd oplosbaar in $\mathbb{Q}$. Om dit in te zien moeten we de vergelijking (5.54) eerst herinterpreteren in $\mathbb{Q}$. Dat kan via de injectie $\mathbb{Z} \overset{\iota'}{\hookrightarrow} \mathbb{Q}$ gegeven door

$$\iota'(k) = [k, 1]', \tag{5.55}$$

Deze is analoog aan de injectie $\mathbb{N} \overset{\iota}{\hookrightarrow} \mathbb{Z}$ via $n \mapsto [n, 0]$. Dan wordt (5.54) herschreven als $[m, 1]'x = [n, 1]'$, met $m \neq 0$, en deze laatste vergelijking wordt in $\mathbb{Q}$ opgelost door $x = [n, m]'$. Immers, vanuit (5.53) geldt inderdaad $[m, 1]' \times [n, m]' = [mn, m]' = [n, 1]'$, want $\langle mn, m\rangle \sim' \langle n, 1\rangle$ via (5.50), zie (3.21) om je geheugen op te frissen! Algemener wordt de vergelijking $[k, l]' \times x = [m, n]'$ met $k, l, m, n \in \mathbb{Z}$ and $k, l, n \neq 0$ in $\mathbb{Q}$ opgelost door $x = [lm, kn]'$: ga weer vanuit (5.53) en (5.50) na dat $[k, l]' \times [lm, kn]' = [m, n]'$.

De "structuur" $(\mathbb{Q}, +, \times)$ heeft daarom nog weer betere eigenschappen dan $(\mathbb{Z}, +, \times)$: het is een ***lichaam***. Dit betekent dat behalve de eigenschappen **R1** t/m **R8**, ook geldt:

$$\mathbf{R9} : \forall_x((x \neq 0) \to \exists_y(x \times y = 1)), \tag{5.56}$$

evenals een eigenschap die ook in $\mathbb{N}$ en $\mathbb{Z}$ geldt maar pas bij de definitie van een lichaam officieel hoeft te worden opgeschreven, namelijk (typisch wiskundige precisie!)

$$\mathbf{R10} : 1 \neq 0. \tag{5.57}$$

Ook hier is eenvoudige te bewijzen dat de y in **R9** uniek is (gegeven x): het is de ***multiplicatieve inverse*** van x, genoteerd als $y = x^{-1}$. Voor breuken $x = p/q$ geldt $x^{-1} = q/p$; in de bovenstaande opzet hebben we $0 = [0, 1]'$, $1 = [1, 1]'$, en, als $l \neq 0$,

$$([k, l]')^{-1} = [l, k]'. \tag{5.58}$$

Net als voor $\mathbb{Z}$ kunnen we ook hier een unieke representant $\langle p, q\rangle \in \mathbb{Z} \times \mathbb{Z}_*$ van een equivalentieklasse $[p', q'] \in \mathbb{Q}$ kiezen. Voor $p, q \in \mathbb{N}_*$ betekent $\mathrm{ggd}(p, q) = 1$ dat er geen $k > 1$ (in $\mathbb{N}$) bestaat zodat $p = kl$ en $q = km$ (ggd = 'grootste gemene deler'). Voor $p' \in \mathbb{N}$ en $q' \in \mathbb{N}_*$, zodat $[p', q']' \in \mathbb{Q}$, kiezen we

$$\langle p, q\rangle \sim' \langle p', q'\rangle \text{ waarbij } \mathrm{ggd}(p, q) = 1. \tag{5.59}$$

Bestaan en uniciteit van p en q volgen uit de unieke ontbinding van natuurlijke getallen in priemfactoren (die we hier niet bewijzen):

$$p' = r_1^{k_1} \cdots r_n^{k_n}; \qquad q' = s_1^{l_1} \cdots s_n^{l_m}, \tag{5.60}$$

met alle $r_i \in \mathbb{N}$ priemgetallen (verschillend van elkaar) en alle $k_i \in \mathbb{N}$, en alle $s_i \in \mathbb{N}$ priem, etc. Gegeven deze ontbindingen kunnen we gelijke factoren in p' en q' tegen elkaar wegstrepen en in wat overblijft is geen enkele factor in de ontbinding van p gelijk aan een factor in q. Analoog voor $p \in \mathbb{Z} \setminus \mathbb{N}_*$ en $q \in \mathbb{N}_*$.

Als brug naar de reële getallen $\mathbb{R}$ (zoals later blijkt) sluiten we af met een mooie stelling.

Stelling 5.9 *1. De gebruikelijke relatie $\leqslant$ op $\mathbb{N}$ is een totale ordening, waarbij*

$$m \leqslant n \text{ desda } \exists_{k\in\mathbb{N}}\,(n = m + k). \tag{5.61}$$

2. De relatie $\leqslant$ op $\mathbb{Z}$, gegeven door

$$[a, b] \leqslant [c, d] \quad \text{desda} \quad a + d \leqslant b + c \text{ (in } \mathbb{N}), \tag{5.62}$$

is welgedefinieerd en is een totale ordening.[10]

3. De relatie $\leqslant$ op $\mathbb{Q}$, gegeven door

$$[k, l]' \leqslant [m, n]' \quad \text{desda} \quad kn \leqslant lm \text{ (in } \mathbb{Z}), \tag{5.63}$$

waarbij we aannemen dat $l, n > 0$, is welgedefinieerd en is een totale ordening.

