Beschrijven en Bewijzen

Beschrijven en Bewijzen

H. Zantema en P.W.H. Lemmens

Delft University Press / 1999

Uitgegeven door:

Delft University Press
Postbus 98
2600MG DELFT
tel. 015–2783254
fax 015–2781661

in opdracht van:

Universiteit Utrecht
Informatica Instituut
Postbus 80089
3508TB UTRECHT
tel. 030–2531454
fax 030–2513791

ISBN: 90–407–1942–X

Printed in the Netherlands

Voorwoord

Dit is de tekst die gebruikt wordt als materiaal bij het vak *Beschrijven en Bewijzen* in de opleiding Informatica aan de Universteit Utrecht. Een groot deel hiervan is gebaseerd op delen van het collegedictaat *Inleiding Logica en Discrete Structuren* zoals dat in de jaren 80 door de tweede auteur is ontwikkeld; de afgelopen jaren is de tekst aanzienlijk uitgebreid en aangepast door de eerste auteur.

In de meest uiteenlopende facetten van de informatica is het wenselijk of noodzakelijk de gemaakte claims objectief en gedegen te onderbouwen, niet in de laatste plaats om anderen van de geldigheid ervan te kunnen overtuigen. Voor het geven van een onderbouwing van de geldigheid van een bewering is een heel scala van wiskundige bewijstechnieken en redeneervormen beschikbaar: *bewijzen*. Alvorens deze technieken toepasbaar te maken en op een uniforme wijze over de problemen te kunnen communiceren, is het in het algemeen noodzakelijk het onderhavige probleem in een formeel raamwerk te modelleren: *beschrijven*. Deze tekst is er op gericht te oefenen in dit modelleren, en vaardigheden op te doen in het toepassen van bewijstechnieken waarbij onderweg een stuk wiskundig begrippenapparaat wordt eigen gemaakt. In wat meer klassieke terminologie zou het ook *Logica en Verzamelingenleer* hebben kunnen heten, waarbij dan wel de nadruk niet alleen op de begrippen zelf ligt, maar vooral op het omgaan met dergelijke precies gedefinieerde begrippen.

Inhoudsopgave

1 Waarom iets bewijzen? 9

1.1 Bewijzen uit het ongerijmde . . . 11
1.2 Bewijzen met gevalsonderscheid . . . 13
1.3 Bewijzen met inductie . . . 14
1.4 Bewijzen met invarianten . . . 14
1.5 Nog wat terminologie . . . 21

2 Proposities 23

2.1 Samenstellen van proposities . . . 25
2.2 Waarheidstafels . . . 26
2.3 Tautologieën . . . 29
2.4 Gelijkwaardige proposities . . . 31
2.5 Speciale vormen . . . 32
2.6 Opgaven . . . 34

3 Bewijzen met deductie 37

3.1 Afleidingsregels . . . 39
3.2 Subbewijzen en hulpstellingen . . . 42
3.3 Opgaven . . . 44

4 Predicaten 45

4.1 Vrij en gebonden, universum . . . 46
4.2 Gelijkwaardige predicaten . . . 49
4.3 Substitutie . . . 52
4.4 Afleidingsregels . . . 53
4.5 Opgaven . . . 56

5 Verzamelingen 59

5.1 Operatoren op verzamelingen . . . 61
5.2 Machtsverzameling en cartesisch product . . . 67
5.3 Vereniging en doorsnede over een indexverzameling . . . 68
5.4 Opgaven . . . 71

6 Afbeeldingen **75**
6.1 Injectieve, surjectieve en bijectieve afbeeldingen . . . 78
6.2 Enkele speciale afbeeldingen . . . 81
6.3 Afbeeldigen op eindige verzamelingen . . . 81
6.4 Samenstellen van afbeeldingen . . . 83
6.5 Inverse afbeeldingen en dekpunten . . . 86
6.6 Opgaven . . . 88

7 Volledige inductie **93**
7.1 Inductieve definities . . . 100
7.2 Binomiaalcoëfficiënten . . . 104
7.3 Opgaven . . . 107

8 Relaties en grafen **109**
8.1 Relaties . . . 109
8.2 Grafen . . . 111
8.3 Equivalentierelaties en partities . . . 115
8.4 Opgaven . . . 122

9 Ordeningen **125**
9.1 Maxima en minima, boven- en ondergrenzen . . . 128
9.2 Sorteren en lexicografische ordening . . . 136
9.3 Opgaven . . . 140

10 Oneindige verzamelingen **145**
10.1 Het diagonaalargument . . . 149
10.2 Opgaven . . . 152

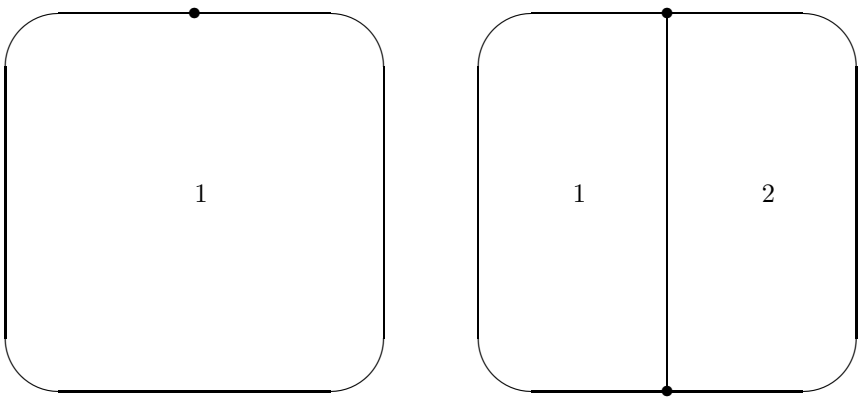
11 Extra opgaven **153**

Index **166**

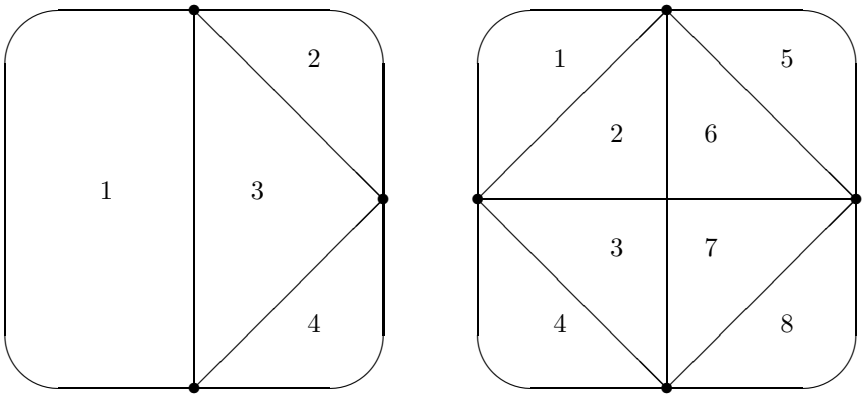
Hoofdstuk 1

Waarom iets bewijzen?

Teken eens een cirkel of aardappel of iets wat daar op lijkt met een punt op de rand. De cirkel bestaat nu uit een stuk. Teken nu een tweede punt op de rand, en verbind die met het eerste punt. Nu bestaat de cirkel uit twee stukken, zie onderstaand plaatje.



Teken nu een derde punt op de rand van de cirkel, en verbind die met de eerder gekozen punten. Nu bestaat de cirkel uit vier stukken. Teken nu een vierde punt op de cirkel, en verbind die met de eerder gekozen punten. Nu is de cirkel opgedeeld in acht stukken. Zie de plaatjes hieronder.



We doen het nog een keer: we kiezen een vijfde punt en verbinden dat met de eerdere vier punten. Als we goed tellen zien we dat nu de cirkel in zestien stukken is opgedeeld. Het zal duidelijk zijn wat het patroon hierin is: we beginnen met een stuk, en elke keer als er een punt bij komt krijgen we twee keer zo veel stukken. Bij een punt hebben we zo $1 = 2^0$ stukken, bij twee punten $2 = 2^1$, bij drie $4 = 2^2$, bij vier $8 = 2^3$ en bij vijf $16 = 2^4$. We concluderen:

> Als je n punten op een cirkel met elkaar verbindt, verdeel je daarmee de cirkel in 2^{n-1} stukken.

Dit lijkt allemaal best aannemelijk, en je bent niet zo gauw geneigd om dit nog uit te proberen voor zes of meer punten, want daarvoor moet je toch wel heel veel tekenen en tellen. Toch is het de moeite waard om dat wel eens te doen: bij zes punten lukt het je namelijk helemaal niet om 32 stukken te krijgen, en blijf je bij 31 steken, ook als je er voor zorgt dat er nergens drie verbindingslijnen door een punt gaan. We zijn er dus met zijn allen ingeluisd, en de hele bewering is niet waar, althans niet voor zes of meer punten.

Wat is nu de moraal van dit verhaal? Dat is dit: als je echt zeker wilt weten dat een bewering waar is, kun je niet vertrouwen op een paar voorbeelden en een aannemelijk verhaal dat een patroon in die voorbeelden verklaart, en dat daarom dat patroon altijd wel zal gelden. In de praktijk, zeker in die van de informatica of van die van medische apparatuur, zijn er heel veel situaties waarin je geen genoegen kunt nemen met een paar testgevallen en een aannemelijk verhaal dat het wel goed zit. Durf je te vliegen in een vliegtuig waarvan je zelf de besturingssoftware hebt geschreven, en best wel voor een redelijk aantal gevallen hebt uitgetest? Er zijn mensen om het leven gekomen door een veel te hoge straling, veroorzaakt door een foutje in de software van bestralingsapparatuur. Dit zijn toch dingen die je graag zou willen voorkomen. Nu kun je niet verwachten dat dat voor heel gecompliceerde dingen altijd zal lukken, maar een stap in die richting kan al heel waardevol zijn. En voor veel beweringen van een eenvoudiger type dan dat je correctheid eist van een ingewikkeld stuk software lukt dat prima. Wat wil je dan wel hebben? Een sluitende redenering dat een bepaalde bewering geldig is. Die redenering kun je dan voor je zelf gebruiken, om je zelf ervan te overtuigen dat je bewering klopt. Maar je kunt diezelfde redenering ook gebruiken om iemand anders te overtuigen. Of misschien jezelf weer, over een hele tijd als je de redenering weer vergeten mocht zijn. Daarvoor is het wel nodig

dat je de redenering opschrijft, en wel zodanig dat iemand anders aan de hand van wat je hebt opgeschreven de hele redenering ook kan volgen. En liefst ook omgekeerd: alles wat je hebt opgeschreven speelt een essentiële rol in de redenering. Zo'n redenering noemen we een *bewijs*. De onderdelen van zo'n bewijs hebben een heel preciese betekenis. Een redenering met een heel preciese betekenis kun je alleen maar geven als alles wat je daarin zegt, inclusief de hele bewering waar het om gaat, heel precies *beschreven is*. En daarmee zijn de voornaamste ingrediënten van dit vak *Beschrijven en Bewijzen* genoemd. Vaak maak je hierbij dankbaar gebruik van manieren om je beweringen heel kort in een soort formuletaal op te schrijven, waarbij je een bijbehorend stel spelregels hebt. In dit dictaat zullen uitgebreid dergelijke notaties en begrippen aan de orde komen, over proposities en predicaten en uit de wiskunde. Voordat we dat gaan doen lopen we eerst een aantal bewijsprincipes langs met bijbehorende voorbeelden, om een beetje een gevoel voor wat bewijsprincipes te ontwikkelen voor we ons in ingewikkelde notaties gaan storten.

1.1 Bewijzen uit het ongerijmde

Bewering:

> Een postbode levert 130 poststukken af in een straat met 43 adressen. Dan is er in die straat minstens één adres waarop vier of meer poststukken zijn afgeleverd.

Hoe kun je het makkelijkst inzien dat deze bewering inderdaad klopt? Stel eens dat de geconcludeerde bewering *er is minstens een adres waarop vier of meer stukken zijn afgeleverd* niet waar is. Dan zijn er op elk adres dus hoogstens drie stukken afgeleverd. Met 43 adressen totaal betekent dat dat er in totaal hoogstens $3 \times 43 = 129$ stukken zijn afgeleverd. En dat is in tegenspraak met het gegeven dat er in totaal 130 stukken zijn bezorgd. Dus is de geconcludeerde bewering *er is minstens een adres waarop vier of meer stukken zijn afgeleverd* wel waar, en hebben we de bewering bewezen.

Het patroon in deze redenering komt heel vaak voor. Steeds is er een bewering waarvan je wilt bewijzen dat die waar is. De redenering ziet er dan als volgt uit:

> Stel de bewering is niet waar. Vanuit deze aanname trek je, eventueel samen met aannamen die deel uitmaken van de gegevens in de bewering, allerlei conclusies, tot je op een bewering uitkomt die niet waar is, of in tegenspraak is met gegevens in de bewering. Daaruit concludeer je dat de aanname *de bewering is niet waar*, niet kan kloppen, en is daarmee de bewering zelf wel waar.

Een redenering van deze vorm wordt wel een *bewijs uit het ongerijmde* genoemd, in het Engels: *proof by contradiction*. In dit speciale voorbeeld wordt een telargument gegeven, dat ook wel het *pigeon hole principle* (*duiventilprincipe*) wordt genoemd; we komen daar later nog op terug (Stelling 6.5).

Als je van een bewering waarvan je denkt dat die waar is, probeert te bewijzen dat die inderdaad waar is, is het een goed idee om eens op een rijtje te zetten wat er allemaal gebeurt als die bewering niet waar is. Als het lukt om daar iets onzinnigs uit te concluderen, is de hele redenering om te vormen tot een bewijs uit het ongerijmde. Een waarschuwing is hier echter wel op zijn plaats: elke bewering die te bewijzen is, is op deze manier als volgt

te bewijzen met een bewijs uit het ongerijmde. Stel de bewering is niet waar, geef een bewijs van de bewering, dit is in tegenspraak met de aanname dat de bewering niet waar is, en dus is de bewering waar. Wat betreft de geldigheid is hier niets tegenin te brengen, maar deze redenering bevat wel een hoop overbodige ballast: het bewijs van de bewering zelf is natuurlijk een stuk korter dan datzelfde bewijs met nog een hoop geredeneer er om heen. Uit het oogpunt van efficientie is een kort bewijs altijd te prefereren boven een langer bewijs. Tegen de tijd dat je een bewijs uit het ongerijmde hebt gevonden, is het dan ook altijd een goed principe om te kijken of je de redenering uit het ongerijmde wel echt nodig hebt, en niet in feite dezelfde redenering korter rechtstreeks kunt geven.

Nauw verwant aan een bewijs uit het ongerijmde is een bewijs met *contrapositie*. Dat betekent dat je als een bewering van de vorm

> Als P geldt, dan geldt ook Q

wilt bewijzen, in plaats hiervan ook mag bewijzen

> Als Q niet geldt, dan geldt ook niet P.

Merk op dat we twee keer het woord 'niet' hebben toegevoegd, en P en Q hebben omgewisseld. We laten nu zien met een bewijs uit het ongerijmde dat dit nieuwe bewijsprincipe inderdaad klopt. We willen de bewering *Als P geldt, dan geldt ook Q* bewijzen, en stellen dat dit niet waar is. Dat kan alleen maar als er een situatie bestaat waarin P wel waar is, maar Q niet; we komen hier later uitgebreid op terug. We hadden aangenomen dat we konden bewijzen *Als Q niet geldt, dan geldt ook niet P*. Omdat in de betreffende situatie Q niet geldt, kunnen we dus concluderen dat dan ook P niet geldt. Maar dit is in tegenspraak met de eerdere aanname dat in die situatie P juist wel geldt.

Zoals gezegd is het een goed principe om van een bewering die je zou willen bewijzen, te gaan uitpluizen wat er allemaal gebeurt als die bewering niet waar is. Als het lukt om daar een tegenspraak uit af te leiden, is daarmee de bewering bewezen met een bewijs uit het ongerijmde. Als het echter niet lukt een tegenspraak te vinden, kun je juist gaan zoeken naar een voorbeeld waarvoor de bewering niet waar is. Als je zo'n voorbeeld hebt gevonden, heet dat een *tegenvoorbeeld*, (Engels: *counterexample*) waarmee dan juist bewezen is dat de bewering niet waar is.

Opgave 1.1

Geef van elk van de volgende beweringen een bewijs of een tegenvoorbeeld:

- in elke groep van 50 mensen zijn er zes of meer die allemaal in dezelfde maand jarig zijn;
- in elke groep van 50 mensen zijn er vijf of meer die allemaal in dezelfde maand jarig zijn;
- in elke groep van 50 mensen zijn er vier of meer die allemaal in dezelfde maand jarig zijn.