Als de breuken al gelijknamig zijn ($l = n$) betekent (5.63) dat $(k/l) \leqslant (m/l)$ desda $k \leqslant m$. We brengen in herinnering dat $[\cdot, \cdot]$ de equivalentieklassen in $\mathbb{Z}$ zijn, zie Definitie 5.7, terwijl $[\cdot, \cdot]'$ de equivalentieklassen in $\mathbb{Q}$ zijn, volgens Definitie 5.8. In punt 2 van Stelling 5.9 betekent "welgedefinieerd" (analoog aan optelling en vermenigvuldiging):

- als $\langle a, b\rangle \sim \langle a', b'\rangle$ en $\langle c, d\rangle \sim \langle c', d'\rangle$, waarbij $\sim$ de relatie (5.38) is, dan geldt

$$[a, b] \leqslant [c, d] \qquad \text{desda} \qquad [a', b'] \leqslant [c', d'], \tag{5.64}$$

  en analoog voor (5.63).

Het bewijs dat (5.62) welgedefinieerd is, is als volgt (doe $\mathbb{Q}$ zelf):

1. Volgens (5.38) hebben we $\langle a, b\rangle \sim \langle a', b'\rangle$ desda $a + b' = a' + b$.
2. Dan geldt $a+d \leqslant b+c$ desda $a+b'+d \leqslant b'+b+c$, d.w.z. $a'+b+d \leqslant b'+b+c$, dus desda $a' + d \leqslant b' + c$, dus desda $a' + c' + d \leqslant b' + c' + c$.
3. Vervolgens is $\langle c, d\rangle \sim \langle c', d'\rangle$ desda $c + d' = c' + d$, zodat de vorige ongelijkheid geldt desda $a' + c + d' \leqslant b' + c + c'$ en dus desda $\langle c, d\rangle \sim \langle c', d'\rangle$.

Het bewijs van Stelling 5.9 is niet zo simpel. Het eerste deel (inclusief de claim dat $\leqslant$ überhaupt een partiële ordening is) moet officieel ofwel vanuit de Peano axioma's worden bewezen,[11] ofwel vanuit de constructie van $\mathbb{N}$ in de verzamelingenleer **ZF** via (2.18) en (2.24). In beide gevallen is het idee dat je de natuurlijke getallen een voor een krijgt door te beginnen bij 0 en daar steeds 1 bij op te tellen. Als m in deze stapsgewijze procedure eerder voorkomt dan n (of $m = n$) dan geldt $m \leqslant n$, en omgekeerd. Het geval $\mathbb{Z}$ volgt dan wel vrij eenvoudig via (5.42), waardoor het probleem tot $\mathbb{N}$ wordt teruggebracht. Ook het bewijs voor $\mathbb{Q}$ volgt (uit $\mathbb{Z}$) door het kiezen van representanten.

11. Zie E. Mendelson, *Introduction to Mathematical Logic, Fifth Edition* (CRC Press, 2010), Prop. 3.7.

5.5 De reële getallen $\mathbb{R}$: constructie volgens Dedekind

De reële getallen $\mathbb{R}$ zijn wenselijk omdat de rationale getallen $\mathbb{Q}$ op een nog precies te definiëren manier *onvolledig* zijn. De oudste indicatie daarvoor (5e eeuw v.Chr.) is:

Stelling 5.10 *De vergelijking $x^2 = 2$ heeft geen oplossing in $\mathbb{Q}$.*

Bewijs (antiek): Stel $(p/q)^2 = 2$, met $p, q \in \mathbb{N}_*$ en $p/q := [p, q]$ als in Definitie 5.8, d.w.z. $p^2 = 2q^2$. We mogen aannemen dat $\mathrm{ggd}(p, q) = 1$, zodat p en q niet beide even kunnen zijn (anders was 2 een gemene deler geweest). Er zijn twee gevallen:

- p is oneven. Dan is ook p^2 oneven,[12] maar $2q^2$ is even, tegenspraak met $p^2 = 2q^2$.
- p is even en q dus oneven, en daarmee dus ook q^2. Dan is p^2 deelbaar door 4 maar $2q^2$ niet, wat opnieuw een tegenspraak geeft met $p^2 = 2q^2$. Q.E.D.

Om de onvolledigheid van $\mathbb{Q}$ beter in kaart te brengen keren we terug naar Definitie 3.6. We geven een aantal voorbeelden met $X = \mathbb{Q}$, waarbij de partiële ordening de gebruikelijke is, zie (5.63), waarover je kunt denken als de normale $\leqslant$ op breuken.

1. De verzameling $Q_r^+ = \{q \in \mathbb{Q} \mid r \leqslant q\} \subset \mathbb{Q}$, waar $r \in \mathbb{Q}$ vast gekozen is, heeft geen bovengrens, laat staan een kleinste, maar wel een infimum, namelijk r.
2. De verzameling $Q_r^- = \{q \in \mathbb{Q} \mid q \leqslant r\}$ heeft iedere $y \geqslant r$ als bovengrens en r als kleinste bovengrens. Deze laatste ligt in Q_r^-. Er is deze keer geen ondergrens.
3. Ook de verzameling $Q_r = \{q \in \mathbb{Q} \mid q < r\}$ met $r \in \mathbb{Q}$ heeft r als kleinste bovengrens, maar deze laatste ligt nu niet in Q_r (en Q_r heeft geen ondergrens).
4. De verzameling $Q_{\sqrt{2}} = \{q \in \mathbb{Q} \mid (q < 0) \vee (q^2 < 2)\}$ heeft geen ondergrens en iedere $y \in \mathbb{Q}$ met $y^2 > 2$ als bovengrens, maar heeft geen *kleinste* bovengrens.