1.2 Bewijzen met gevalsonderscheid

Als je de getallen van 1 tot en met 100 bij elkaar optelt, wat komt er dan uit? Als je gaat rekenen: $1+2=3$, $3+3=6$, $6+4=10$, $10+5=15$, enzovoorts, dan ben je nog al even bezig. Het kan ook handiger:

$$1+100=101,\ 2+99=101,\ 3+98=101,\ldots,\ 50+51=101.$$

Nu hebben we de 100 getallen in 50 groepjes van twee opgesplitst, waarbij voor elk groepje van twee de som 101 is. Het totaal is dus $50\times 101=5050$.

Laten we het algemener bekijken (overigens ook een algemeen principe: probeer eerst een speciaal geval en als je daar iets voor verzonnen hebt, probeer dat dan algemener te maken). Als k en n gehele getallen zijn met $k<n$, en ik tel alle $n-k+1$ getallen van k tot en met n bij elkaar op, wat komt daar dan uit? Met hetzelfde truukje van zonet tellen we de eerste bij de laatste op, de op een na eerste bij de op een na laatste, en zo verder:

$$k+n=k+n,\ (k+1)+(n-1)=k+n,\ (k+2)+(n-2)=k+n,\ldots.$$

Hoe eindigt dit? We zien dat het uitmaakt of het aantal $n-k+1$ even is of niet. Als dit aantal even is, krijgen we precies $\frac{n-k+1}{2}$ groepjes van twee waarvan de som steeds $k+n$ is. De som van de hele rij getallen is dus $(k+n)\times\frac{n-k+1}{2}=\frac{(k+n)(n-k+1)}{2}$.

Als het aantal oneven is, krijgen we $\frac{n-k}{2}$ groepjes van twee waarvan de som steeds $k+n$ is, en houden we het middelste van de rij getallen over. Dat middelste getal is het gemiddelde van de eerste en de laatste, dus $\frac{k+n}{2}$. De som van al deze getallen is dus

$$(k+n)\times\frac{n-k}{2}+\frac{k+n}{2}=\frac{(k+n)(n-k)+(k+n)}{2}=\frac{(k+n)(n-k+1)}{2}.$$

We zien dus dat ook in dit geval de som van de hele rij $\frac{(k+n)(n-k+1)}{2}$ is, en concluderen dat het in alle gevallen zo is. We hebben dus bewezen:

> Als k en n gehele getallen zijn met $k<n$, dan is de som van alle getallen van k tot en met n gelijk aan $\frac{(k+n)(n-k+1)}{2}$.

In het bewijs van deze bewering hebben we een *gevalsonderscheid* (Engels: *case analysis*) gemaakt: voor het geval dat het aantal even was hebben we een bewijs gegeven, en voor het geval dat het aantal oneven was hebben we een ander bewijs gegeven. Aangezien elk geheel getal even of oneven is, hebben we hiermee voor alle gevallen een bewijs gegeven.

Net zoals bij bewijzen uit het ongerijmde is het bij bewijzen met gevalsonderscheid een goed principe om te kijken of je het gevalsonderscheid wel echt nodig hebt. Als je het namelijk niet nodig hebt, kun je waarschijnlijk een korter bewijs geven. In dit voorbeeld is dat inderdaad mogelijk als we met het maken van groepjes van twee niet stoppen als we op de helft zijn, maar nog even doorgaan:

$$k+n=k+n,\ (k+1)+(n-1)=k+n,\ (k+2)+(n-2)=k+n,\ldots$$

$$\ldots,(n-1)+(k+1)=k+n,\ n+k=k+n.$$

Nu hebben we evenveel groepjes van twee gemaakt als het aantal getallen wat we bij elkaar op wilden tellen, namelijk $n-k+1$. Elk van deze groepjes heeft $k+n$ als som, al deze

groepjes hebben dus samen $(k+n)(n-k+1)$ als som. In deze groepjes komen elk van de getallen precies twee keer voor: een keer als linkerlid van een groepje en een keer als rechterlid. Daarmee is tweemaal de gevraagde som dus gelijk aan $(k+n)(n-k+1)$, en concluderen we zonder gevalsonderscheid te maken dat de gevraagde som altijd gelijk is aan $\frac{(k+n)(n-k+1)}{2}$.

In het eerste bewijs hebben we een opsplitsing in twee gevallen gemaakt: het aantal is even of het aantal is oneven. Het is ook mogelijk een probleem in meer dan twee gevallen op te splitsen. Van belang is altijd dat alle situaties die aan de voorwaarden van de bewering voldoen, onder tenminste een van de aangegeven gevallen vallen: de opsplitsing moet *uitputtend* zijn, in het Engels: *exhaustive*. Dat sommige situaties onder meer dan een van de gevallen vallen is niet erg. Dit illustreren we met het volgende voorbeeld:

Voor elk reëel getal x geldt dat $x \times x \geq 0$.

We bewijzen dit als volgt: we maken het gevalsonderscheid $x \geq 0$ of $x \leq 0$. Dit onderscheid is inderdaad uitputtend: voor elk reëel getal x geldt een van beide voorwaarden.

Als $x \geq 0$ dan is $x \times x$ het product van twee getallen die elk tenminste 0 zijn; het product is dan ook tenminste 0.

Als $x \leq 0$ dan is $-x \geq 0$, en is $x \times x = (-x) \times (-x)$ het product van twee getallen die elk tenminste 0 zijn; het product is dan ook tenminste 0.

Voor beide gevallen hebben we nu een bewijs gegeven, en daarmee is het bewijs voltooid. Merk op dat het geval dat $x = 0$ onder beide gevallen valt. In feite hebben we de bewering voor dit geval dus twee keer bewezen.

Het is een goed gebruik bij gevalsonderscheid te beginnen bij de makkelijkste gevallen en het moeilijkste voor het laatst te bewaren.

Opgave 1.2

Wat komt er uit als je alle even getallen van 2 tot en met 100 bij elkaar optelt? En wat komt er uit als je alle oneven getallen van 17 tot en met 47 bij elkaar optelt? Geef een formule die voor elke n aangeeft wat de som is van alle even getallen van 2 tot en met $2n$.

Opgave 1.3

Bewijs dat het kwadraat van een oneven getal altijd te schrijven is als $8n + 1$ voor een geheel getal n.

1.3 Bewijzen met inductie

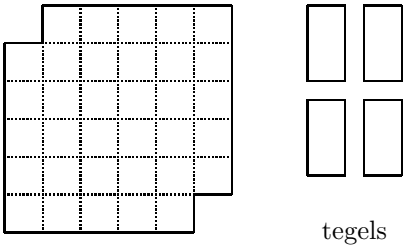
Voor beweringen die afhangen van een natuurlijk getal n is het vaak handig in het bewijs gebruik te maken van het gegeven dat de bewering voor kleinere waarden dan n al waar is. Dat je daarmee toch een correct bewijs mee kunt leveren zegt het *principe van volledige inductie*. In hoofdstuk 7 zal dit uitgebreid aan de orde komen.

1.4 Bewijzen met invarianten

Alvorens het principe uit te leggen beginnen we met een aantal puzzels.

De keukenvloer

We hebben een vierkante keukenvloer met een zijde van n decimeter. In de rechter onderhoek en in de linker bovenhoek mist een vierkante decimeter (voor een verwarmingsbuis). Voor welke n kan de keukenvloer met tegels van 2×1 decimeter betegeld worden? Bijvoorbeeld voor $n = 6$ is de situatie als volgt:



vloer tegels

De koffiekan

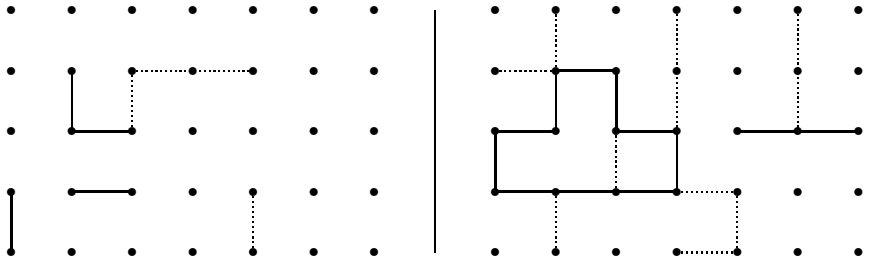
In een koffiekan zitten 25 zwarte en 25 witte bonen. De volgende handeling wordt uitgevoerd zolang dat mogelijk is: *haal twee bonen uit de kan; als ze dezelfde kleur hebben, stop dan een zwarte boon in de kan; als ze verschillend van kleur zijn, stop dan de witte terug in de kan.* Er is een voldoende voorraad extra zwarte bonen. Vraag: wat is de kleur van de laatste boon in de kan?

Het lijnen-spel

Het speelbord bestaat uit een rechthoek met punten. Twee spelers, A en B, doen om beurten een zet; A begint. Speler A doet een zet door twee aangrenzende punten met een horizontale of een verticale lijn te verbinden, speler B doet hetzelfde, maar dan met stippellijnen. Spelers mogen reeds verbonden punten niet nog eens verbinden. Na vier zetten van beide spelers kan het bord er bijvoorbeeld uitzien als links in onderstaand plaatje.

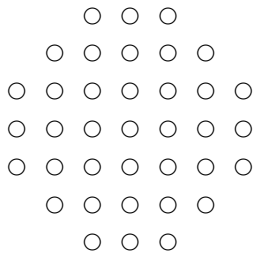
Speler A wint als hij een gesloten figuur kan maken, zoals in het rechter plaatje; speler B heeft een andere opdracht: B wint als ze A kan verhinderen een gesloten figuur te maken.

Vraag: is er voor één van beide spelers een winnende strategie? Zo ja, welke?



Solitaire

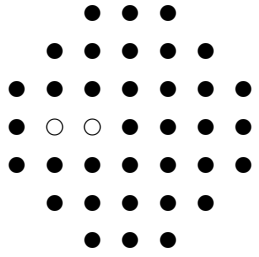
We beschouwen het spelletje *solitaire*, dat — de naam zegt het al — je in je eentje kunt spelen. We kijken hier naar de Franse versie van het spel, dat gespeeld wordt op een bord bestaande uit 37 velden dat er als volgt uitziet:



In de beginsituatie is het middelste veld leeg en staat er op elk ander veld een pionnetje, dus 36 in totaal. Nu mag er geslagen worden: horizontaal en verticaal mag een pionnetje over een een buurpionnetje heenspringen naar het daarachter gelegen lege veld, waarbij het pionnetje waar over heen gesprongen is weggenomen wordt. Laten we pionnetjes met een zwart rondje aangeven en onbezette velden met een open rondje; als dan de volgende situatie op het bord voorkomt

dan kan het linker pionnetje over zijn rechterbuurman heenspringen en is het resultaat:

Na één zet kan het bord er dus als volgt uit zien:



De bedoeling van het spel is nu om net zo lang volgens deze spelregel te spelen totdat er nog maar slechts één pionnetje over is, dat dan liefst ook nog in het midden moet staan. In

het begin is het niet zo moeilijk om te zetten, maar na een tijdje spelen staan er ineens een stuk of wat pionnetjes verspreid over het bord waarvan er geen twee naast elkaar staan, en kan er dus niet meer gezet worden. De vraag is nu: is het mogelijk om te eindigen in een situatie waarbij er nog maar één pionnetje over is?

De oplossingen

Deze vier puzzels zijn allemaal gebaseerd op herhaling: herhaald tegels leggen, herhaald bonen trekken, herhaald regels toepassen en herhaald zetten doen. Ze kunnen opgelost worden door steeds een geschikte *invariant* te beschouwen: een eigenschap die steeds blijft gelden. We geven eerst de definitie.

Definitie 1.1 Een invariant is een eigenschap van een proces of een programma, die voldoet aan het volgende:

- aan het begin geldt de invariant, en
- als de invariant geldt en er wordt vervolgens een stap gedaan, dan geldt na afloop van die stap de invariant weer.

Als we zo'n eigenschap hebben, blijft die dus altijd gelden, hoeveel stappen er ook worden uitgevoerd. Als na eindig veel stappen het proces of programma voltooid is, geldt de invariant na afloop dus nog steeds. Deze observatie is cruciaal voor de oplossingen van elk van de puzzels, en is een belangrijk bewijsprincipe in de informatica.

Hier volgen de oplossingen:

De keukenvloer

We maken een gevalsonderscheid. Als n oneven is dan is n^2 oneven, en $n^2 - 2$ dus ook. Een vloer van een oneven aantal dm^2 is nooit te betegelen met tegels die elk 2 dm^2 groot zijn.

Als n even is dan kleuren we de vloer in gedachten als een schaakbord: om en om wit en zwart, met de rechter onderhoek wit. De twee verwarmingsbuizen staan in een wit veld. Er moeten dus twee zwarte velden méér betegeld worden dan witte velden. Omdat elke tegel één zwart en één wit veld bedekt, zullen we, hoe we ook tegelen, altijd twee zwarte velden overhouden. Een betegeling is dus niet mogelijk.

We hebben gebruik gemaakt van de invariant

$$\textit{aantal onbetegelde zwarte velden} = \textit{aantal onbetegelde witte velden} + 2$$

Deze uitspraak is in het begin waar, en blijft invariant bij het leggen van een tegel. De uitspraak geldt dus voor alle gedeeltelijke betegelingen, en er is geen betegeling waarin geen onbetegelde zwarte velden over zijn.

De koffie-kan

Allereerst merken we op dat bij elke trekking er twee bonen verwijderd worden, en één teruggelegd. Na 49 trekkingen zal er dus nog één boon over zijn.

Het ondoenlijk alle mogelijkheden te proberen, dat zijn er heel erg veel. In plaats daarvan zoeken we naar een geschikte invariant. We kijken naar het netto effect op het aantal witte en zwarte bonen bij elk van de vier mogelijke trekkingen:

trekking	actie	Z	W
$-ZZ$	$+Z$	-1	0
$-WW$	$+Z$	$+1$	-2
$-ZW$	$+W$	-1	0
$-WZ$	$+W$	-1	0

Het aantal witte bonen in de kan blijft gelijk of neemt met twee af. Het oneven-zijn van het aantal witte bonen is dus een invariant in dit spel!

Het aantal witte bonen blijft dus altijd oneven, in het bijzonder aan het eind. De laatste boon is dus altijd wit.

Opgave 1.4

In een doos zitten 100 rode, 100 witte en 100 blauwe ballen. Zolang dat mogelijk is, worden er drie ballen uit de doos gepakt. Als alle drie de ballen dezelfde kleur hebben, wordt er één van die drie teruggelegd. Als alle drie de ballen een verschillende kleur hebben, wordt een rode bal teruggelegd. Als er twee ballen dezelfde kleur hebben, wordt de afwijkende derde teruggelegd en bovendien een blauwe. Is het mogelijk te eindigen met een rode en een blauwe bal?

Het lijnen-spel

Op een bord van 2×2 punten kan A niet winnen: er zijn minstens 4 lijnen nodig om een gesloten figuur te maken. Laten we daarom eerst kijken of er een winnende strategie voor B is. Het spel vaak spelen geeft weinig inzicht in een strategie. Daarom kijken we naar de eigenschappen van gesloten figuren. Als B kan verhinderen dat één van deze eigenschappen op het bord komt, kan ze winnen. De invariant luidt dan: het bord bevat geen figuur met de betreffende eigenschap.

Welke eigenschappen heeft een gesloten figuur? Er zitten parallelle lijnen in, maar die kan B niet verhinderen. Er zit een even aantal parallelle lijnen in, maar ook dat kan B niet verhinderen. Er zitten tenminste vier hoeken in, maar B kan niet verhinderen dat A hoeken tekent. Er zit minstens één L-vormige hoek in met de punt links onder, en díe kan B verhinderen! Elke keer als A een horizontale of verticale lijn trekt, kan B deze aanvullen tot een L-vorm (tenzij A op de boven- of rechterrand zet; dan mag B een willekeurige zet doen). A kan dan nooit zelf een L-vorm in zijn figuur maken, en dus geen gesloten figuur. Op grond van de invariant: '*het bord bevat geen* L*-vormen van* A' kunnen we concluderen: B heeft een winnende strategie.

Solitaire

We maken een indeling van de 37 velden in A-velden, B-velden en C-velden, en wel als volgt:

```
      A B C
    A B C A B
  A B C A B C A
  B C A B C A B
  C A B C A B C
    B C A B C
      A B C
```

Verder definiëren we:

- a is het aantal A-velden waarop een pionnetje staat,
- b is het aantal B-velden waarop een pionnetje staat,
- c is het aantal C-velden waarop een pionnetje staat.

Opgave 1.5

Bewijs dat het solitaire spel niet kan eindigen in een situatie waarin er nog slechts één pion op het bord staat.

(Aanwijzing: gebruik de invariant:

a, b en c zijn alle drie even of ze zijn alle drie oneven.)

Bij puzzels zoals deze worden invarianten vaak gebruikt om aan te tonen dat bepaalde oplossingen niet mogelijk zijn. Gelukkig spelen ze in de informatica meestal een wat positievere rol, namelijk om aan te tonen dat na afloop van het uitvoeren van een programma een bepaalde gewenste eigenschap wèl geldt. Een aardig voorbeeld hiervoor is het volgende programma waarmee je handig twee getallen kunt vermenigvuldigen:

z := 0;
a := A;
b := B;
zolang $a \neq 0$ doe dan:
als a oneven is dan: $a := a - 1$;
$z := z + b$
als a even is dan: $a := a/2$;
$b := 2b$

Hierin zijn A en B de getallen die je wilt vermenigvuldigen; aangenomen wordt dat $A \geq 0$. In de variabele z komt het antwoord te staan, en a en b zijn hulpvariabelen. De notatie $x := \cdots$ betekent dat de variabele x de waarde $\cdots$ krijgt. Dat na afloop de waarde van z inderdaad $A \times B$ is, volgt uit het feit dat

$$z + a \times b \;=\; A \times B$$

een invariant is van het "zolang"-stuk van het programma. Voordat aan de uitvoering van dat stuk van het programma begonnen wordt heeft z de waarde 0 en geldt $a = A$ en $b = B$. Dan geldt inderdaad $z + a \times b = 0 + A \times B = A \times B$.

Als de invariant geldt en a is oneven, dan wordt een stap gedaan waarbij a wordt vervangen door $a - 1$ en z wordt vervangen door $z + b$. Vanwege $(z + b) + (a - 1) \times b = z + a \times b = A \times B$ geldt na afloop van die stap dus weer de invariant.

Als de invariant geldt en a is even, dan wordt een stap gedaan waarbij a wordt vervangen door $a/2$ en b wordt vervangen door $2b$. Vanwege $z + (a/2) \times 2b = z + a \times b = A \times B$ geldt na afloop van die stap dus weer de invariant.

We concluderen dat na afloop[1] de invariant nog steeds geldt. In dat geval is $a = 0$, want zolang $a \neq 0$ stop het programma nog niet. Vanwege de invariant hebben we dan

$$z \;=\; z + 0 \times b \;=\; z + a \times b \;=\; A \times B$$

waarmee we bewezen hebben dat z inderdaad de waarde van het gevraagde product heeft.

Opgave 1.6

Bereken 13×17 met bovenstaande methode.

Opgave 1.7

Met de volgende regels kun je van rijtjes symbolen andere rijtjes symbolen maken:

1. achter een rijtje met een I aan het eind mag je een U zetten;
2. van het rijtje Mx mag je Mxx maken, voor elk rijtje symbolen x;
3. als er III in een rijtje staat, mag je dat vervangen door U;
4. als er UU in een rijtje staat, mag je dat weglaten.

Als voorbeeld bekijken we een aantal rijtjes die je uit MI kunt produceren:

a.	MI	gegeven
b.	MII	uit a volgens regel 2
c.	MIIII	uit b volgens regel 2
d.	MIIIIU	uit c volgens regel 1
e.	MUIU	uit d volgens regel 3
f.	MUIUUIU	uit e volgens regel 2
g.	MUIIU	uit f volgens regel 4

Vraag: is het mogelijk om beginnend met het rijtje MI uit te komen op het rijtje MU? Zo ja, hoe? Zo nee, waarom niet?

(Aanwijzing: laat zien dat in geen enkel opgebouwd rijtje het aantal I's een drievoud is.)

[1] Het is inderdaad in te zien dat dit programma niet oneindig lang doorgaat, en zelfs vrij snel tot zijn einde komt

1.5 Nog wat terminologie

Een belangrijke bewering waarvoor een bewijs bestaat, wordt vaak een *stelling* genoemd; in het Engels *theorem*. Een iets minder belangrijke bewering waarvoor een bewijs bestaat, wordt wel een *propositie* genoemd; in het Engels *proposition*. Een bewering met een bewijs waarvan het belang niet op zich zelf staat, maar voornamelijk dient als hulpresultaat om een stelling te bewijzen, heet een *lemma*. Een gevolg van een stelling wordt wel *corollarium* genoemd; in het Engels *corollary*. Het precies vastleggen van de betekenis van een nieuw begrip heet een *definitie*. Een fundamentele bewering die je niet bewijst maar als uitgangspunt hanteert heet een *axioma*.

Bij een bewijs is het handig om te zien waar het begin en eindigt. Meestal begint het met het woord *bewijs* (in het Engels *proof*), en eindigt het met een blokje □. In sommige teksten wordt een bewijs wel afgesloten met de afkorting Q. E. D.. Dit staat voor *quod erat demonstrandum*, hetgeen Latijn is voor "hetgeen bewezen moest worden". In dit dictaat zullen we een bewijs vaak afsluiten met de woorden *einde bewijs*.

Een bewering waarvan je verwacht dat die waar is, maar waarvoor geen bewijs gevonden is, heet een *vermoeden*; in het Engels *conjecture*. Het is verbazend dat er veel eenvoudig te formuleren beweringen bestaan waarvan de juistheid wel vermoed wordt, er is dan ook nooit een tegenvoorbeeld voor gevonden, maar waarvoor ook na uitgebreide inspanning van zeer knappe mensen nog nooit een bewijs is gevonden. Enkele voorbeelden van dergelijke vermoedens zijn:

- Elk even getal groter dan 2 is de som van twee priemgetallen.
- Er bestaan oneindig veel priemgetallen p waarvoor $p + 2$ ook een priemgetal is.
- Begin met een willekeurig positief geheel getal. Herhaal steeds het volgende proces: als het even is deel je het door twee, en als het oneven is vermenigvuldig je het met drie en telt er daarna 1 bij op. Vermoeden: dit proces komt altijd terecht in $\cdots \to 1 \to 4 \to 2 \to 1 \to \cdots$.

Het komt ook wel voor dat dergelijke vermoedens toch nog bewezen worden. Een frappant voorbeeld hiervoor is de *laatste stelling van Fermat*, rond 1637 door Fermat geformuleerd: er bestaan geen gehele getallen $n > 2$ en $a, b, c > 0$ waarvoor $a^n + b^n = c^n$. Hoewel Fermat zelf beweerde hiervoor een wonderbaarlijk bewijs te hebben gevonden dat helaas te groot was om in de kantlijn op te nemen, is dat 'bewijs' niet bewaard gebleven en is deze bewering honderden jaren een vermoeden geweest. Tot 1993: toen gaf Andrew Wiles hiervan een bewijs, dat compact opgeschreven enige honderden pagina's besloeg, exclusief de bewijzen van de vele gebruikte veelal zeer diepe al eerder bekende stellingen.

Hoofdstuk 2

Proposities

In de wiskunde en in de informatica, en ook in veel andere disciplines, is er behoefte aan redeneren. Om dat goed te kunnen doen moet men allereerst beschikken over een arsenaal van begrippen en uitdrukkingswijzen. Alleen wanneer men over deze zaken tot overeenstemming kan komen, bestaat er een redelijke kans dat twee of meer beoefenaren van een vak met elkaar kunnen praten zonder al te vaak in onzekerheid te verkeren over de betekenis van mededelingen die worden uitgewisseld.

We geven een paar voorbeelden van zinnen die men in de krant zou kunnen lezen:

"niemand kan dit bijna doen"

"kamer aangeboden voor student, tot 25 jaar"

"wegens lekkage kerncentrale gesloten"

Er bestaat in bovenstaande voorbeelden weinig kans op misverstanden omdat verkeerde (?) interpretatie onwaarschijnlijke situaties schetst. Echter ... het laatste bericht zou ook op de deur van een winkel kunnen hangen. En het is menigmaal voorgekomen dat een verdachte vrijgesproken is op grond van een onduidelijk gestelde beschuldiging.

Voorbeelden van een "vaktaal" in andere disciplines vinden we heel duidelijk in de protocollen van gerechtelijke uitspraken, en in notariële akten. Ook daar heeft men gekozen voor bepaalde vaste formuleringen om de zaken ondubbelzinnig vast te leggen. Voor een buitenstaander wordt het daardoor echter meestal niet duidelijker, vaak is juist het tegendeel het geval!

De manier waarop iets is opgeschreven valt onder het begrip *syntax*, de betekenis van het opgeschrevene valt onder het begrip *semantiek*. We kunnen dus zeggen dat "zeven" en "7" syntactisch verschillend en semantisch hetzelfde zijn.

We definiëren, omschrijven is een beter woord, nu het belangrijkste begrip van dit hoofdstuk. Graag zouden we dat wat preciezer doen, maar dat precieze begrippenapparaat moeten we juist nog opbouwen.

Definitie 2.1 Een *propositie* is een zinvolle bewering, een vaststelling met een duidelijke betekenis: *waar* of *niet waar*.

Het is erg lastig om een fundamenteel begrip zoals "propositie" ondubbelzinnig vast te leggen. Hoe objectief zijn "zinvol" en "duidelijk" ? Wanneer we ons beperken tot de beweringen in een programmeertaal, dan is het tamelijk eenvoudig om precies te definiëren wat een propositie is, dat wil zeggen: hoe een propositie er syntactisch uitziet. We hebben dan een erg beperkte woordenschat, en kunnen gebruik maken van de syntactische schema's die de programmeertaal definiëren. Wij zullen ons hier echter niet zo strikt vastleggen op de syntax, omdat we de theorie toepasbaar willen laten zijn op algemene onderwerpen uit wiskunde èn informatica.

Voorbeelden van proposities zijn:

"in deze zaal zitten 140 mensen"
"een plus een is twee" "drie plus vijf is zes"
"de maan is een spiegel" "$3 + 5 = 6$"
"dit bewijs is fout" "$1 - 1 = 0$"

We laten nu een paar voorbeelden zien van uitspraken die geen proposities zijn, en geven bij iedere uitspraak een kort commentaar tussen haakjes

"x is gelijk aan y" (ik weet niet wat x is en wat y is)

"ga naar huis" (dit is geen vaststelling, maar een bevel)

"zou het regenen?" (wel goed is "het regent")

"jan te ver kaas" (wat zou hiervan de betekenis zijn?, dit voldoet ook niet aan de syntax van de nederlandse taal)

Tenslotte nog een paar voorbeelden van uitspraken die wat complexer van aard zijn, en daarom meer aandacht vragen als het gaat om de vraag of het proposities zijn

"alle mensen zijn dieren"

"als het gras nat wordt, dan regent het"

"Jan is een zoon van Kees en Mien is de moeder van Jaap"

"de zon schijnt of het regent"

Een nieuw element in bovenstaande uitspraken is dat er verschillende beweringen in één uitspraak worden gedaan. We komen hierop nog terug.

In enkele van de voorbeelden hebben we al gezien dat een propositie niet waar hoeft te zijn.

In de definitie van het begrip propositie hebben we gëist dat hij hetzij *waar* hetzij *onwaar* is (precies één van beide). Dit betekent echter niet dat we over de waarheid onmiddellijk uitsluitsel moeten kunnen geven. Zo beschouwen we de uitspraak

"onder de eerste tien miljard decimalen van π komen precies één miljard cijfers 9 voor"

wel als een propositie. Immers zij is waar of onwaar, maar we kunnen (nog) niet vaststellen of zij waar dan wel onwaar is. Daarentegen is

"deze zin is onwaar"

geen propositie. Immers deze bewering kan niet waar zijn (want dan zegt zij zelf onwaar te zijn) en zij kan ook niet onwaar zijn (want dan zegt zij zelf waar te zijn). Men kan ook zeggen dat deze bewering zowel waar als onwaar is. Naar onze begrippen is de betekenis van deze bewering niet duidelijk.

Merk op dat we gebruik hebben gemaakt van een nog onuitgesproken afspraak, die we nu expliciet zullen vastleggen.

Afspraak:

"niet onwaar" betekent hetzelfde als "waar"

Deze fundamentele afspraak (we noemen zoiets ook wel een *axioma*) is een grondpeiler van de klassieke logica. Hierdoor wordt het mogelijk om een bewijs uit het ongerijmde te leveren zoals dat in het vorige hoofdstuk ook al aan de orde kwam: als de ontkenning van een propositie onwaar is, dan is de propositie zelf waar!

In het vervolg zullen we de betekenis van een propositie verengen tot het waar danwel onwaar zijn van de propositie.

2.1 Samenstellen van proposities

We hebben net al door voorbeelden aangestipt dat het wenselijk is als we proposities kunnen samenstellen. In feite willen we iets meer, namelijk zo'n samenstelling zou weer een propositie moeten zijn. Daarvoor is nodig dat de samenstelling ook voldoet aan de definitie van propositie, en dus moeten we precies vastleggen wat we zullen bedoelen met uitspraken zoals

"... en ..."

"... of ..."

"als ... dan ..."

"... dan, en slechts dan, als ..."

"niet ..."

waarin op de plaats van de stippeltjes proposities kunnen worden ingevuld.

Een eerste stap in de goede richting is het vastleggen van een notatie voor deze samenstellingen. Het is niet verstandig om hiervoor alleen het gewone woordgebruik te kiezen. Immers aan het begin van dit hoofdstuk hebben we al gezien dat hierdoor misverstanden zouden kunnen ontstaan bij de interpretatie. Daarnaast heeft het invoeren van een compacte notatie het voordeel dat ingewikkelder uitdrukkingen die we daarmee opbouwen, nog steeds betrekkelijk compact opgeschreven kunnen worden.

Notatie

Laten p en q proposities voorstellen. We gebruiken de volgende notaties:

$p \wedge q$	voor	"p en q"
$p \vee q$	voor	"p of q"
$p \rightarrow q$	voor	"als p dan q"
$p \leftrightarrow q$	voor	"p dan, en slechts dan, als q"
$\neg p$	voor	"niet p"

De symbolen $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\neg$ heten *connectieven*, of ook wel *Boolse operatoren*. Ze staan respectievelijk bekend onder de namen *conjunctie*, *disjunctie*, *implicatie*, *equivalentie*, *negatie*.

2.2 Waarheidstafels

We gaan nu de betekenis van deze samenstellingen vastleggen. Omdat de uitspraken p en q proposities zijn, is hun betekenis per definitie duidelijk: waar of niet waar. Omdat er maar twee mogelijkheden zijn kunnen we de betekenis van een samenstelling vastleggen door voor alle mogelijke waarden van p en q het resultaat vast te leggen. We doen dit met behulp van *waarheidswaarde* en *waarheidstafels*.

Definitie 2.2 De waarheidswaarde van een propositie is 0 of 1:
een propositie die waar is, heeft waarheidswaarde 1,
een propositie die onwaar is heeft waarheidswaarde 0.

Vervolgens stellen we de zogenaamde waarheidstafels op: we sommen systematisch alle combinaties van waarheidswaarden van p en q op, en geven bij elke samenstelling aan wat het gewenste resultaat is. Dit kunnen we voor elke samenstelling afzonderlijk doen, maar we kunnen het ook combineren in een grote tabel:

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

Deze tabel kan gezien worden als een compact opgeschreven definitie van alle samenstellingen.

Als we willen weten hoe de waarheidswaarde van bijvoorbeeld $p \wedge q$ afhangt van de waarheidswaarden van p en van q, dan vergelijken we de kolommen van p en q met de kolom van $p \wedge q$ en lezen de gewenste informatie horizontaal af. Hieruit zien we dan de definitie van $p \wedge q$:

Definitie 2.3 De propositie $p \wedge q$ is waar als p en q beide waar zijn. In alle andere gevallen is $p \wedge q$ onwaar.

Analoog hebben we de definitie van $p \vee q$:

Definitie 2.4 De propositie $p \vee q$ is onwaar als p en q beide onwaar zijn. In alle andere gevallen is $p \vee q$ waar.

Hetzelfde kunnen we doen met $\neg p$. Omdat $\neg p$ alleen afhangt van p kunnen we ook de kleinere tafel

p	$\neg p$
0	1
1	0

raadplegen en vinden als definitie

Definitie 2.5 De propositie $\neg p$ is waar als p onwaar is en onwaar als p waar is.

De definitie van de overige ter sprake gekomen samenstellingen zouden we na deze twee voorbeelden aan de lezer kunnen overlaten, maar we vinden het toch wenselijk om wat uitvoeriger stil te staan bij $p \to q$.

Uit de tabel zien we

Definitie 2.6 De propositie $p \to q$ is onwaar als p waar en q onwaar is. In alle andere gevallen is $p \to q$ waar.