Deze kleinste bovengrens van $Q_{\sqrt{2}}$ in $\mathbb{Q}$ zou $\sqrt{2}$ moeten zijn, maar dat is volgens Stelling 5.10 geen breuk. $\mathbb{Q}$ heeft dus niet-lege deelverzamelingen die wel een bovengrens hebben maar geen *kleinste* bovengrens (in $\mathbb{Q}$). We gaan dit gebrek nu verhelpen.[13]

Definitie 5.11 *Een* **Dedekind ondersnede** *van $\mathbb{Q}$ is een deelverzameling $Q \subset \mathbb{Q}$ zodat*

$$Q \neq \emptyset \text{ en } Q \neq \mathbb{Q}; \tag{5.65}$$
$$\forall_{p\in\mathbb{Q}} \forall_{q\in Q} (p < q \to p \in Q); \tag{5.66}$$
$$\forall_{p\in Q} \exists_{q\in Q} (q > p). \tag{5.67}$$

De **reële getallen** *zijn de volgende deelverzameling $\mathbb{R} \subset P(\mathbb{Q})$:*

$$\mathbb{R} := \{Q \subset \mathbb{Q} \mid Q \text{ is een Dedekind ondersnede van } \mathbb{Q}\}. \tag{5.68}$$

12. Dit kan met volledige inductie worden bewezen, zie §5.2. Voor $p = 1$ is de claim waar. Stel de claim is waar voor vaste oneven p. Dan is $(p + 2)^2 = p^2 + 2p + 4$ de som van het getal p^2 dat volgens de inductiehypothese oneven is, en het even getal $2p + 4 = 2(p + 2)$. Daarmee is $(p + 2)^2$ oneven. Volgens het principe van volledige inductie, oftewel axioma **PA7**, geldt de claim dan voor iedere oneven p.

13. Deze definitie werd oorspronkelijk gegeven door middel van ***Dedekind sneden*** van $\mathbb{Q}$: dit zijn partities $\{Q, R\} \subset P(\mathbb{Q})$, bestaande uit twee niet-lege deelverzamelingen $Q \subset \mathbb{Q}$ en $R \subset \mathbb{Q}$, die naast $Q \cap R = \emptyset$ en $Q \cup R = \mathbb{Q}$ voldoen aan $Q < R$ (voor alle $q \in Q$ en $r \in R$ geldt $q < r$) en aan (5.67). Hieruit volgt dat Q een Dedekind ondersnede van $\mathbb{Q}$ is desda $\{Q, R = \mathbb{Q} \setminus Q\}$ een Dedekind snede van $\mathbb{Q}$ is.

Reële getallen zijn dus gedefineerd als speciale deelverzamelingen van $\mathbb{Q}$! Daarmee is een reëel getal zelf een verzameling, zoals ieder wiskundig object! Ook π! Conditie (5.66) houdt in dat Q alsmaar naar links (d.w.z. in de richting van kleiner worden getallen) doorloopt. Conditie (5.67) betekent dat Q geen bovengrens *in* $\mathbb{Q}$ heeft. Er zijn twee kwalitatief verschillende Dedekind ondersneden, namelijk Q_r met $r \in \mathbb{Q}$, en bijvoorbeeld $Q_{\sqrt{2}}$: de eerste heeft een kleinste bovengrens *in* $\mathbb{Q}$ (nl. r) en de tweede niet. Zo zijn er twee fundamenteel verschillende soorten reële getallen: als $Q = Q_r$ voor $r \in \mathbb{Q}$, dan "is" Q in feite het rationale getal $r \in \mathbb{Q}$, en daarmee hebben we een injectie $\mathbb{Q} \hookrightarrow \mathbb{R}$, nl. $r \mapsto Q_r$. Aan (5.67) is voldaan omdat voor alle breuken $p < r$ er een $q \in \mathbb{Q}$ is met $p < q < r$ (bewijs zelf). Als $Q \neq Q_r$ voor $r \in \mathbb{Q}$, dan is Q een *irrationaal* getal.

We definiëren nu een partiële ordening op $\mathbb{R}$. Omdat per definitie $\mathbb{R} \subset P(\mathbb{Q})$ kunnen we de canonieke ordening op $P(Z)$ uit Stelling 3.7 met $Z = \mathbb{Q}$ beperken tot $\mathbb{R}$:

Definitie 5.12 *Voor (Dedekind ondersneden)* $Q, R \in \mathbb{R}$ *geldt* $Q \leqslant R$ *desda* $Q \subset R$.

Je ziet direct dat als $r, s \in \mathbb{Q}$ met $r \leqslant s$, dan $Q_r \subset Q_s$ en dus per definitie $Q_r \leqslant Q_s$. Als we net als boven $\mathbb{Q}$ als een deelverzameling van $\mathbb{R}$ opvatten via $r \mapsto Q_r$, breidt de ordening op $\mathbb{R}$ de al bekende ordening op $\mathbb{Q}$ dus uit (preciezer: als $\iota(r) := Q_r$ voor $r \in \mathbb{Q}$, dan geldt $r \leqslant s \Rightarrow \iota(r) \leqslant \iota(s)$). Bovendien is de partiële ordening op $\mathbb{R}$ net als op $\mathbb{Q}$ totaal (opgave). We kunnen ook uitdrukken dat $Q \geqslant 0$: dit betekent $Q_0 \subset Q$.

Stelling 5.13 *De (totaal) geordende verzameling* $\mathbb{R}$ *is* **volledig***: iedere niet-lege deelverzameling* $S \subset \mathbb{R}$ *met een bovengrens heeft ook een* kleinste *bovengrens, namelijk*

$$\sup S = \cup S. \tag{5.69}$$

Bewijs. We gaan eerst na dat $\cup S \in \mathbb{R}$ als $S \subset \mathbb{R}$. Volgens Definitie 5.11 moet dus gelden:

1. $\cup S \neq \emptyset$. Iedere $Q \in S$ is (als deelverzameling van $\mathbb{Q}$) niet leeg (want $Q \in \mathbb{R}$), dus stel $q \in Q$. Dan is ook $q \in \cup S$ en is $\cup S$ dus niet leeg.
2. $\cup S \neq \mathbb{Q}$. Als $R \in \mathbb{R}$ een bovengrens van S is geldt $Q \subset R$ voor alle $Q \in S$. Omdat $Q \in \mathbb{R}$ is er een $q \in \mathbb{Q}$ zodat $q \notin Q$. Dus $q \notin Q$ voor alle $Q \in S$ en dus $q \notin \cup S$.
3. $\forall_{p \in \mathbb{Q}} \forall_{q \in \cup S} (p < q \to p \in \cup S)$. We hebben $q \in Q$ voor zekere $Q \in S$, i.h.b. $Q \in \mathbb{R}$, en daarvoor geldt de eis (5.66), zodat $p \in Q$ en daarmee ook $p \in \cup S$.
4. $\forall_{p \in \cup S} \exists_{q \in \cup S}\, p < q$. Gaat bijna hetzelfde als de vorige stap (opgave).