Een consequentie van deze definitie van $p \to q$ is, dat er voor de waarheid van $p \to q$ *geen verband* tussen p en q vereist is.
Als we dus voor p en q twee ware proposities invullen die niets met elkaar te maken hebben, dan is $p \to q$ een ware uitspraak.
Een ware uitspraak is bijvoorbeeld

$1 = 1 \to$ de diagonalen van een ruit staan loodrecht op elkaar

Het is *af te raden* "$p \to q$" uit te spreken als "uit p volgt q": geldigheid van $p \to q$ zegt alleen dat q waar is als p waar is, en niet dat daarbij sprake is van een oorzakelijk verband.

Een andere consequentie is, dat $p \to q$ altijd waar is als p onwaar is. Nu vinden we dat misschien niet zo erg vreemd, omdat we een uitspraak zoals

"als Pasen en Pinksteren op één dag vallen, dan ..."

niet als een leugen opvatten, ook al zou er op de plaats van de stippeltjes iets onwaars staan. Plastisch gezegd: Uit een absurde veronderstelling kan men alles concluderen.

Toch zal menigeen de wenkbrouwen fronsen bij het lezen van de ware uitspraak

$$e = \pi \ \to \ 1 = 1.$$

Analoge opmerkingen kunnen worden gemaakt over de samenstelling $p \leftrightarrow q$.

We kunnen samenstellingen weer opnieuw samenstellen en daarmee ingewikkelde constructies maken, zoals bijvoorbeeld

$(p \wedge q) \rightarrow r$

$(p \rightarrow q) \rightarrow p$

$(((\neg p) \rightarrow q) \wedge ((\neg q) \rightarrow p)) \leftrightarrow (p \leftrightarrow \neg q)$

die alle weer proposities zijn. Hierbij gebruiken we haakjes om de struktuur duidelijk te maken.
Veel haakjes zijn overbodig als er (bijvoorbeeld door de syntax) afspraken gemaakt worden over de prioriteit van de connectieven. Wij zullen hierover geen expliciete regels vastleggen, maar toch proberen zo weinig mogelijk haakjes te gebruiken. Zo schrijven we $p \rightarrow \neg q$ in plaats van $p \rightarrow (\neg q)$ omdat er geen verwarring mogelijk is. Daarentegen schrijven we wel $(\neg p) \rightarrow q$ in plaats van $\neg p \rightarrow q$.

Van dit soort combinaties kunnen we ook weer waarheidstafels maken: som weer alle mogelijkheden voor p en q systematisch op en bereken wat het resultaat is. Omdat we dat voor elk van de connectieven al hadden vastgelegd, ligt het resultaat voor elke daarmee opgebouwde combinatie ook vast.

In onze gewone taal komen nog andere connectieven voor dan alleen de zojuist behandelde. Zo kennen we bijvoorbeeld de uitdrukkingen

"noch ..., noch ..."
"òf ..., òf ..."
"wel ..., maar niet ..."

De waarheidstafel van een connectief dat twee proposities p en q verbindt, bestaat uit 4 regels. Er zijn dus 16 verschillende mogelijkheden om een waarheidstafel voor zo'n connectief te construeren: op elke plek kunnen we een 0 of een 1 zetten. Daaronder komen ook de connectieven voor die alleen iets doen met p of alleen iets met q of die helemaal onafhankelijk zijn van p en q. Van deze laatste soort zijn er twee, ze worden weergegeven door T en F. De waarheidswaarde van T is in alle gevallen 1, en de waarheidswaarde van F is in alle gevallen 0. De letters T en F zijn afkortingen voor true (waar) en false (onwaar). Je zou bijna denken dat T hetzelfde is als 1 en F hetzelfde is als 0. Dat is niet helemaal waar: T en F zijn proposities en 1 en 0 zijn waarden. Je kunt zeggen dat T en F horen tot de *syntax* van proposities, net zoals alle connectieven, en dat 0 en 1 de *semantiek* weergeven van respectievelijk F en T.

In de tabel hebben we maar 5 van de 16 mogelijkheden geëtaleerd, enerzijds omdat juist die de connectieven zijn waarvan men zich bedient in redeneringen, anderzijds omdat elke samengestelde propositie reeds kan worden geformuleerd met de connectieven $\wedge$, $\vee$ en $\neg$. Een paar voorbeelden:

$p \rightarrow q$ heeft dezelfde waarheidstafel als $(\neg p) \vee q$

"noch p, noch q" heeft dezelfde waarheidstafel als $(\neg p) \wedge \neg q$

We komen hier nog uitgebreid op terug.

2.3 Tautologieën

Sommige proposities zijn steeds waar, andere zijn soms waar en soms onwaar, afhankelijk van de situatie waarop ze betrekking hebben. Zo is "de brug is open" waar als de brug open is, en anders is deze uitspraak onwaar. Wanneer men in een computerprogramma twee variabelen x en y heeft, dan is de als test te gebruiken propositie "$x = y$" waar als x en y dezelfde waarde hebben, en anders onwaar. De propositie "$x = x$" is echter steeds waar.

Wat ons vooral interesseert zijn samengestelde proposities en hoe men aantoont dat een propositie steeds waar is. Bij een uit een klein aantal proposities p, q, r, ... samengestelde propositie A kan men gemakkelijk controleren of A steeds waar is door de waarheidstafel van A op te stellen en te kijken of de waarheidswaarde van A steeds 1 is. De elementaire bouwstenen p, q, r, ... heten wel *atomen* of *atomaire proposities*. Omdat elk atoom twee waarheidswaarden kan hebben, bestaat de waarheidstafel voor een propositie opgebouwd uit n atomen uit 2^n regels. Als $n = 3$ of $n = 4$ is dat nog best te doen, maar als n minstens 10 is praat je toch wel over meer dan duizend regels, en komt de vraag op of het niet met minder werk kan.

We zullen nu een manier aangeven om te manipuleren met samengestelde proposities, het vervangen van een propositie door een andere propositie met dezelfde betekenis. Met dergelijke manipulaties is het opstellen en nalopen van waarheidstafels vaak te vermijden.

Twee proposities A en B, beide opgebouwd uit p, q, r, ... , hebben dezelfde betekenis precies dan als $A \leftrightarrow B$ steeds waar is. Dit is hetzelfde als te zeggen dat de waarheidstafels van A en B aan elkaar gelijk zijn.

Definitie 2.7 Een *tautologie* is een steeds ware propositie, oftewel voor elke keuze van waarheidswaarden voor de erin voorkomende atomen is de waarheidswaarde van de propositie 1.
Twee proposities A en B heten *gelijkwaardig* of *equivalent* als $A \leftrightarrow B$ een tautologie is, oftewel voor elke keuze van waarheidswaarden voor de erin voorkomende atomen is de waarheidswaarde van A gelijk aan die van B.
We schrijven dan wel $A \equiv B$, of ook wel $A \Leftrightarrow B$.

Een propositie is dus een tautologie als hij gelijkwaardig is met T.

We maken een lijst van belangrijke tautologieën en een lijst van gelijkwaardige proposities, zodat we die niet telkens weer opnieuw hoeven te bewijzen. De in de lijsten voorkomende letters zijn atomen. Hiervoor mag men willekeurige concrete proposities invullen, onder de conditie dat voor hetzelfde atoom ook steeds dezelfde propositie wordt ingevuld.

Stelling 2.8 Alle proposities in de volgende lijst zijn tautologieën

1. $p \vee \neg p$
2. $\neg(p \wedge \neg p)$
3. $p \rightarrow (q \rightarrow p)$
4. $(\neg p) \rightarrow (p \rightarrow q)$
5. $(p \wedge \neg p) \rightarrow q$
6. $(p \leftrightarrow q) \rightarrow (p \rightarrow q)$
7. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
8. $(p \rightarrow q) \vee (q \rightarrow p)$
9. $(p \rightarrow q) \rightarrow ((q \rightarrow r) \rightarrow (p \rightarrow r))$
10. $((p \rightarrow q) \wedge (r \rightarrow s)) \rightarrow ((p \wedge r) \rightarrow (q \wedge s))$
11. $((p \rightarrow q) \vee (r \rightarrow s)) \rightarrow ((p \wedge r) \rightarrow (q \vee s))$
12. $((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \rightarrow (p \leftrightarrow r)$
13. T
14. $\neg\mathsf{F}$

Het lijkt een lange lijst, maar de regels 1 t/m 6 liggen nogal voor het oprapen. Regel 7 drukt uit dat implicatie *transitief* is

Hopelijk geven de regels 8 en 11 de lezer het gevoel dat het niet allemaal zo vanzelfsprekend is.

Een stelling is pas echt een stelling als er ook een bewijs bij is; in dit geval betekent dat dat we voor elke regel moeten bewijzen dat de genoemde propositie een tautologie is. Dat kunnen we met waarheidstafels doen: als we systematisch alle mogelijke combinaties van waarheidswaarden voor p, q en r en we zien dat de waarheidswaarde voor de propositie in alle gevallen 1 is, hebben we bewezen dat het een tautologie is. Dit doen we hier alleen voor regel 7; voor de overige regels gaat het op soortgelijke wijze en laten we het aan de lezer over. Voor regel 7 moeten we laten zien dat $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ een tautologie is, en daarvoor moeten we eerst de waarheidswaarden van $p \rightarrow q$, van $q \rightarrow r$, van $(p \rightarrow q) \wedge (q \rightarrow r)$ en van $p \rightarrow r$ bepalen. Dat zouden we afzonderlijk kunnen doen door hier aparte waarheidstafels van de maken, maar het kan ook in één keer met een grote waarheidstafel, waarin we onder de pijl van $p \rightarrow q$ de waarheidswaarde van $p \rightarrow q$ invullen, vervolgens onder de pijl van $q \rightarrow r$ de waarheidswaarde van $q \rightarrow r$, dan onder de $\wedge$ van $(p \rightarrow q) \wedge (q \rightarrow r)$ de waarheidswaarde van $(p \rightarrow q) \wedge (q \rightarrow r)$, dan onder de pijl van $p \rightarrow r$ de waarheidswaarde van $p \rightarrow r$, en tenslotte onder de resterende pijl de waarheidswaarde van de gehele propositie:

p	q	r	$((p \rightarrow q)$	$\wedge$	$(q \rightarrow r))$	$\rightarrow$	$(p \rightarrow r)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	0	1	1	0
1	0	1	0	0	1	1	1
1	1	0	1	0	0	1	0
1	1	1	1	1	1	1	1
						↑	

Inderdaad zien we in de met ↑ aangewezen kolom alleen maar enen staan, waarmee bewezen is dat de hele propositie een tautologie is.

In principe maakt de volgorde van de mogelijke combinaties van waarheidswaarden niet uit, als alle mogelijke combinaties maar opgesomd worden. Hier is de systematiek gevolgd waarbij bij het laatste atoom (r) afwisselend 0 en 1 is ingevuld, bij het voorlaatste (q) afwisselend twee nullen en twee enen, en daar weer voor (bij p) eerst vier nullen en dan vier enen. Dit breidt op een voor de hand liggende manier uit naar elk willekeurig aantal atomen: bij n atomen staan er in de eerste n kolommen de getallen van 0 tot en met $2^n - 1$ in *binaire notatie*.

2.4 Gelijkwaardige proposities

Stelling 2.9 In de volgende lijst zijn de proposities op eenzelfde regel gelijkwaardig

1.	p	$\neg(\neg p)$	$p \wedge p$	$p \vee p$
2.	$p \vee q$	$q \vee p$		
3.	$p \wedge q$	$q \wedge p$		
4.	$p \leftrightarrow q$	$q \leftrightarrow p$		
5.	$(p \vee q) \vee r$	$p \vee (q \vee r)$		
6.	$(p \wedge q) \wedge r$	$p \wedge (q \wedge r)$		
7.	$p \leftrightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow p)$	$(p \wedge q) \vee ((\neg p) \wedge \neg q)$	
8.	$p \rightarrow q$	$(\neg p) \vee q$		
9.	$p \rightarrow q$	$(\neg q) \rightarrow \neg p$		
10.	$\neg(p \rightarrow q)$	$p \wedge \neg q$		
11.	$\neg(p \vee q)$	$(\neg p) \wedge \neg q$		
12.	$\neg(p \wedge q)$	$(\neg p) \vee \neg q$		
13.	$(p \vee q) \rightarrow r$	$(p \rightarrow r) \wedge (q \rightarrow r)$		
14.	$p \rightarrow (q \wedge r)$	$(p \rightarrow q) \wedge (p \rightarrow r)$		
15.	$p \rightarrow (q \rightarrow r)$	$(p \wedge q) \rightarrow r$		
16.	$(p \vee q) \wedge r$	$(p \wedge r) \vee (q \wedge r)$		
17.	$(p \wedge q) \vee r$	$(p \vee r) \wedge (q \vee r)$		
18.	p	$p \vee \mathsf{F}$	$p \wedge \mathsf{T}$	
19.	$p \vee \neg p$	$p \vee \mathsf{T}$	T	
20.	$p \wedge \neg p$	$p \wedge \mathsf{F}$	F	

Regels 2, 3 en 4 geven aan dat de operatoren $\vee$, $\wedge$ en $\leftrightarrow$ *commutatief* zijn.
Regels 5 en 6 geven aan dat de operatoren $\vee$ en $\wedge$ *associatief* zijn.
Regel 8 geeft eigenlijk de definitie van de implicatie.
Regels 10, 11 en 12 laten zien hoe we met ontkenningen moeten omgaan. De regels 11 en 12 staan bekend als de wetten van *DeMorgan*.
Regel 9 geeft de wet van de *contrapositie*: om de waarheid van $p \rightarrow q$ vast te stellen, kan men even goed de waarheid van $(\neg q) \rightarrow \neg p$ vaststellen.
Regels 16 en 17 beschrijven dat $\wedge$ en $\vee$ *distributief* zijn, preciezer: regel 16 zegt dat $\wedge$ *distribueert over* $\vee$, en regel 17 zegt dat $\vee$ distribueert over $\wedge$. Regel 18 zegt dat F een

neutraal element voor $\vee$ is en dat T een neutraal element voor $\wedge$ is. Regels 19 en 20 geven nog enkele voor de hand liggende verbanden met T en F.

Van deze lijst is het handig om in ieder geval de regels 1 t/m 9, 11, 12 en 16 t/m 20 te kennen en altijd paraat te hebben.

Ook deze stelling kan zonder enig probleem worden bewezen door voor de onderhavige proposities de waarheidstafels op te stellen en te controleren dat de zaak klopt: steeds moet je laten zien dat proposities op dezelfde regel precies gelijke kolommen geven in de waarheidstafel.

Voor het toepassen van Stelling 2.9 zijn de volgende opmerkingen van groot belang:

- Voor p, q, r, ... mogen steeds willekeurige proposities worden ingevuld.
- De regels zijn niet alleen van toepassing op de hele uitdrukking, maar ook op delen daarvan. Zo mogen we uit $A \equiv B$ concluderen: $\neg A \equiv \neg B$, $p \vee A \equiv p \vee B$, $A \vee p \equiv B \vee p$, $p \wedge A \equiv p \wedge B$, et cetera.

Het op deze manier toepassen van Stelling 2.9 en andere spelregels van dit hoofdstuk wordt ook wel *propositierekening* genoemd.

Soms kan een regel ook worden bewezen uit een combinatie van andere regels.
Als voorbeeld laten we zien hoe regel 10 van Stelling 2.9 volgt uit andere regels door proposities te vervangen door gelijkwaardige proposities. Een dergelijk bewijs heet een *equationeel bewijs*.

$$\begin{array}{lcll} \neg(p \to q) & \equiv & \neg((\neg p) \vee q) & \text{(regel 8)} \\ & \equiv & (\neg(\neg p)) \wedge \neg q & \text{(regel 11)} \\ & \equiv & p \wedge \neg q & \text{(regel 1)} \end{array}$$

Op deze manier kunnen ook nieuwe gelijkwaardigheden worden afgeleid, bijvoorbeeld

$$\begin{array}{lcll} p \wedge (q \vee r) & \equiv & (q \vee r) \wedge p & \text{(regel 3)} \\ & \equiv & (q \wedge p) \vee (r \wedge p) & \text{(regel 16)} \\ & \equiv & (p \wedge q) \vee (r \wedge p) & \text{(regel 3)} \\ & \equiv & (p \wedge q) \vee (p \wedge r) & \text{(regel 3)} \end{array}$$

Door herhaaldelijk toepassen van de regels 2 en 5 van Stelling 2.9 kan men laten zien dat in $p \vee q \vee \cdots \vee r$ de haakjes willekeurig geplaatst mogen worden, en dat de volgorde er niet toe doet. Daarom laten we in samenstellingen met alleen het connectief $\vee$ vaak de haakjes weg.
Een analoge opmerking geldt voor $p \wedge q \wedge \cdots \wedge r$, hetgeen volgt door herhaaldelijk toepassen van de regels 3 en 6.