Ten slotte is het bewijs dat $\cup S$ een bovengrens is voor S, en vervolgens dat het de kleinste bovengrens is, is vrijwel hetzelfde als in Stelling 3.7. Q.E.D.

In §5.6 definiëren we optelling en vermenigvuldiging in $\mathbb{R}$ zodat aan de eigenschappen **R1** t/m **R10** voldaan is. Ten opzichte van $\leqslant$ gelden dan de eigenschappen:

1. $x \leqslant y \Rightarrow x + z \leqslant y + z$, voor alle x, y, z (de ordening is *lineair*);
2. $0 \leqslant x$ en $0 \leqslant y \Rightarrow 0 \leqslant x \cdot y$, voor alle x, y, z (de ordening is *mulitplicatief*).[14]

14. Een lichaam met lineaire en mulitplicatieve partiële ordening heet een ***partieel geordend lichaam***.

5.6 De reële getallen $\mathbb{R}$: Decimale expansies

We geven nu een handige *notatie* voor reële getallen, die al gedefinieerd zijn in de vorige sectie. Deze notatie lost het probleem op dat de constructie van $\mathbb{R}$ volgens Dedekind weliswaar als voordeel heeft dat de volledigheid van $\mathbb{R}$ er mooi uitrolt, maar als nadeel dat optellen en vermenigvuldigen vreselijk is en de constructie bovendien niet aansluit bij je intuïtie over reële getallen. Maar Definitie 5.11 was niet voor niets!

Definitie 5.14 *Een* **decimale expansie** *is een eindige of oneindige rij getallen* $x_0.x_1x_2\cdots$, *met* $x_0 \in \mathbb{N}$ *en* $x_k \in \{0,1,\ldots,9\}$ *voor* $k > 0$, *met uiteindelijk niet alle* $x_k = 9$. *Iets formeler: iedere functie* $x : \mathbb{N} \to \mathbb{N}$ *met* $x_k := x(k) \in \{0,1,\ldots,9\}$ *voor alle* $k > 0$ *(met de gegeven beperking op negens als waarde) definieert een decimale expansie.*[15]

We identificeren nu ieder eindig stuk $x_{|N} = x_0.x_1x_2\cdots x_N$ met een element van $\mathbb{Q}$ via

$$\begin{aligned} x_{|N} = x_0.x_1\cdots x_N &:= \sum_{k=0}^{N} x_k \cdot 10^{-k} = \frac{x_0}{10^0} + \frac{x_1}{10^1} + \cdots + \frac{x_k}{10^k} + \cdots \frac{x_N}{10^N} \\ &= \frac{10^N x_0 + 10^{N-1}x_1 + \cdots + 10^{N-k}x_k + \cdots + 10^0 x_N}{10^N} \end{aligned} \tag{5.70}$$

met $x_{|0} := x_0$, en daarmee met een element $Q_{x_{|N}}$ van $\mathbb{R}$ (in de vorige constructie volgens Dedekind). De deelverzameling $S = \{Q_{x_{|0}}, Q_{x_{|1}}, Q_{x_{|2}}, \ldots\}$ van $\mathbb{R}$ heeft een bovengrens, bijvoorbeeld Q_{x_0+1} (immers $\sum_{k=0}^{N} x_k \cdot 10^{-k} < x_0 + 1$ in $\mathbb{Q}$ voor alle N). Volgens Stelling 5.13 heeft S dus ook een *kleinste* bovengrens (5.69), en dit element van $\mathbb{R}$ is per definitie

$$x = x_0.x_1x_2\cdots := \sup\{Q_{x_{|0}}, Q_{x_{|1}}, Q_{x_{|2}}, \ldots\} = \{q \in \mathbb{Q} \mid \exists_{N\in\mathbb{N}}\,(q < x_{|N})\}, \tag{5.71}$$

waarbij $x_{|N}$ is gedefinieerd door (5.70); de laatste gelijkheid in (5.71) is instructief maar niet belangrijk voor het vervolg; je kunt als opgave nagaan dat de verzameling helemaal rechts een Dedekind ondersnede is en gelijk is aan het supremum in het midden. Hiermee is een decimale notatie ingevoerd voor alle positieve reële getallen van de vorm (5.71). Dat je *alle* positieve reële getallen op die manier krijgt volgt uit:

Stelling 5.15 *Ieder positief reëel getal* $x \in \mathbb{R}$ *heeft een unieke decimale expansie* $x = x_0.x_1x_2\cdots$, *waarin de getallen* $x_0 \in \mathbb{N}$ *en* $x_k \in 10$ *voor* $k > 0$ *recursief zijn bepaald door*

$$x_0 = \max\{N \in \mathbb{N} \mid N \leqslant x\}; \tag{5.72}$$
$$x_1 = \max\{N \in \{0,1,\ldots,9\} \mid N \leqslant 10\cdot(x - x_0)\}; \tag{5.73}$$
$$x_2 = \max\{N \in \{0,1,\ldots,9\} \mid N \leqslant 10^2\cdot(x - x_0.x_1)\}; \tag{5.74}$$
$$\cdots \tag{5.75}$$
$$x_n = \max\{N \in \{0,1,\ldots,9\} \mid N \leqslant 10^n\cdot(x - x_0.x_1\cdots x_{n-1})\}, \tag{5.76}$$

waarbij in de definitie van x_n *alle eerdere* x_k, $k < n$, *bepaald zijn in de vorige stappen.*

$\mathbb{Q}$ en $\mathbb{R}$ zijn zelfs *totaal geordende lichamen*. Maar slechts $\mathbb{R}$ is een *volledig totaal geordend lichaam*. Als zodanig is het zelfs uniek "op isomorfisme na", zoals Hilbert in 1900 bewees: ieder volledig totaal geordend lichaam is een "kopie" van $\mathbb{R}$ uit Definitie 5.11. Stelling 5.15 is hier een voorbeeld van.