2.5 Speciale vormen

Aan het eind van sectie 2.2 hebben we aangekondigd dat elk connectief zich laat schrijven met behulp van de connectieven $\wedge$, $\vee$ en $\neg$. Inderdaad, laat A een propositie zijn, opgebouwd uit eindig veel p, q, r, ... Dan stellen we van A de waarheidstafel op, en kijken hoe de waarheidswaarden van p, q, r, ... moeten zijn opdat A de waarheidswaarde 1 heeft. We inventariseren die waarden met $\wedge$ en $\neg$ voor elke rij waarin voor A de waarde

1 staat. Het totaal wordt vervolgens samengevoegd met $\vee$. We krijgen op die manier vanzelf een uitdrukking in p, q, r, ... en $\wedge$, $\vee$, $\neg$ (en haakjes, uiteraard).
Als voorbeeld nemen we $A(p,q,r,s)$ met als waarheidstafel (we laten alleen de rijen zien waarin A de waarde 1 heeft)

p	q	r	s	A
1	0	1	1	1
0	1	0	1	1
1	0	0	1	1

Dan is $A(p,q,r,s)$ gelijkwaardig met

$$(p \wedge (\neg q) \wedge r \wedge s) \ \vee \ ((\neg p) \wedge q \wedge (\neg r) \wedge s) \ \vee \ (p \wedge (\neg q) \wedge (\neg r) \wedge s)$$

Dit is een zogenaamde *disjunctieve normaalvorm* van A, oftewel een disjunctie van een aantal conjuncties van literals. Hierbij wordt onder een *literal* verstaan een van de uitdrukkingen p, $\neg p$, q, $\neg q$, r, $\neg r$, ... , oftewel een atoom met al of niet een ontkenning ervoor.

Preciezer gezegd: een disjunctieve normaalvorm van een propositie opgebouwd uit de atomen p_1, p_2, ..., p_r is een equivalente propositie van de vorm $X_1 \vee X_2 \vee \ldots \vee X_s$, waarbij elke X_i van de vorm $(Y_1 \wedge Y_2 \wedge \ldots \wedge Y_{n_i})$ is, en elke Y_j van de vorm p_k of $\neg p_k$ is voor zekere k.

Een propositie kan meer dan één disjunctieve normaalvorm hebben: zo is $p \vee (q \wedge r)$ zelf al een disjunctieve normaalvorm, maar levert de methode met de waarheidstafel hiervoor een equivalente disjunctieve normaalvorm die een disjunctie van vijf conjuncten is.

Ook zonder gebruik te maken van waarheidstafels kan men een disjunctieve normaalvorm van een samengestelde propositie opstellen, namelijk via een equationeel bewijs. Dit kan heel systematisch door alleen de volgende equivalenties van links naar rechts toe te passen:

$$\begin{array}{lcl}
p \leftrightarrow q & \equiv & (p \wedge q) \vee ((\neg p) \wedge \neg q) \\
p \rightarrow q & \equiv & (\neg p) \vee q) \\
\neg(\neg p) & \equiv & p \\
\neg(p \vee q) & \equiv & (\neg p) \wedge \neg q \\
\neg(p \wedge q) & \equiv & (\neg p) \vee \neg q \\
p \wedge (q \vee r) & \equiv & (p \wedge q) \vee (p \wedge r) \\
(p \vee q) \wedge r & \equiv & (p \wedge r) \vee (q \wedge r).
\end{array}$$

Al deze regels komen voor of volgen direct uit Stelling 2.9. Desgewenst mogen we onderweg de betreffende uitdrukking nog vereenvoudigen door toepassing van regels 1, 18, 19 en 20 van Stelling 2.9. We geven een voorbeeld: we willen een disjunctieve normaalvorm van

$(p \leftrightarrow q) \wedge (q \rightarrow r)$ bepalen:

$$\begin{array}{rcl}
(p \leftrightarrow q) \wedge (q \rightarrow r) & \equiv & ((p \wedge q) \vee ((\neg p) \wedge \neg q)) \wedge (q \rightarrow r) \\
& \equiv & ((p \wedge q) \vee ((\neg p) \wedge \neg q)) \wedge ((\neg q) \vee r) \\
& \equiv & (p \wedge q \wedge ((\neg q) \vee r)) \vee ((\neg p) \wedge (\neg q) \wedge ((\neg q) \vee r)) \\
& \equiv & (p \wedge q \wedge \neg q) \vee (p \wedge q \wedge r) \vee ((\neg p) \wedge (\neg q) \wedge ((\neg q) \vee r)) \\
& \equiv & (p \wedge \mathsf{F}) \vee (p \wedge q \wedge r) \vee ((\neg p) \wedge (\neg q) \wedge ((\neg q) \vee r)) \\
& \equiv & \mathsf{F} \vee (p \wedge q \wedge r) \vee ((\neg p) \wedge (\neg q) \wedge ((\neg q) \vee r)) \\
& \equiv & (p \wedge q \wedge r) \vee ((\neg p) \wedge (\neg q) \wedge ((\neg q) \vee r)) \\
& \equiv & (p \wedge q \wedge r) \vee ((\neg p) \wedge (\neg q) \wedge (\neg q)) \vee ((\neg p) \wedge (\neg q) \wedge r) \\
& \equiv & (p \wedge q \wedge r) \vee ((\neg p) \wedge (\neg q)) \vee ((\neg p) \wedge (\neg q) \wedge r).
\end{array}$$

Een disjunctieve normaalvorm van $(p \leftrightarrow q) \wedge (q \rightarrow r)$ is dus

$$(p \wedge q \wedge r) \vee ((\neg p) \wedge (\neg q)) \vee ((\neg p) \wedge (\neg q) \wedge r).$$

Het kan nog korter: vanwege $((\neg p) \wedge (\neg q)) \vee ((\neg p) \wedge (\neg q) \wedge r) \equiv (\neg p) \wedge \neg q$ is ook $(p \wedge q \wedge r) \vee ((\neg p) \wedge \neg q)$ een disjunctieve normaalvorm van $(p \leftrightarrow q) \wedge (q \rightarrow r)$.

Door directe controle of door de regels 1 en 11 van Stelling 2.9 te combineren, ziet men dat $p \vee q$ gelijkwaardig is met $\neg((\neg p) \wedge \neg q)$.
Daarmee blijkt uit de disjunctieve normaalvorm dat elke propositie zelfs gelijkwaardig is met een uitdrukking in alleen $\neg$ en $\wedge$.
We laten het aan de lezer over om aan te tonen dat ook de paren $\vee$, $\neg$ en $\rightarrow$, $\neg$ voldoende zijn.

Het is zelfs mogelijk om te volstaan met één teken, bijvoorbeeld de *Sheffer stroke* p/q, die gelijkwaardig is met $\neg(p \wedge q)$. Immers voor dit connectief geldt

$\neg p$	is gelijkwaardig met	p/p,
$p \wedge q$	is gelijkwaardig met	$(p/q)/(p/q)$.

2.6 Opgaven

Opgave 2.1

Welke van de volgende uitspraken is een propositie en welke niet?

a. $7 + 7 = 13$.

b. $7 + 7 = 14$.

c. Er bestaan groene koeien.

d. Er bestaat leven op een andere planeet.

e. Het schilderij *De Nachtwacht* van Rembrandt is mooi.

f. Koningin Beatrix vindt het schilderij *De Nachtwacht* van Rembrandt mooi.

g. Het schilderij *De Nachtwacht* van Rembrandt is mooier dan het schilderij *De Zonnebloemen* van Van Gogh.

h. Het schilderij *De Nachtwacht* van Rembrandt is zwaarder dan het schilderij *De Zonnebloemen* van Van Gogh.

i. Deze zin bestaat uit meer dan twintig letters.

Opgave 2.2

Construeer de waarheidstafels van de volgende samengestelde proposities

a. $(p \wedge q) \wedge ((\neg q) \vee r)$

b. $p \rightarrow (q \vee r)$

c. $\neg((\neg p) \vee \neg((\neg q) \vee \neg p))$

d. $p \leftrightarrow (q \leftrightarrow r)$

e. $p \leftrightarrow (q \leftrightarrow p)$

Opgave 2.3

Kijk of de waarheidstafels voor de proposities in de vorige opgave aanleiding geven tot eenvoudigere gelijkwaardige samenstellingen.

Opgave 2.4

Bewijs met behulp van waarheidstafels dat

a. $((p \rightarrow q) \vee (r \rightarrow s)) \rightarrow ((p \wedge r) \rightarrow (q \vee s))$ een tautologie is

b. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ een tautologie is

c. $\neg(p \rightarrow \neg q)$ en $p \wedge q$ gelijkwaardig zijn

Opgave 2.5

Bewijs dat regels 13, 14 en 15 van Stelling 2.9 inderdaad gelijkwaardige proposities aangeven.

Opgave 2.6

Bewijs door uitsluitend gelijkwaardige proposities uit Stelling 2.9 door elkaar te vervangen, dat

a. $a \leftrightarrow b$ en $(\neg a) \leftrightarrow \neg b$ gelijkwaardig zijn

b. $((\neg a) \wedge \neg b) \rightarrow c$ en $(\neg a) \rightarrow (b \vee c)$ gelijkwaardig zijn

Opgave 2.7

a. Druk $(p \vee q) \wedge r$ uit met de connectieven $\rightarrow$ en $\neg$

b. Druk $(p \vee q) \wedge r$ uit met / als enige connectief

Opgave 2.8

Definieer het connectief $\downarrow$ door:

$$p \downarrow q \text{ is gelijkwaardig aan } \neg(p \vee q).$$

Dit connectief $\downarrow$ heet de *Quine dagger*.

a. Laat zien dat elk connectief uit te drukken is in alleen $\downarrow$.

b. Druk $(p \vee q) \wedge r$ uit met $\downarrow$ als enige connectief.

Opgave 2.9

Geef een disjunctieve normaalvorm van

a. $p \rightarrow (q \rightarrow r)$

b. $(p \vee q) \wedge r$

c. $(p \vee q) \wedge (r \vee q)$

d. $(p \wedge r) \rightarrow (q \wedge r)$

Opgave 2.10

Een *conjunctieve normaalvorm* van een propositie opgebouwd uit p_1, p_2, ..., p_r is een equivalente propositie van de vorm $X_1 \wedge X_2 \wedge \ldots \wedge X_s$, waarbij elke X_i van de vorm $(Y_1 \vee Y_2 \vee \ldots \vee Y_{n_i})$ is, en elke Y_j van de vorm p_k of $\neg p_k$ is voor zekere k.

a. Leid een conjunctieve normaalvorm van $\neg(p \rightarrow (q \rightarrow r))$ af uit een disjunctieve normaalvorm van $p \rightarrow (q \rightarrow r)$ (zie vorige opgave, deel a).

b. Geef een conjunctieve normaalvorm van $p \rightarrow (q \rightarrow r)$.

Hoofdstuk 3

Bewijzen met deductie

De stellingen 2.8 en 2.9 kunnen, zoals reeds opgemerkt, worden bewezen door voor de onderhavige proposities de waarheidstafels op te stellen en te controleren of de zaak klopt. Dit is echter soms wel erg bewerkelijk. Zo bevat de propositie op regel 10 van stelling 2.8 vier verschillende letters. De waarheidstafel van die propositie heeft dus maar liefst 16 ($= 2^4$) regels. Bovendien is die propositie tamelijk ingewikkeld, zodat er veel kolommen moeten worden ingevuld.

Soms kunnen we toe met aanzienlijk minder werk.

In wat nu volgt veronderstellen we dat A en B proposities zijn, opgebouwd uit p, q, r, ...
Dan hoeven we bijvoorbeeld voor de controle van de waarheid van $A \to B$ alleen te kijken naar waarheidswaarden van p, q, r, ... waarvoor A waar is, en voor die waarden te controleren of B waar is. Volgens de definitie is $A \to B$ immers altijd waar als A onwaar is. We formuleren dit als een apart principe.

> Als B waar is voor alle waarheidswaarden van p, q, r, ... waarvoor A waar is, dan is $A \to B$ een tautologie.

Dit heet het principe van *deductie*. Iets minder precies gezegd luidt dit principe:

> Als B waar is onder de veronderstelling dat A waar is, dan is $A \to B$ een tautologie.

Toch zullen we in het vervolg deze formulering vaker gebruiken, daarbij afsprekend dat de zinsnede "onder de veronderstelling dat" gelezen moet worden als

"voor alle waarheidswaarden van p, q, r, ... waarvoor"

Als illustratie bewijzen we regel 10 van Stelling 2.8.

te bewijzen: $((p \to q) \wedge (r \to s)) \to ((p \wedge r) \to (q \wedge s))$ is een tautologie.

BEWIJS:
B1 stel $(p \to q) \wedge (r \to s)$ is waar, dan

B2 $p \to q$ is waar (B1 en '$P \wedge Q$ waar, dan P waar')
B3 $r \to s$ is waar (B1 en '$P \wedge Q$ waar, dan Q waar')
B4 te bewijzen: $(p \wedge r) \to (q \wedge s)$ is waar
BEWIJS van B4:
B4.1 stel $p \wedge r$ is waar, dan
B4.2 p is waar (B4.1 en '$P \wedge Q$ waar, dan P waar')
B4.3 r is waar (B4.1 en '$P \wedge Q$ waar, dan Q waar')
B4.4 q is waar (B4.2, B2 en 'P en $P \to Q$ waar, dan Q waar')
B4.5 s is waar (B4.3, B3 en) 'P en $P \to Q$ waar, dan Q waar')
B4.6 $q \wedge s$ is waar (B4.4, B4.5 en 'P en Q waar, dan $P \wedge Q$ waar')
EINDE BEWIJS van B4 (wegens deductie)
EINDE BEWIJS (wegens deductie)

Dit ziet er op het eerste gezicht een beetje raar uit, maar het is niet meer dan een voor de hand liggende logische redenering die in heel veel detail is opgeschreven. De basisstructuur is het toepassen van het deductieprincipe: als we een *bewijs* moeten geven dat $P \to Q$ een tautologie is, beginnen we met een regel 'stel P', en proberen vanuit dat gegeven te bewijzen dat Q geldt. Als dat lukt is daarmee het gevraagde bewezen. In zo'n redenering noemen we dan ook P de *veronderstelling* en Q de *conclusie*. Hierin kunnen P en Q zelf weer net zulke ingewikkelde proposities zijn als je zelf wilt. Verder is het bewijs opgebouwd in een aantal regels. Elke regel is zelf weer een bewering die waar is op grond van wat je op dat moment weet. Als het op een regel past, staat het waarom van de geldigheid van die bewering er tussen haakjes achter, anders is er weer een apart *subbewijs* voor nodig. In die verantwoording mag men refereren aan eerder gemaakte afspraken of stellingen of axioma's, of aan *eerder in het bewijs opgeschreven* proposities. Om deze laatste referenties goed te kunnen aangeven, worden de verschillende regels *genummerd*. Ook de stappen in een subbewijs worden genummerd met als *prefix* het nummer van de te bewijzen propositie. Zo kun je aan dat nummer precies zien waar je bent: zo is B3.2.4 een bewering die je doet binnen het bewijs van bewering B3.2, welke op zijn beurt weer voorkomt binnen het bewijs van bewering B3. Het is in principe niet nodig om elke bewering zo'n identificatie mee te geven, maar omdat we van te voren niet weten naar welke beweringen we later nog zullen gaan verwijzen, geven we voorlopig voor de zekerheid elke propositie in een bewijs maar zo'n nummer mee.

Bij de verantwoording van de stappen in een subbewijs mag ook worden gerefereerd aan de eerder in het grote bewijs opgeschreven proposities, met uitzondering van de te bewijzen propositie. Verder mag in het grote bewijs niet worden gerefereerd aan proposities in een eerder subbewijs: als je binnen een subbewijs 'stel P' gezegd heb, mag je na het afsluiten van het subbewijs niet aannemen dat P nog steeds geldt. Deze spelregels vatten we samen in de *scope-regels voor referentie*:

> In de verantwoording van regel B$n_1.n_2 \ldots n_r$ ($r \geq 1$) mag worden gerefereerd aan regel B$m_1.m_2 \ldots m_s$ ($s \geq 1$), mits elk van de volgende drie voorwaarden vervuld is:
>
> 1. $s \leq r$
> 2. $m_s < n_s$ (echt kleiner)

3. als $s > 1$, dan moet $m_k = n_k$ gelden voor alle k die voldoen aan $1 \leq k < s$

Het begrip *scope* heet in het Nederlands ook wel *bereik*.

We geven enkele voorbeelden:

B4	refereert aan B2	goed
B4.3.5	refereert aan B4.3.3	goed
B4.3.5	refereert aan B4.2	goed
B4.3.5	refereert aan B3	goed
B4.3.5	refereert aan B4.3	fout, wegens voorw.2
B4.3.5	refereert aan B6	fout, wegens voorw.2
B4.3.5	refereert aan B4	fout, wegens voorw.2
B4.3.5	refereert aan B3.2.1	fout, wegens voorw.3
B4.3.5	refereert aan B4.3.5	fout, wegens voorw.2
B4.3.5	refereert aan B4.3.5.1	fout, wegens voorw.1

De scope-regels voor referentie lijken dus veel op de scope-regels in een programmeertaal met betrekking tot de variabelen.

3.1 Afleidingsregels

In het gegeven bewijs hebben we in de motivaties voor de stappen de volgende spelregels geformuleerd en gebruikt:

- als $P \wedge Q$ waar is, dan is P waar
- als $P \wedge Q$ waar is, dan is Q waar
- als P en $P \rightarrow Q$ waar zijn, dan is Q waar
- als P en Q waar zijn, dan is $P \wedge Q$ waar

Dit zijn allemaal regels waarvan iedereen op zijn klompen aanvoelt dat het wel klopt, maar het is toch goed en handig om een zo volledig mogelijke lijst op te stellen van zogenaamde *afleidingsregels* die mogen worden gebruikt. We zullen ook elke regel een naam geven, zodat we in motivaties in bewijzen alleen die naam hoeven te noemen in plaats van de hele regel zelf op te schrijven.

Voor de afleidingsregels gebruiken we de volgende notatie.

$$A,\ B, \ldots \ \vdash \ C,\ D, \ldots$$

dient als volgt gelezen te worden: als *elk* van de proposities *links* van $\vdash$ waar is of verondersteld wordt waar te zijn, dan mag de waarheid van elke propositie *rechts* van $\vdash$ geconcludeerd worden.

Een andere veel gebruikte notatie voor hetzelfde doel is de conclusiestreep

$$\frac{A, B, \ldots}{C, D, \ldots} \text{ betekent hetzelfde als } A, B, \ldots \ \vdash \ C, D, \ldots$$

Dan geven we nu de lijst afleidingsregels.

- *deductie*:
  (sub)bewijs beginnend met A (veronderstelling) en eindigend met B
  $\vdash \quad A \to B$
- *modus ponens*:
  $A,\ A \to B \ \vdash \ B$
- *introductie* $\wedge$:
  $A,\ B \ \vdash \ A \wedge B,\ B \wedge A$
- *eliminatie* $\wedge$:
  $A \wedge B \ \vdash \ A,\ B$
- *introductie* $\vee$:
  $A \ \vdash \ A \vee B,\ B \vee A$
- *eliminatie* $\vee$:
  $A \vee B,\ A \to C,\ B \to C \ \vdash \ C$
- *introductie* $\leftrightarrow$:
  $A \to B,\ B \to A \ \vdash \ A \leftrightarrow B$
- *eliminatie* $\leftrightarrow$:
  $A \leftrightarrow B \ \vdash \ A \to B,\ B \to A$
- *introductie* $\neg$:
  $B \to \mathsf{F} \ \vdash \ \neg B$
- *introductie false*:
  $A,\ \neg A \ \vdash \ \mathsf{F}$
- *eliminatie false*:
  $\mathsf{F} \ \vdash \ A$
- *gevalsonderscheid*:
  $\vdash \ A \vee \neg A$

Op deze wijze hebben we voor elk van de connectieven een introductieregel waarmee een propositie *bewezen* kan worden waarin dat connectief voorkomt, en voor elk van de binaire connectieven een eliminatieregel waarmee een propositie *gebruikt* kan worden waarin dat connectief voorkomt. Hierin speelt deductie de rol van *introductie* $\to$ en modus ponens de rol van *eliminatie* $\to$. Om historische redenen gebruiken we echter de begrippen deductie en modus ponens.

In plaats van de regel *gevalsonderscheid* hadden we ook een regel $\vdash \mathsf{T}$ kunnen invoeren onder de naam *introductie true* en een regel $\mathsf{T} \vdash A \vee \neg A$ onder de naam *eliminatie true*. Deze regels worden echter voornamelijk in combinatie gebruikt, en daarom hebben we de

combinatie gelijk maar als regel ingevoerd. Zo kan hij vaak handig kan worden gebruikt, in het bijzonder om 'eliminatie $\vee$' te kunnen toepassen: als we $A \to C$ en $\neg A \to C$ hebben afgeleid, kunnen we met deze regel en 'eliminatie $\vee$' concluderen dat dan ook C geldt. Hiermee is C in feite bewezen door een gevalsonderscheid tussen A en $\neg A$ te maken; vandaar dat we de regel *gevalsonderscheid* hebben genoemd. Omdat er bij deze regel niets voor het $\vdash$-symbool staat mogen we hem op elk gewenst moment voor elke zelf te kiezen A toepassen.

Er zijn nog wel meer regels te verzinnen. In zijn algemeenheid geldt dat als $A \to B$ een tautologie is, dat dan

$$A \quad \vdash \quad B$$

ook als geldige afleidingsregel toegevoegd zou mogen worden. We beperken ons echter tot de hier gegeven lijst.

De systematiek van de lijst kun je opvatten als hulpmiddel om een bewijs te vinden. Zo word je gedwongen de bijbehorende introductieregel toe te passen als je de geldigheid van een bepaalde propositie wilt bewijzen. Preciezer gezegd:

- Als je de geldigheid van $A \to B$ wilt bewijzen, moet je deductie toepassen, oftewel je begint met A te stellen en moet vervolgens B bewijzen.
- Als je de geldigheid van $A \wedge B$ wilt bewijzen, moet je introductie $\wedge$ toepassen, oftewel je moet zowel A als B bewijzen.
- Als je de geldigheid van $A \vee B$ wilt bewijzen, moet je introductie $\vee$ toepassen, oftewel je moet A bewijzen of B bewijzen.
- Als je de geldigheid van $\neg A$ wilt bewijzen, moet je introductie $\neg$ toepassen, oftewel je moet $A \to \mathsf{F}$ bewijzen, en dat moet je weer met deductie doen. In feite geef je hiermee een *bewijs uit het ongerijmde*.

Als voorbeeld bewijzen we, uitsluitend gebruik makend van deze afleidingsregels:

te bewijzen: $(p \to q) \to ((\neg p) \vee q)$ is een tautologie

BEWIJS:
B1 $p \to q$ (veronderstelling)
B2 $p \vee \neg p$ (gevalsonderscheid)
B3 te bewijzen: $p \to ((\neg p) \vee q)$
BEWIJS van B3:
B3.1 p (veronderstelling)
B3.2 q (B3.1, B1, modus ponens)
B3.3 $(\neg p) \vee q$ (B3.2, intr. $\vee$)
EINDE BEWIJS van B3 (deductie)
B4 te bewijzen: $(\neg p) \to ((\neg p) \vee q)$
BEWIJS van B4:
B4.1 $\neg p$ (veronderstelling)
B4.2 $(\neg p) \vee q$ (B4.1, intr. $\vee$)
EINDE BEWIJS van B4 (deductie)

B5 $(\neg p) \vee q$ (B2, B3, B4, elim. $\vee$)
EINDE BEWIJS (deductie)

Het is geenszins de bedoeling van dit hoofdstuk om een keurslijf van exacte, doch cryptisch opgeschreven bewijzen op te dringen. Integendeel, een in goed Nederlands opgeschreven heldere redenering heeft het grote voordeel dat iedereen het kan volgen. Vaak echter schiet het gewone taalgebruik te kort om een argumentatie in weinig woorden waterdicht te maken. Juist in die gevallen is een strak systeem van groot nut. Wel geldt uiteraard bij alle bewijzen dat ze moeten voldoen aan de hier gegeven spelregels, ook als de verschillende beweringen niet expliciet genummerd zijn. De hier gegeven spelregels zijn niet gegeven om het je moeilijk te maken, maar zijn een weerslag van de consensus over wat correcte en geldige redeneringen zijn, en hopen juist een hulpmiddel te zijn om dergelijke redeneringen gestructureerd te kunnen geven.

In de praktijk zal men veelal conclusies trekken, zonder de verantwoording tot in de allerkleinste details op te schrijven. Men geeft dan alleen de grote lijnen weer. Op zich is dat niet erg, het hoort bij de ontwikkeling tot beoefenaar van een vak. Naarmate die ontwikkeling vordert worden steeds complexere combinaties tot een geheel. Hierin schuilen uiteraard wel grote gevaren voor vergissingen! Probeer nooit een bewijs zo "uit te dunnen" dat je zelf na een paar dagen moeite hebt om te zien "hoe het ook weer zat".

3.2 Subbewijzen en hulpstellingen

Een *subbewijs* binnen een groter bewijs heeft als nadeel dat het binnen dat grote bewijs soms veel ruimte kost, waardoor men het overzicht verliest. Bovendien moet men erg oppassen dat de scope-regels niet worden overtreden. Indien gewenst, kan men een subbewijs weghalen en vervangen door een aparte stelling. Dit gaat als volgt. Stel dat een bewijs er uitziet als

```
. .   . .
10    A
. .   . .
15    X
      BEWIJS van 15:
      15.1   . .
      . . .  . .
      EINDE BEWIJS van 15
16    . .
. .   . .
```

waarbij in het bewijs van regel 15 wordt gerefereerd aan regel 10, maar niet aan een andere regel buiten dat subbewijs. Dan kan men als volgt een zelfstandige *hulpstelling* of *lemma* maken.

HULPSTELLING: $A \rightarrow X$
BEWIJS:
1. A (veronderstelling)
2. {Schrijf nu hier in regel $n+1$ de oorspronkelijke regel
. . $15.n$ op, waarbij elke referentie naar 10 wordt vervangen
. . door een referentie naar 1, en elke referentie naar $15.m$
. . door een referentie naar $m+1$}
EINDE BEWIJS HULPSTELLING.

Nu kan het oorspronkelijke bewijs vanaf regel 15 als volgt worden gemodificeerd:

. . . .
10 A
. . . .
15 $A \rightarrow X$ (hulpstelling)
16 X (10 en 15, met 4.7.1) {dit is oude regel 15}
17 {vanaf hier komen de oude regels vanaf 16, waarbij elk
. . regelnummer met 1 wordt opgehoogd en elke verwijzing
. . naar een regel n met $n \geq 15$ wordt vervangen door een
. . verwijzing naar regel $n+1$}

We hebben de deductie hier ingevoerd via een subbewijs, dat de status heeft van een verantwoording *na* de bewering $A \rightarrow B$. Dit heeft het voordeel dat een veronderstelling nooit zomaar uit de lucht komt vallen, maar het heeft aan de andere kant het nadeel dat de bewering $A \rightarrow B$ wordt gedaan *voordat* hij bewezen wordt, evenwel voor de duidelijk voorzien van 'te bewijzen'.
Een andere notatie van bewijzen (onder andere gebruikt in het vak Formele Methoden) concludeert de bewering $A \rightarrow B$ pas *nadat* het bewijs daarvan is geleverd. Om dan aan te geven dat het toch een subbewijs betreft waaraan verder niet mag worden gerefereerd, zet men een dergelijk subbewijs tussen grote haken.

Dit idee van een subbewijs weghalen en vervangen door een aparte stelling heeft een sterke analogie met programmeren: in een groot stuk programma is het vaak ook handig om van een stuk daarvan een aparte *procedure* te maken; in objectgeörienteerde terminologie heet dat een aparte *methode*. Er zijn verschillende argumenten waarom je dat zou willen doen:

- door conceptueel bij elkaar horende onderdelen af te zonderen wordt het geheel overzichtelijker;
- het afgezonderde gedeelte kan ook afzonderlijk en vanuit andere plekken worden gebruikt.

Verder is het een goed streven de opzet zo te maken dat je het afgezonderde gedeelte zo algemeen mogelijk kunt gebruiken. Deze principes zijn zowel van toepassing bij de opzet van een groot bewijs als bij de opzet van een groot programma.

In onze notatie van bewijzen met deductie schrijven we eerst de bewering $A \to B$ en geven daarna pas het bewijs. Hierbij moeten we ons goed realiseren dat we $A \to B$ nog moeten bewijzen en nog niet mogen gebruiken, zoals we ook al bij de scope-regels hebben geformuleerd. Om dit extra duidelijk te maken schrijven we op:

$$\text{te bewijzen: } A \to B$$

Verder is het wel gebruikelijk om zo'n bewijs dan te beginnen met

$$\text{stel } A$$

in plaats van de motivatie 'veronderstelling' er tussen haakjes achter te zetten. Vooral als bewijzen in woorden worden gegeven in plaats van genummerde regels wemelt het vaak van 'te bewijzen' en 'stel'.

3.3 Opgaven

Om de techniek van deductieve bewijzen te oefenen, mogen in de volgende opgaven geen waarheidstafels, gelijkwaardigheden of tautologieën worden gebruikt. Men make uitsluitend gebruik van de in dit hoofdstuk gegeven afleidingsregels.

Opgave 3.1

Bewijs dat $(p \to q) \to ((p \wedge r) \to (q \wedge r))$ een tautologie is.

Opgave 3.2

Bewijs dat $((p \to q) \wedge (q \to r)) \to (p \to r)$ een tautologie is.

Opgave 3.3

Bewijs dat $((p \to q) \wedge (r \to s) \wedge p \wedge r) \to (q \wedge s))$ een tautologie is.

Opgave 3.4

Bewijs dat $((p \to q) \wedge (p \to \neg q)) \to \neg p$ een tautologie is.

Opgave 3.5

Bewijs dat $(\neg p) \to (p \to q)$ een tautologie is.

Opgave 3.6

Bewijs dat $(p \to q) \to ((\neg q) \to \neg p)$ een tautologie is.

Opgave 3.7

Bewijs dat $((\neg p) \leftrightarrow q) \to \neg(p \leftrightarrow q)$ een tautologie is.

Hoofdstuk 4

Predicaten

Tot nu toe hebben we ons beziggehouden met proposities, en gezien hoe we daarmee moeten omgaan. Proposities zijn echter niet toereikend om daarin alle overwegingen te formuleren waarvan we gebruik willen maken. Als voorbeeld komen we terug op de postbode uit het eerste hoofdstuk. De redenering begon als volgt:

Stel dat de bewering

er is een adres waarop vier of meer stukken zijn afgeleverd

niet waar is, dan geldt:

voor alle adressen zijn er hoogstens drie stukken afgeleverd.

Voor het redeneren met *vier of meer* en *hoogstens drie* kunnen we gewone rekenregels voor getallen toepassen, maar voor het redeneren met *er is een* en *voor alle* hebben we nog niets En dat is precies wat we in dit hoofdstuk gaan doen.

Definitie 4.1 We schrijven

$$\exists x \langle P \rangle$$

voor:

er is een x zo dat P geldt,

en we schrijven

$$\forall x \langle P \rangle$$

voor:

voor elke x geldt P.

Hierin mag P een willekeurige bewering zijn waar x in voor mag komen.
De tekens $\forall$ en $\exists$ heten *quantoren*,
$\forall$ heet de *universele quantor*, en
$\exists$ heet de *existentiële quantor*.

4.1 Vrij en gebonden, universum

Eerst moeten we wat meer vertrouwd raken met het gebruik van de notaties $\forall x\langle P\rangle$ en $\exists x\langle P\rangle$.

Iedere quantor wordt gevolgd door een variabele (bijvoorbeeld $\forall x$, of $\exists y$). Meestal is de uitspraak P waarop de quantificering betrekking heeft zelf van een vorm die aan een propositie doet denken. Het essentiële verschil met een propositie is echter dat er in P *variabelen* kunnen optreden die staan voor *verschillende objecten*.

We herinneren er nog eens aan dat een propositie gekenmerkt wordt doordat hij waar of onwaar is.
$2 > 1$ is een propositie, evenals $1 > 2$, maar $x > 1$ is geen propositie, immers we kunnen niet uitmaken of $x > 1$ waar is. Dat hangt van de waarde van x af. De aanwezigheid van variabelen verstoort dus het propositie-karakter.

Definitie 4.2 Door $\forall x\langle P\rangle$ worden de in P eventueel voorkomende variabelen x *gebonden* door de quantor $\forall$.
Een niet door een quantor gebonden variabele in een uitspraak heet een *vrije variabele* in die uitspraak. De vrije variabelen in $\forall x\langle P\rangle$ zijn dus de vrije variabelen in P, met uitzondering van x.
Het voorgaande geldt ook met betrekking tot $\exists$.
Een *predicaat* is een uitspraak die waar of niet waar kan zijn, en waarin vrije variabelen en quantoren mogen optreden.