In deze stelling is x een element van het Dedekind-model van $\mathbb{R}$, waarin we optellen en aftrekken niet hebben gedefinieerd, zodat we helaas geen bewijs kunnen geven. Wat je wel kunt doen is aannemen dat x al in decimale expansie gegeven is en nagaan dat je de getallen x_k waar je mee begon via (5.72) t/m (5.76) ook weer terugkrijgt. Ga tevens na dat $x_k \in \{0, 1, \ldots, 9\}$ voor $k > 0$, aangezien een grotere waarde tot tegenspraak met de vorige stap zou leiden, en dat voor iedere $m \in \mathbb{N}$ een $k > m$ bestaat met $x_k \neq 9$.
We hebben het tot nu toe alleen over *positieve* reële getallen gehad; de negatieve kunnen uit de positieve worden gemaakt door er een min-teken voor te zetten.[16]

In het Duits zegt men: "*Der Mohr hat seine Arbeit getan, der Mohr kann gehen.*"[17] Nu het Dedekind-model van $\mathbb{R}$ zijn werk heeft gedaan via Stelling 5.13 en als illustratie van het idee dat de reële getallen binnen de verzamelingenleer kunnen worden gedefinieerd (hetgeen uit decimale expansies allerminst duidelijk is) kan het gaan. Je denken over reële getallen kan verder plaatsvinden rond decimale expansies, zolang je maar onthoudt dat Stelling 5.13 daar ook voor geldt, echter met formule (5.69) vervangen door de limiet, zoals zal worden gedefinieerd in het college Analyse 1. De partiële (en zelfs totale) ordening $\leqslant$ is nu, met $x = x_0.x_1x_2\cdots$ en $y = y_0.y_1y_2\cdots$, gedefinieerd door

$x \leqslant y$ desda $x_0 < y_0$, of $x_0 = y_0$ en $x_1 < y_1$, of $x_0 = y_0$ en $x_1 = y_1$ en $x_2 < y_2$, enz.

Als $x < y$ volgt dat na eindig veel verificaties, maar voor $x = y$ zijn er oneindig veel nodig! Optelling $x + y$ en vermenigvuldiging $x \times y$ worden eerst volgens de gebruikelijke regels in $\mathbb{Q}$ op alle eindige segmenten $x_{|N}$ en $y_{|N}$ van x en y uitgevoerd, waarna in het geval dat $x \geqslant 0$ en $y \geqslant 0$ het supremum over N in $\mathbb{R}$ wordt genomen (bedenk zelf hoe de andere drie gevallen gaan, via gevalsonderscheidingen en mintekens).[18]

Het decimale model geeft ook een mooi bewijs van het volgende resultaat van Cantor:

Stelling 5.16 *De verzameling $\mathbb{R}$ is overaftelbaar.*

Bewijs. We beschrijven iedere $x \in \mathbb{R}$ via zijn decimale expansie (5.71). Stel, als bewijs uit het ongerijmde, nu dat $\mathbb{R}$ aftelbaar is. Dan is er een bijectie $F : \mathbb{N} \to \mathbb{R}$ en krijgen we een opsomming $(x(0), x(1), \ldots)$ van alle $x \in \mathbb{R}$, met $x(n) := F(n)$:

$$\begin{array}{lcccccc} x(0) & = & x(0)_0. & x(0)_1 & x(0)_2 & x(0)_3 & \ldots \\ x(1) & = & x(1)_0. & x(1)_1 & x(1)_2 & x(1)_3 & \ldots \\ x(2) & = & x(2)_0. & x(2)_1 & x(2)_2 & x(2)_3 & \ldots \\ x(3) & = & x(3)_0. & x(3)_1 & x(3)_2 & x(3)_3 & \ldots \end{array}$$

16. In het Dedekind-model is $Q \geqslant 0$ gedefinieerd door $Q_0 \subset Q$, evenzo $Q \leqslant 0$ door $Q \subset Q_0$, met $Q_0 = \{q \in \mathbb{Q} \mid q < 0\}$. Als $Q \leqslant 0$ definieer je $-Q = \{q \in \mathbb{Q} \mid \exists_{p \in \mathbb{Q}}\, (p > 0) \wedge (-q - p \notin Q)\}$ en past daarop de constructies boven toe. Test: als $Q = Q_r$ met $r \in \mathbb{Q}$, dan is $-q - p \notin Q$ hetzelfde als $-p - q > r$, d.w.z. $p + q < -r$, dus $\exists_{p \in \mathbb{Q}_r}\, (p > 0) \wedge (-q - p \notin Q)$ is $q \leqslant -r$, zodat met $r < 0$ volgt dat $-Q_r = Q_{-r}$.
17. F. Schiller, *Die Verschwörung des Fiesco zu Genua*, 1782. 3. Akt, 4. Auftritt, Andrea Doria.
18. Voorbeeld: als $y < 0$ en $x < -y$, dan is $x + y = -(-y - x)$, met $-y - x > 0$ via een supremum.