Het verschijnsel van *gebonden variabelen* komt in vele andere onderwerpen ook voor, bijvoorbeeld bij integralen en bij het declareren van variabelen in computerprogramma's. In een formule zoals

$$\int_a^b f(x)dx$$

is x gebonden, a en b zijn vrij, het maakt niets uit als we x vervangen door v (in $f(x)$ en in dx). Ook bij de quantoren betekent bijvoorbeeld $\exists x\langle x \neq 0\rangle$ hetzelfde als $\exists v\langle v \neq 0\rangle$.

Er zijn hier weer *scope-regels*: in $\int_a^b f(x)dx$ slaat de x in dx alleen op de variabelen x die voorkomen tussen de tekens $\int$ en d, en in $\exists x\langle x \neq 0\rangle$ slaat de x in $\exists x$ alleen op de variabelen x die die voorkomen tussen de tekens $\langle$ en $\rangle$.

Het gebruik van een variabele in een predikaat of bij een quantor heeft alleen zin als we van te voren afspreken welke de mogelijke objecten zijn waarop zo'n variabele betrekking heeft (het *type* van de variabele). De verzameling van die objecten noemen we het *universum*. Wil men iets zeggen over gehele getallen, dan ligt het voor de hand om als universum de verzameling der gehele getallen te kiezen. Het kan ook zijn dat iemand alleen maar geïnteresseerd is in uitspraken over autobanden, of alleen maar in uitspraken over priemgetallen, of alleen maar in uitspraken over reële getallen, of alleen maar in uitspraken over de informaticastudenten die in 1998 met hun studie zijn begonnen.
In het laatste geval betreft het een *eindig* universum. Dan kunnen we eventueel ook zonder quantoren toe.

Laten we bijvoorbeeld eens aannemen dat het universum bestaat uit de getallen 1, 2, 3 en dat $P(x)$ een predikaat is dat een betekenis heeft als men voor x respectievelijk 1, 2 of 3 invult, denk bijvoorbeeld aan $P(x) := (x^2 - 2x = 0)$.
Dan betekent $\exists x\langle P(x)\rangle$ hetzelfde als $(1 - 2 = 0 \vee 4 - 4 = 0 \vee 9 - 6 = 0)$,
en betekent $\forall x\langle P(x)\rangle$ hetzelfde als $(1 - 2 = 0 \wedge 4 - 4 = 0 \wedge 9 - 6 = 0)$.

Hieruit zien we dat $\exists$ een generalisatie is van $\vee$ en dat $\forall$ een generalisatie is van $\wedge$.

In verschillende boeken zie je soms variaties op de hier gebruikte notatie. De notatie $\forall$ en $\exists$ is wel algemeen in gebuik. In een grijs verleden is wel eens geprobeerd om hiervoor respectievelijk $\wedge$ en $\vee$ te gebruiken omdat het inderdaad generalisaties van conjunctie en disjunctie zijn, maar dat heeft het nooit echt gehaald. In de nostalgische tijd van de schrijfmachines is wel eens **A** gebruikt voor $\forall$ en **E** voor $\exists$, maar ook dat is lang geleden. Als historisch verantwoord ezelsbruggetje is het wel aardig: $\forall$ is een omgekeerde A van 'alle', en $\exists$ is een omgekeerde E van 'existentie', 'er is een'.

De variatie in de notatie zit hem in de haakjes. Wij gebruiken $\langle$ en $\rangle$ omdat dat soorten haakjes zijn die we verder nauwelijks tegenkomen, en dus zo weinig mogelijk verwarring op kan leveren. Maar alle mogelijke soorten haakjes zijn hiervoor in omloop. Soms zie je ook helemaal geen haakjes, en zie je $\forall x : P$ of $\forall x \cdot P$ in plaats van $\forall x\langle P\rangle$. Hier is een waarschuwing echter wel op zijn plaats: door het ontbreken van het sluithaakje is het niet altijd duidelijk waar de *scope* van de variabele x afgelopen is: tot hoever in de uitdrukking is elke x gebonden door deze quantor $\forall$? In onze notatie geeft '$\rangle$' precies het eind van de *scope* aan; we komen hier nog op terug.

Variatie in notatie is er ook in het aangeven van het universum. Vooruitlopend op de notatie $\in$ uit de verzamelingenleer zoals we die in de komende hoofdstukken ook zullen gebruiken, schrijven wij

$$\forall x \in U\langle P\rangle \quad \text{en} \quad \exists x \in U\langle P\rangle$$

om expliciet aan te geven dat U het universum van x is. Als uit de situatie duidelijk is wat het universum is, laten we het gewoon weg.

Als er in een uitspraak meerdere quantoren in een groep bij elkaar staan, laten we overbodige haakjes wel eens weg. Voorbeelden hiervan zijn

$$\forall x\exists y\langle x < y\rangle \qquad \exists x\forall y\langle x < y\rangle \qquad \exists x\exists y\langle x < y\rangle \qquad \forall x\forall y\langle x < y\rangle$$

Dan betekenen deze uitspraken respectievelijk

$$\forall x\langle\exists y\langle x < y\rangle\rangle \qquad \exists x\langle\forall y\langle x < y\rangle\rangle \qquad \exists x\langle\exists y\langle x < y\rangle\rangle \qquad \forall x\langle\forall y\langle x < y\rangle\rangle$$

Als de quantoren gemengd voorkomen, dus $\forall$ gevolgd door $\exists$ of omgekeerd, dan hangt de betekenis sterk af van de volgorde waarin ze voorkomen. Immers de eerste zin is duidelijk waar: neem voor y maar $x+1$. Daarentegen is de tweede zin duidelijk niet waar: er bestaat geen getal dat kleiner is dan alle getallen.
In groepjes van quantoren van dezelfde soort mag men wel naar believen de volgorde verwisselen. Zo hebben in het volgende lijstje de uitdrukkingen op dezelfde regel dezelfde betekenis

$$\begin{array}{lll}
\forall x\forall y\forall z\langle P\rangle & \forall y\forall x\forall z\langle P\rangle & \forall z\forall y\forall x\langle P\rangle \\
\forall x\forall y\exists z\langle P\rangle & \forall y\forall x\exists z\langle P\rangle & \\
\forall x\forall y\exists z\forall u\forall v\langle P\rangle & \forall x\forall y\exists z\forall v\forall u\langle P\rangle & \\
\exists x\exists y\exists z\forall u\forall v\langle P\rangle & \exists z\exists y\exists x\forall v\forall u\langle P\rangle &
\end{array}$$

Van deze verwisselingsmogelijkheid maakt men gebruik bij het "vertalen" van zo'n uitdrukking naar gewoon Nederlands. We geven weer een paar voorbeelden:

$\forall x \forall y \exists z \forall u \forall v \langle P \rangle$ wordt
"Voor elke x en y is er een z zo dat voor elke u en v uitspraak P geldt"

$\exists x \exists y \exists z \forall u \forall v \langle P \rangle$ wordt
"Er zijn x, y en z zo dat voor elke u en v uitspraak P geldt"

Soms wordt ook wel kortweg '$\forall x, y$' geschreven in plaats van '$\forall x \forall y$', en wordt '$\exists x, y$' geschreven in plaats van '$\exists x \exists y$'.

De zaken kunnen behoorlijk ingewikkeld worden, wanneer er in een uitspraak quantoren voorkomen die niet alle vooraan in een groepje staan. Men kan dan situaties krijgen zoals

$$\forall x \langle x > 2 \rightarrow \exists y \langle y < 7 \rangle \rangle \quad \text{of} \quad \forall x \langle x > 2 \rightarrow \exists x \langle x < 7 \rangle \rangle$$

Beide bovenstaande uitdrukkingen hebben dezelfde betekenis!

Dit komt omdat $\exists y \langle y < 7 \rangle$ een uitdrukking is waarin y naar buiten toe geen rol vervult. Immers $\exists y \langle y < 7 \rangle$ heeft dezelfde betekenis als $\exists z \langle z < 7 \rangle$ en ook dezelfde betekenis als $\exists x \langle x < 7 \rangle$. De variabele x in $x < 7$ wordt gebonden door $\exists x$, en daarmee is $\exists x \langle x < 7 \rangle$ een *gesloten uitdrukking* voor x. We moeten dus een aanvulling geven op definitie 4.2:

Door $\forall x \langle P \rangle$ en $\exists x \langle P \rangle$ worden alleen de *vrij voorkomende* x-en in P gebonden.

Vanzelfsprekend geeft het grote kans op verwarring wanneer in een predikaat eenzelfde letter voorkomt als vrije en tevens als gebonden variabele. Daarom raden we ten sterkste aan om als eerste aktie bij het bestuderen van een uitdrukking die quantoren bevat, ervoor te zorgen dat alle quantoren quantificeren over verschillende variabelen. Daartoe moeten we eventueel de vrij voorkomende x-en binnen de *scope* (het *bereik*) van $\exists x$ respectievelijk van $\forall x$ vervangen door een nog niet gebruikte letter, zeg z, en dan uiteraard ook schrijven $\exists z$ respectievelijk $\forall z$. Dit proces heet *herbenoemen* van variabelen, in het Engels *renaming*. Omdat de gekozen naam van zo'n gebonden variabele er blijkbaar niet toe doet, heet zo'n variabele ook wel een *dummy*.

Hier zien we een sterke analogie met computerprogramma's waar in een procedure gebruikte lokale variabelen niet bekend zijn buiten die procedure, maar waar het voor de menselijke lezer prettig is als er geen lokale en globale variabelen optreden onder dezelfde naam.

Als S een deel van het universum is, dan hebben

$$\forall x \in S \langle P \rangle \quad \text{en} \quad \exists x \in S \langle P \rangle,$$

respectievelijk dezelfde betekenis als

$$\forall x \langle (x \in S) \rightarrow P \rangle \quad \text{en} \quad \exists x \langle (x \in S) \wedge P \rangle$$

In de praktijk hebben de notaties $\forall x \in S\ \langle P \rangle$ en $\exists x \in S\ \langle P \rangle$ het belangrijke voordeel dat meteen duidelijk is van welk type x is (tot welke verzameling we ons kunnen beperken).

Er zijn twee speciale gevallen met betrekking tot het universum die we expliciet willen noemen, namelijk het geval dat het universum leeg is, en het geval dat de door een quantor gebonden variabele niet vrij voorkomt in het predikaat.
Is het universum leeg, dan is $\forall x\ \langle P \rangle$ waar en is $\exists x\ \langle P \rangle$ onwaar, onafhankelijk van het predikaat P.
Is het universum niet leeg, en is P een predikaat waarin de variabele x niet vrij voorkomt, dan zijn $\forall x\ \langle P \rangle$ en $\exists x\ \langle P \rangle$ beide equivalent met P.
Meestal zullen we aannemen dat het universum niet leeg is.

De hele machinerie van predikaten, quantoren enz. is opgezet om op een systematische manier te kunnen redeneren. Daarbij is de manier van opschrijven van groot belang. Wij hebben gekozen voor de zogenaamde *prefixnotatie* voor quantoren, dat wil zeggen dat quantoren voor de uitspraak staan. Soms zet men in een slordige bui de quantoren achter de uitspraak, als "afterthought" als het ware. We zien dan uitspraken als

$$x^2 \geq 0 \qquad (\forall x)$$

We raden ten sterkste aan om dit te vermijden, aangezien de binding tussen de twee x-en verloren gaat, en de betekenis afgeleid moet worden uit de typografische vormgeving ($\forall x$ staat op dezelfde regel als $x^2 \geq 0$). Beter is het in zo'n geval te schrijven

$$x^2 \geq 0 \text{ is geldig voor alle } x$$

zodat de betekenis uit het zinsverband blijkt.
Nog beter is natuurlijk

$$\text{voor alle } x \text{ geldt } x^2 \geq 0.$$

4.2 Gelijkwaardige predicaten

Behalve de al genoemde regels over de volgorde van quantoren, zijn er nog andere rekenregels die van groot nut zijn. We maken een lijst van gelijkwaardige uitdrukkingen

Stelling 4.3 In de volgende lijst zijn de uitdrukkingen op eenzelfde regel gelijkwaardig

1.	$\forall x\langle \neg P \rangle$	$\neg \exists x \langle P \rangle$
2.	$\exists x\langle \neg P \rangle$	$\neg \forall x \langle P \rangle$
3.	$\forall x\langle P \wedge Q \rangle$	$\forall x\langle P \rangle \wedge \forall x \langle Q \rangle$
4.	$\exists x\langle P \vee Q \rangle$	$\exists x\langle P \rangle \vee \exists x \langle Q \rangle$

Ga zelf aan de hand van voorbeelden na dat de stelling klopt. Suggesties zijn:
"niet iedere Nederlander draagt een bril"
"er is geen reëel getal waarvan het kwadraat -1 is".

Met de opmerking in gedachten dat de universele quantificatie een generalisatie is van de conjunctie, en de existentiële quantificatie een generalisatie van de disjunctie, kunnen we regels 1 en 2 zien als generalisaties van de regels van DeMorgan, regel 3 als generalisatie van de commutativiteit van de conjunctie, en regel 4 als generalisatie van de commutativiteit van de disjunctie. We merken op dat regel 2 door negatie te verkrijgen is uit regel 1, en idem regel 4 uit regel 3.

Waarschuwing:
$\forall x\langle P \vee Q\rangle$ is *niet* gelijkwaardig met $\forall x\langle P\rangle \vee \forall x\langle Q\rangle$

$\exists x\langle P \wedge Q\rangle$ is *niet* gelijkwaardig met $\exists x\langle P\rangle \wedge \exists x\langle Q\rangle$

We illustreren dit aan een paar voorbeelden.
Bekijk met de gehele getallen als universum de predikaten $P := (x < 10)$ en $Q := (x > 0)$, dan is $\forall x\langle P \vee Q\rangle$ een ware bewering, maar $\forall x\langle P\rangle$ is onwaar, en $\forall x\langle Q\rangle$ is onwaar, dus is ook $\forall x\langle P\rangle \vee \forall x\langle Q\rangle$ onwaar.

Bekijken we daarentegen eveneens met de gehele getallen als universum de predikaten $P := (x > 10)$ en $Q := (x < 0)$, dan is $\exists x\langle P\rangle$ waar en $\exists x\langle Q\rangle$ is waar, dus $\exists x\langle P\rangle \wedge \exists x\langle Q\rangle$ is waar, maar $\exists x\langle P \wedge Q\rangle$ is onwaar.

Het komt erop neer dat er bij $\exists x\langle P \wedge Q\rangle$ één waarde voor x moet bestaan waarvoor P en Q beide waar zijn, terwijl bij $\exists x\langle P\rangle \wedge \exists x\langle Q\rangle$ er een waarde x is waarvoor P waar is, en ook een waarvoor Q waar is, maar die hoeven niet dezelfde te zijn. Hoewel beide bewering dus niet gelijkwaardig zijn is het wel zo dat als $\exists x\langle P \wedge Q\rangle$ waar is, dan is ook $\exists x\langle P\rangle \wedge \exists x\langle Q\rangle$ waar. Op soortgelijke wijze geldt dat als $\forall x\langle P\rangle \vee \forall x\langle Q\rangle$ waar is, dan is ook $\forall x\langle P \vee Q\rangle$ waar.

Onder beperkende voorwaarden bestaan er wel gelijkwaardigheden van de soort waarvoor we zojuist gewaarschuwd hebben. We geven deze in de volgende stelling.

Stelling 4.4 Als in Q de variabele x niet vrij voorkomt, en het universum is niet leeg, dan zijn in de volgende lijst de uitspraken op eenzelfde regel gelijkwaardig

1.	$\forall x\langle Q\rangle$	Q
2.	$\exists x\langle Q\rangle$	Q
3.	$\forall x\langle Q \vee P\rangle$	$Q \vee \forall x\langle P\rangle$
4.	$\exists x\langle Q \wedge P\rangle$	$Q \wedge \exists x\langle P\rangle$
5.	$\exists x\langle Q \to P\rangle$	$Q \to \exists x\langle P\rangle$
6.	$\forall x\langle Q \to P\rangle$	$Q \to \forall x\langle P\rangle$
7.	$\exists x\langle P \to Q\rangle$	$\forall x\langle P\rangle \to Q$
8.	$\forall x\langle P \to Q\rangle$	$\exists x\langle P\rangle \to Q$

Dit lijkt een ingewikkelde lijst, maar al deze regels volgen uit eenzelfde principe: een predicaat waarin de variabele x niet vrij voorkomt mag je buiten een quantor over x halen. De laatste regels zien er ingewikkelder uit omdat soms $\forall$ overgaat in $\exists$ en omgekeerd, maar volgen direct door het combineren van propositierekening en het toepassen van Stelling

4.3. Als voorbeeld bewijzen we regel 8 van Stelling 4.4, waarbij we steeds een uitdrukking vervangen door een equivalente uitdrukking met tussen haakje de motivatie er achter:

$$\begin{array}{rcll} \forall x\langle P \to Q\rangle & \equiv & \forall x\langle(\neg P) \vee Q\rangle & \text{(propositierekening)} \\ & \equiv & \forall x\langle Q \vee (\neg P)\rangle & \text{(propositierekening)} \\ & \equiv & Q \vee \forall x\langle\neg P\rangle & \text{(Stelling 4.4, regel 3)} \\ & \equiv & Q \vee \neg(\exists x\langle P\rangle) & \text{(Stelling 4.3, regel 1)} \\ & \equiv & \neg(\exists x\langle P\rangle) \vee Q & \text{(propositierekening)} \\ & \equiv & \exists x\langle P\rangle \to Q & \text{(propositierekening)} \end{array}$$

Hiermee hebben we het bewijs geleverd van regel 8 van Stelling 4.4, uitgaande van propositierekening, Stelling 4.3 en regel 3 van Stelling 4.4.