Nu construeren we via een voorbeeld van een "diagonaalargument" à la Cantor een getal y dat niet op deze lijst voorkomt, namelijk het getal met decimale expansie

$$y_k = x(k)_k + 1 \tag{5.77}$$

voor $k > 0$ modulo 10, dus als $x(k)_k = 9$, dan is $x(k)_k + 1 = 0$. Als y op de lijst staat, i.,e. in het beeld ligt van de bijectie F, is er een $n \in \mathbb{N}$ met $y = x(n)$ en dus $y_k = x(n)_k$ voor alle $k \in \mathbb{N}$. En dus ook voor $k = n$, zodat $y_n = x(n)_n$. Maar we hadden per definitie van y dat $y_n = x(n)_n + 1$, tegenspraak! Q.E.D.

Stelling 5.16 is hoogst opmerkelijk, omdat wel geldt

$$\mathbb{Z} \cong \mathbb{N}; \tag{5.78}$$

$$\mathbb{Q} \cong \mathbb{N}. \tag{5.79}$$

De eerste volgt uit de definitie (5.39) en (5.42), waaruit volgt:[19]

$$\mathbb{Z} \cong S = \mathbb{N} \cup \mathbb{N}_* \subset \mathbb{N} \times \mathbb{N} \cong \mathbb{N}, \tag{5.80}$$

zodat $\mathbb{Z} \leqslant \mathbb{N}$, maar ook weten we dat $\mathbb{N} \leqslant \mathbb{Z}$ via de injectie $n \mapsto [n, 0]$, zodat (5.78) volgt uit Stelling 4.10. Het bewijs van (5.79) berust op (5.51), (5.78), (4.15), en opnieuw het kiezen van $\mathbb{Q} \cong S \subset \mathbb{Z} \times \mathbb{Z}$, waaruit volgt dat $\mathbb{Q} \leqslant \mathbb{Z} \times \mathbb{Z}$. Net als in (4.15) geldt

$$\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}, \tag{5.81}$$

zodat $\mathbb{Q} \leqslant \mathbb{Z}$ en daarmee $\mathbb{Q} \leqslant \mathbb{N}$ vanwege (5.78). Omdat we een injectie $\mathbb{Z} \hookrightarrow \mathbb{Q}$ hebben geldt ook $\mathbb{Z} \leqslant \mathbb{Q}$ en daarmee $\mathbb{N} \leqslant \mathbb{Q}$. Stelling 4.10 geeft dan (5.79).[20]

Met iets meer moeite kunnen we Stelling 5.16 aanscherpen tot het concrete resultaat

$$\mathbb{R} \cong P(\mathbb{N}). \tag{5.82}$$

Omdat iedere functie $f : \mathbb{N} \to 2$ een reëel getal $f(0).f(1)f(2)\cdots$ geeft, levert de constructie van $\mathbb{R}$ via decimale expansies een injectie $2^{\mathbb{N}} \hookrightarrow \mathbb{R}$, zodat $2^{\mathbb{N}} \leqslant \mathbb{R}$. Stelling 4.12 geeft een bijectie $P(\mathbb{N}) \cong 2^{\mathbb{N}}$, en dus $P(\mathbb{N}) \leqslant \mathbb{R}$. De constructie van $\mathbb{R}$ volgens Dedekind geeft een injectie $\mathbb{R} \hookrightarrow P(\mathbb{Q})$, zodat $\mathbb{R} \leqslant P(\mathbb{Q})$. Vgl. (5.79) geeft tevens een bijectie

$$P(\mathbb{Q}) \cong P(\mathbb{N}), \tag{5.83}$$

zie opgave, zodat $\mathbb{R} \leqslant P(\mathbb{N})$. Alweer Stelling 4.10 geeft (5.82).[21] Q.E.D.

19. Altijd geldt $X/\sim \leqslant X$; dit volgt uit het keuzeaxioma, dat een injectie $s : X/\sim \to X$ geeft, zie §4.6.
20. In deze bewijzen gebruiken we herhaaldelijk dat $\cong$ zich gedraagt als een equivalentierelatie op alle verzamelingen, zie §4.2, zodat $A \cong A$, $(A \cong B) \wedge (B \cong C) \to A \cong C$, en $A \cong B \leftrightarrow B \cong A$. Ook is $\leqslant$ 'bijna' een partiële ordening: er geldt $A \leqslant A$, $(A \leqslant B) \wedge (B \leqslant C) \to A \leqslant C$, en $(A \leqslant B) \wedge (B \leqslant A) \to A \cong B$ (maar dus niet: $\to A = B$). Zie Velleman, Theorems 8.1.5 en 8.1.6 voor een alternatief bewijs van (5.79). Voor een expliciete bijectie $\mathbb{N} \to \mathbb{Q}$, zie `http://oeis.org/A002487` (met dank aan Jelmer Firet).
21. Cantor vroeg zich al af of er verzamelingen X bestaan zodat $\mathbb{N} < X < P(\mathbb{N})$, oftewel $\mathbb{N} < X < \mathbb{R}$. Het vermoeden dat dit *niet* zo is heet de *Continuüm Hypothese*. Deze blijkt binnen **ZF** onbeslisbaar.

5.7 De complexe getallen $\mathbb{C}$

Met de invoering van de complexe getallen $\mathbb{C}$ voltooien we de stijgende rij (5.1).

Definitie 5.17 *Als verzameling zijn de complexe getallen gegeven door*

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}. \tag{5.84}$$

Op deze verzameling definiëren we een optelling en een vermenigvuldiging door

$$\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle; \tag{5.85}$$
$$\langle a, b\rangle \times \langle c, d\rangle = \langle ac - bd, ad + bc\rangle. \tag{5.86}$$

Het getal $i \in \mathbb{C}$ *is gedefinieerd door* $i = \langle 0, 1\rangle$ *en we schrijven*

$$a + bi := \langle a, b\rangle. \tag{5.87}$$

Het heeft lang geduurd voor deze definitie werd gevonden.[22] De regel $i^2 = -1$ volgt direct uit (5.86) en als we dit eenmaal weten volgt (5.86) daar ook weer uit, in de vorm

$$(a + bi) \times (c + di) = (ac - bd) + (ad + bc)i. \tag{5.88}$$

De meetkundige interpretatie van complexe getallen als punten in het vlak volgt direct uit de definitie. We hebben een injectie $\iota : \mathbb{R} \hookrightarrow \mathbb{C}$ gegeven door $\iota(a) = \langle a, 0\rangle$, met

$$\iota(a + b) = \iota(a) + \iota(b); \tag{5.89}$$
$$\iota(a \times b) = \iota(a) \times \iota(b). \tag{5.90}$$

Uit Definitie 5.17, Stelling 5.16, (5.82), en $\mathbb{R} \times \mathbb{R} \cong \mathbb{R}$ (opgave) volgt, net als in (5.82),

$$\mathbb{C} \cong \mathrm{P}(\mathbb{N}). \tag{5.91}$$

Stelling 5.18 *De complexe getallen vormen een lichaam onder* (5.85) *en* (5.86).

Bewijs dit zelf. Het neutrale element voor optelling is $\langle 0, 0\rangle$, dat voor vermenigvuldiging is $\langle 1, 0\rangle$, en de inverse van $\langle a, b\rangle \neq \langle 0, 0\rangle$ onder vermenigvuldiging is

$$(a + bi)^{-1} := \langle a, b\rangle^{-1} = \left\langle \frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right\rangle =: \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} \cdot i. \tag{5.92}$$

Er bestaat geen totale lineaire en multiplicatieve ordening van $\mathbb{C}$, maar er is wel een goed afstandsbegrip, via (5.84) gegeven door eerst de bekende absolute waarde

$$|a + bi| = \sqrt{a^2 + b^2}, \tag{5.93}$$

en dan de afstand (of metriek) $d(w, z) = |z - w|$, met $w, z \in \mathbb{C}$. In afwezigheid van een geschikte partiële ordening is het begrip volledigheid nu anders gedefinieerd dan boven voor $\mathbb{R}$, namelijk via het feit dat iedere Cauchy-rij in $\mathbb{C}$ (ten opzichte van deze metriek) convergeert. Zie Analyse 1. In die zin is $\mathbb{C}$ net als $\mathbb{R}$ een volledig lichaam.

22. Complexe of imaginaire getallen werden voor het eerst in de 16e eeuw in Italië gebruikt in de oplossing van kwadratische en kubische vergelijkingen en heetten toen *quantitates impossibiles*. Isaac Newton (1642–1727) vermeed ze nog. De eerste die er niet meer van schrok was Carl Friedrich Gauss (1777–1855) en de bovenstaande definitie is afkomstig van William Rowan Hamilton (1805–1865).

5.8 Opgaven bij hoofdstuk 5

Zie ook de exercises in Velleman, §8.2, en over inductie in §§6.1 t/m 6.4.

Opgave 5.1

Bewijs uit de (Dedekind–)Peano-axioma's **PA1** t/m **PA6** dat $\vdash 1 \times 1 = 1$.

Opgave 5.2

Bewijs uit de Peano-axioma's **PA1** t/m **PA4** en desgewenst ook hun gevolgen **R1** t/m **R3** dat $\vdash 2 + 2 = 4$.

Opgave 5.3

Bewijs met volledige inductie dat voor alle $n \in \mathbb{N}$ geldt dat

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

Opgave 5.4

Bewijs met volledige inductie dat voor elke $n \in \mathbb{N}$ en elke $r \neq 1$ geldt dat

$$1 + r + r^2 + \cdots + r^n =: \sum_{k=0}^{n} r^k = \frac{r^{n+1} - 1}{r - 1}.$$

Dit is de ***meetkundige reeks***.

Opgave 5.5

Bewijs de volgende twee varianten van het inductieprincipe vanuit de oorspronkelijke formulering (d.w.z.: uit $F(0)$ en $\forall_{n\in\mathbb{N}}(F(n) \to F(n+1))$ volgt $\forall_{n\in\mathbb{N}}F(n)$):

- Voor alle $m \in \mathbb{N}$: uit $F(m)$ en $\forall_{n\geqslant m}(F(n) \to F(n+1))$ volgt $\forall_{n\geqslant m}F(n)$,
- Uit $\forall_{n\in\mathbb{N}}((\forall_{m<n}F(m)) \to F(n))$ volgt $\forall_{n\in\mathbb{N}}\, F(n)$.

Opgave 5.6

a) Bewijs direct (niet als speciaal geval van (5.26)) dat $\sum_{k=0}^{n}\binom{n}{k} = 2^n$, $\forall n \geqslant 1$.
b) Bewijs dat $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$ voor alle $n \geqslant 1$.

Opgave 5.7

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***:

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

Opgave 5.8

Een functie $f : \mathbb{N}^n \to \mathbb{N}$ heet ***primitief recursief*** als hij verkregen kan worden uit de volgende basisfuncties door eindig veel toepassingen van het schema van primitieve recursie (Stelling 5.6) en het samenstellen van de volgende functies:

- de constante 0 (opgevat als functie $f(x_1, \ldots, x_n) = 0$, voor willekeurige n);
- de opvolgerfunctie $S(x) = x + 1$,
- de projectiefuncties $\mathscr{P}_i^n : \mathbb{N}^n \to \mathbb{N}$ gedefinieerd door $\mathscr{P}_i^n(x_1, \ldots, x_n) = x_i$;
- alle functies die zo door samenstelling verkregen kunnen worden (iteratie).

Bewijs dat de volgende functies primitief recursief zijn:

a) $f(x_1, \ldots, x_n) = k$ (voor een vaste $k \in \mathbb{N}$);
b) $f(x_1, x_2) = x_1 + x_2$ (nu al functie van *beide* variabelen);
c) $f(x_1, x_2) = x_1 \times x_2$ (*idem dito*);
d) $f(x_1, x_2) = x_1^{x_2}$ (*idem dito*).

Opgave 5.9

Ga na dat de relatie in (5.38) een equivalentierelatie is.

Opgave 5.10

Ga na dat de relatie in (5.50) een equivalentierelatie is. Ga ook na dat de operaties in (5.52) welgedefinieerd zijn.

Opgave 5.11

Bewijs Stelling 5.9.

Opgave 5.12

Laat zien dat $Q = \{q \in \mathbb{Q} \mid (q < 0) \vee (q^2 < 2)\}$ een ondersnede is (i.h.b. dat voldaan is aan (5.67)).

Opgave 5.13

Ga na dat Definitie 5.12 een totale ordening op $\mathbb{R}$ geeft en dat $r \leqslant s \Rightarrow Q_r \leqslant Q_s$.

Opgave 5.14

Bewijs de = in (5.71), d.w.z. $\cup\{Q_{x_{|0}}, Q_{x_{|1}}, Q_{x_{|2}}, \ldots\} = \{q \in \mathbb{Q} \mid \exists_{N \in \mathbb{N}}\,(q < x_{|N})\}$.

Opgave 5.15

Bewijs dat $\mathbb{R} \times \mathbb{R} \cong \mathbb{R}$ (zie exercise 12 in §8.3 van Velleman).

Opgave 5.16

Laat zien dat uit $X \cong Y$ volgt dat $P(X) \cong P(Y)$.

Opgave 5.17

Ga na dat $\langle a, b\rangle \times \langle a, b\rangle^{-1} = \langle 1, 0\rangle$, zie (5.88) en (5.92).

Bewijsregels:

1. $\dfrac{A}{A}$ (*herhaling*)

2. $\dfrac{\begin{array}{c}[\neg A]\\ \cdots\\ \cdots\\ \bot\end{array}}{A}$ (*RAA = Reductio Ad Absurdum*)

3. $\dfrac{A \qquad A \to B}{B}$ ($\to$*-Eliminatie = Modus Ponens*)

4. $\dfrac{\begin{array}{c}[A]\\ \cdots\\ \cdots\\ B\end{array}}{A \to B}$ ($\to$*-Introductie*)

5. $\dfrac{\neg A}{A \to \bot}$ ($\neg$*-Eliminatie =* $\bot$*-Introductie*)

6. $\dfrac{A \to \bot}{\neg A}$ ($\neg$*-Introductie =* $\bot$*-Eliminatie*)

7. $\dfrac{A \wedge B}{A}$ en $\dfrac{A \wedge B}{B}$ ($\wedge$*-Eliminatie*)

8. $\dfrac{A \quad B}{A \wedge B}$ ($\wedge$*-Introductie*)

9. $\dfrac{A \vee B \quad A \to C \quad B \to C}{C}$ ($\vee$*-Eliminatie*)

10. $\dfrac{A}{A \vee B}$ en $\dfrac{B}{A \vee B}$ ($\vee$*-Introductie*)

11. $\dfrac{F(x)}{\forall_x F(x)}$ (∀-Introductie); 12. $\dfrac{\forall_x F(x)}{F(t)}$ (∀-*Eliminatie*);

13. $\dfrac{F(t)}{\exists_x F(x)}$ (∃-*Introductie*); 14. $\dfrac{F(x) \to G \qquad \exists_x F(x)}{G}$ (∃-*Eliminatie*).

15. $\dfrac{\cdots}{x = x}$ $\qquad \dfrac{x = y \qquad y = z}{x = z}$ $\qquad \dfrac{x = y}{y = x}$

16. $\dfrac{F(x_1, \ldots x_n) \qquad x_1 = y_1 \ldots x_n = y_n}{F(y_1, \ldots, y_n)}$ 17. $\dfrac{x_1 = y_1 \ldots x_n = y_n}{t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)}$

Afgeleide regels:

A. $\dfrac{\bot}{A}$ B. $\dfrac{A \to B \qquad B \to C}{A \to C}$ C. $\dfrac{\neg B \qquad A \to B}{\neg A}$ D. $\dfrac{\neg B \to \neg A}{A \to B}$

E. $\dfrac{A \vee B \qquad \neg A}{B}$ F. $\dfrac{A \quad \neg A}{\bot}$ G. $\dfrac{\neg\neg A}{A}$ H. $\dfrac{A \leftrightarrow B \qquad B \leftrightarrow C}{A \leftrightarrow C}$

I. $\dfrac{\forall_x F(x)}{\forall_y F(y)}$ J. $\dfrac{\exists_x F(x)}{\exists_y F(y)}$

K. $\dfrac{\forall_x \forall_y F(x, y)}{\forall_y \forall_x F(x, y)}$ L. $\dfrac{\exists_x \exists_y F(x, y)}{\exists_y \exists_x F(x, y)}$

M. $\dfrac{\forall_x (F(x) \wedge G(x))}{(\forall_x F(x)) \wedge (\forall_y G(y))}$ N. $\dfrac{(\forall_x F(x)) \wedge (\forall_y G(y))}{\forall_x (F(x) \wedge G(x))}$

O. $\dfrac{\forall_x (F(x) \to G(x))}{(\forall_x F(x)) \to (\forall_y G(y))}$ P. $\dfrac{\forall_x (F(x) \leftrightarrow G(x))}{(\forall_x F(x)) \leftrightarrow (\forall_y G(y))}$

Q. $\dfrac{(\forall_x F(x)) \vee (\forall_y G(y))}{\forall_x (F(x) \vee G(x))}$ R. $\dfrac{(\exists_x F(x)) \to (\forall_y G(y))}{\forall_x (F(x) \to G(x))}$

S. $\dfrac{\forall_x (F(x) \to G(x))}{(\exists_x F(x)) \to (\exists_y G(y))}$ T. $\dfrac{\exists_x (F(x) \vee G(x))}{(\exists_x F(x)) \vee (\exists_y G(y))}$