Het toepassen van commutativiteit van $\vee$ en $\wedge$ zullen we in het vervolg niet steeds meer als aparte stap opschrijven, zo gelden wegens regels 1 en 2 van Stelling 4.4 de volgende equivalenties:

$$\forall x\langle P \vee Q\rangle \equiv \forall x\langle P\rangle \vee Q, \quad \text{en} \quad \exists x\langle P \wedge Q\rangle \equiv \exists x\langle P\rangle \wedge Q,$$

waarin x niet vrij voorkomt in Q en het universum niet leeg is.

Met het toepassen van de stellingen 4.3 en 4.4, propositierekening en herbenoemen van variabelen kunnen de quantoren altijd naar voren worden gehaald, preciezer gezegd, elk predicaat opgebouwd uit quantoren en connectieven kan herschreven worden naar een equivalent predicaat van de vorm $A\langle P\rangle$ waarin A een rij quantoren is, elk met een bijbehorende variable, en P een uitdrukking is waarin die variabelen wel mogen voorkomen, maar geen quantoren. Een predicaat van deze speciale vorm heet een *prenex normaalvorm*. We geven een voorbeeld van een dergelijke herleiding naar prenex normaalvorm, waarbij we aannemen dat het universum niet leeg is. Hierin zijn $P(x)$ en $Q(x)$ willekeurige uitdrukkingen waarin de variabele x voor mag komen, en is $Q(y)$ verkregen uit $Q(x)$ door elk vrij voorkomen van x in $Q(x)$ te vervangen door y, waarbij y zelf niet vrij in $P(x)$ en $Q(x)$ voorkomt.

$$\begin{array}{rcll} \exists x\langle P(x)\rangle \to \exists x\langle Q(x)\rangle & \equiv & \neg\exists x\langle P(x)\rangle \vee \exists x\langle Q(x)\rangle & \text{(propositierekening)} \\ & \equiv & \forall x\langle\neg P(x)\rangle \vee \exists x\langle Q(x)\rangle & \text{(Stelling 4.3, regel 1)} \\ & \equiv & \forall x\langle\neg P(x)\rangle \vee \exists y\langle Q(y)\rangle & \text{(herben. van var.)} \\ & \equiv & \forall x\langle\neg P(x) \vee \exists y\langle Q(y)\rangle\rangle & \text{(Stelling 4.4, regel 3)} \\ & \equiv & \forall x\langle\exists y\langle\neg P(x)\rangle \vee \exists y\langle Q(y)\rangle\rangle & \text{(Stelling 4.4, regel 2)} \\ & \equiv & \forall x\exists y\langle\neg P(x) \vee Q(y)\rangle & \text{(Stelling 4.3, regel 4)} \end{array}$$

Als het universum wel leeg is is het allemaal nog veel gemakkelijker: dan kunnen we elke $\exists x\langle\cdots\rangle$ vervangen door F en elke $\forall x\langle\cdots\rangle$ vervangen door T. Hiermee houden we een uitdrukking over waarin helemaal geen quantoren voorkomen, en die is zeker in prenex normaalvorm.

Hoewel het zeer nuttige regels zijn, zijn de regels van stellingen 4.3 en 4.4 niet in alle gevallen toereikend om bewijzen te geven waarbij je de geldigheid van een predicaat moet gebruiken of bewijzen. Daartoe is het zeer gewenst dat we quantoren kunnen elimineren en weer kunnen invoeren, op een soortgelijke manier als we afleidingsregels hebben voor proposities. Eerst moeten we daartoe echter nog wat voorbereidingen treffen.

4.3 Substitutie

Bij het werken met predikaten in bewijzen wordt een zeer belangrijke rol gespeeld door *substitutie* van variabelen: het vervangen van een variabele door iets anders. Een speciaal geval hiervan zijn we al tegengekomen in de vorm van het *herbenoemen* van variabelen. Daar ging het nog om het vervangen van een vrije variabele door een andere naam met als doel de betekenis te verduidelijken.

Soms is het echter ook nodig om een variabele te vervangen door een constante, of zelfs door een ingewikkelder uitdrukking. Voorbeelden hiervan (met als universum de reële getallen) zijn

> Uit de uitspraak $\forall x\langle x^2 \geq 0\rangle$ wil ik kunnen concluderen $3^2 \geq 0$. Dit betekent dat de x in $x^2 \geq 0$ wordt vervangen door 3.
>
> Uit $3 > 2$ wil ik kunnen concluderen $\exists x\langle 3 > x\rangle$. Dat kan worden gerechtvaardigd door op te merken dat het predikaat $3 > x$ voor $x = 2$ een ware propositie is.

Met P^x_y duiden we, analoog als bij de proposities, aan dat alle vrij voorkomende x-en in P vervangen worden door y. Hiermee worden de bovenstaande voorbeelden geformaliseerd tot de regels

$$\begin{array}{lcll} \forall x\langle P\rangle & \vdash & P^x_3 & \text{(waarbij } P \text{ staat voor } x^2 \geq 0) \\ P^x_2 & \vdash & \exists x\langle P\rangle & \text{(waarbij } P \text{ staat voor } 3 > x) \end{array}$$

In deze voorbeelden was P een zeer eenvoudig predikaat. Als het predikaten betreft met een ingewikkelder structuur, dan is waakzaamheid vereist:

Alleen de in P vrij voorkomende x-en worden vervangen.

De x vervangende y kan een constante (bijvoorbeeld het getal 2) zijn. Maar y mag ook een variabele of algemener een *expressie* zijn. Het is wel essentieel dat x een variabele is, anders kunnen we geen zinvolle betekenis aan P^x_y geven.

Om het raamwerk zo algemeen mogelijk te houden willen we hier niet heel precies vastleggen wat een expressie is, maar het wordt gemakkelijker naarmate men met meer wiskunde kennis heeft gemaakt. Ruwweg gezegd is een expressie een uitdrukking die (eventueel na invullen van waarden voor variabelen) een waarde in het universum heeft. Wat een expressie is, hangt dus af van het universum waarin wordt gewerkt. In ieder geval worden variabelen en constanten altijd tot de expressies gerekend.

Met de reële getallen als universum rekenen we tot de expressies ook zinvolle uitdrukkingen die ontstaan door op variabelen en constanten bewerkingsoperaties zoals optellen, aftrekken, vermenigvuldigen, delen, machtverheffen en bekende functies toe te passen. Voorbeelden van expressies zijn

$$\begin{array}{cccccc} x & z & x+z & x+\sin(z) & 2(x-z) \\ 2 & 3 & \ln(x) & 3+4-7 & x+z/u \end{array}$$

In expressies komen behalve eventuele bewerkingssymbolen ($+$, $-$, $\cdot$, $/$) en functiesymbolen (sin, cos, tan, ln, log, etc.) ook variabelen en constanten voor. En juist die variabelen

kunnen roet in het eten gooien. Immers, we mogen niet door 0 delen, en bijvoorbeeld ook niet de logaritme nemen van een niet-positief getal. Maar er is meer.

Bekijk bijvoorbeeld het geval $\forall x \exists z \langle x - z = 0 \rangle$. Dit is voor de reële getallen waar. Nu wil ik hieruit graag concluderen $\exists z \langle 2 - z = 0 \rangle$ en $\exists z \langle a - z = 0 \rangle$. Tot zover is er geen vuiltje aan de lucht, want voor alle x is het predikaat $\exists z \langle x - z = 0 \rangle$ waar, dus ook als ik voor x iets invul, zoals 2 of a. Maar stel nu eens dat ik voor x wil invullen $3 + z$. Dat gaat fout, want $\exists z \langle 3 + z - z = 0 \rangle$ is onwaar!

De reden van deze fout is, dat een *vrije variabele* (namelijk z) in de vervanger $3 + z$ wordt *gebonden* door de substitie. Daarom stellen we als eis

> Een vrije variabele in de vervanger mag niet worden gebonden door de substitutie.

Ongelukken zoals hierboven kunnen worden voorkomen door alvorens de substitutie P_y^x daadwerkelijk uit te voeren, eerst te kijken of er wellicht in P gebonden variabelen voorkomen met dezelfde naam als welke in y vrij voorkomen. Geef dan eerst zulke in P gebonden voorkomende variabelen een andere naam: ga ze *herbenoemen*.

In ingewikkelde bewijzen kan het voorkomen dat men variabelen en dergelijke gebruikt, die niet alle hetzelfde *type* (reële getallen, gehele getallen, boolse variabelen etc.) hebben. Ook dan moet men oppassen, omdat een expressie in het algemeen alleen zinvol is binnen één type. Dus mag men bij een substitutie in het algemeen

> niet een variabele vervangen door een uitdrukking van een ander type.

al zijn er uitzonderingen zoals bijvoorbeeld het substitueren van een geheel getal in een reële variabele. Op de spelregels over het omgaan met typen gaan we hier verder niet in.

4.4 Afleidingsregels

Nu hebben we voldoende voorbereidingen getroffen om de *afleidingsregels voor predikaten* te geven. Voor beide quantoren $\forall$ en $\exists$ geven we een introductieregel om een uitdrukking met die quantor te kunnen bewijzen, en een eliminatieregel om een uitdrukking met die quantor te kunnen gebruiken.

Met P en Q geven we predikaten aan. In de motiveringen schrijven we soms $P(x)$ in plaats van P om te benadrukken welke variabele in P ons interesseert.

- *introductie* $\forall$: $\quad P \quad \vdash \quad \forall x \langle P \rangle$

  mits in het voorafgaande geen veronderstellingen over x gemaakt zijn.
  Motivering: stel dat $P(x)$ afgeleid is zonder iets over x te veronderstellen, dan mag voor x ieder object worden ingevuld. Maar dat is precies de betekenis van $\forall x \langle P(x) \rangle$.

- *eliminatie* $\forall$: $\quad \forall x \langle P \rangle \quad \vdash \quad P_a^x$

  als a een expressie is.
  Motivering: als P geldt voor alle objecten van het universum, dan ook voor speciale gevallen.

- *introductie* $\exists$: $\quad P_a^x \quad \vdash \quad \exists x\langle P\rangle$

  als a een expressie is.
  Motivering: als $P(x)$ het predikaat is, en $P(a)$ (a invullen voor x) al bewezen is, dan is er dus een object (nl. a) dat aan P voldoet.

- *eliminatie* $\exists$: $\quad \exists x\langle P\rangle \quad \vdash \quad Q$

  mits $P_a^x \to Q$ eerder in een subbewijs is bewezen, waarbij a een variabele is die alleen in dat subbewijs, maar *niet* in Q, voorkomt.
  Motivering: in de praktijk zeggen we "er is een element dat aan P voldoet, laten we het zolang a noemen en daarmee verder werken". Aangezien er verder geen eigenschappen van dat element bekend zijn, mag over die a in het voorgaande dus niets gezegd zijn. Bovendien mag Q niet van a afhangen, want uiteindelijk weten we niet welk element die a dan wel is.

We geven een voorbeeld; als universum nemen we de reële getallen.

$\forall x\langle\forall y\langle y > 0 \to x \leq y\rangle \to x \leq 0\rangle$

BEWIJS:
1 $\forall y\langle y > 0 \to x \leq y\rangle \to x \leq 0$
  BEWIJS van 1:
  1.1 $\forall y\langle y > 0 \to x \leq y\rangle$ (veronderstelling)
  1.2 $x > 0 \to \mathsf{F}$
    BEWIJS van 1.2
    1.2.1 $x > 0$ (veronderstelling)
    1.2.2 $x/2 > 0$ (1.2.1, elementaire rekenkunde)
    1.2.3 $\langle y > 0 \to x \leq y\rangle^y_{x/2}$ (1.1, elim. $\forall$, subst. $x/2$ voor y)
    1.2.4 $x/2 > 0 \to x \leq x/2$ (betekenis van 1.2.3)
    1.2.5 $x \leq x/2$ (1.2.2, 1.2.4, modus ponens)
    1.2.6 $x \leq 0$ (1.2.5, elementaire rekenkunde)
    1.2.7 $\neg(x > 0)$ (betekenis van 1.2.6)
    1.2.8 F (1.2.1, 1.2.7, introd. F)
    EINDE BEWIJS van 1.2 (deductie)
  1.3 $\neg(x > 0)$ (1.2, contradictie)
  1.4 $x \leq 0$ (betekenis van 1.3)
  EINDE BEWIJS van 1 (deductie)
2 $\forall x\langle\forall y\langle y > 0 \to x \leq y\rangle \to x \leq 0\rangle$ (1, introd. $\forall$, regel 1 veronderstelt niets over x)
EINDE BEWIJS

Merk op dat in het bewijs wel veronderstellingen zitten over x, maar uitsluitend in het subbewijs van regel 1.

Hiermee is dus bewezen dat de bewering

$$\forall x\langle\forall y\langle y > 0 \to x \leq y\rangle \to x \leq 0\rangle$$

altijd waar is, anders gezegd, equivalent is aan T. Bij proposities noemden we dat een *tautologie*; nu noemen we dat ook wel een *stelling*, in aansluiting op het begrip stelling zoals we dat al eerder hebben gezien.

Deze zelfde stelling bewijzen we nu nog eens via de contrapositie, en daarna nog eens uit het ongerijmde. Preciezer gezegd: we vervangen de te bewijzen bewering door een andere bewering die volgens bekende equivalenties equivalent is aan de oorspronkelijke bewering. Vervolgens geven we een bewijs van de aldus aangepaste bewering. Wel zullen we sommige argumentaties wat bekorten. We zullen zien dat een aantal argumenten wel steeds terug komen, maar dat de bewijzen verder toch wel verschillend zijn.

Met standaardequivalenties (waaronder contrapositie) herschrijven we bovenstaande uitdrukking naar een equivalente vorm die we vervolgens gaan bewijzen.

$$\begin{array}{ll} & \forall x\langle \forall y\langle y > 0 \to x \leq y\rangle \to x \leq 0\rangle \\ \equiv & \forall x\langle \neg(x \leq 0) \to \neg(\forall y\langle y > 0 \to x \leq y\rangle)\rangle \\ \equiv & \forall x\langle x > 0 \to \exists y\langle \neg(y > 0 \to x \leq y)\rangle\rangle \\ \equiv & \forall x\langle x > 0 \to \exists y\langle \neg(\neg(y > 0) \vee x \leq y)\rangle\rangle \\ \equiv & \forall x\langle x > 0 \to \exists y\langle y > 0 \wedge \neg(x \leq y)\rangle\rangle \\ \equiv & \forall x\langle x > 0 \to \exists y\langle y > 0 \wedge x > y\rangle\rangle \end{array}$$

Stelling: $\forall x\langle x > 0 \to \exists y\langle y > 0 \wedge x > y\rangle\rangle$

BEWIJS:

1 $x > 0 \to \exists y\langle y > 0 \wedge x > y\rangle$

BEWIJS van 1:

1.1 $x > 0$ (veronderstelling)

1.2 $x/2 > 0 \wedge x > x/2$ (1.1, elementaire rekenkunde)

1.3 $(y > 0 \wedge x > y)^{y}_{x/2}$ (dit is 1.2, subst. $x/2$ voor y)

1.4 $\exists y\langle y > 0 \wedge x > y\rangle$ (1.3, introductie $\exists$)

EINDE BEWIJS van 1 (deductie)

2 $\forall x\langle x > 0 \to \exists y\langle y > 0 \wedge x > y\rangle\rangle$ (1, introductie $\forall$)

EINDE BEWIJS

Toelichting: regel 2 is geoorloofd, omdat de enige veronderstelling over x zit in het subbewijs van regel 1.

Zoals beloofd bewijzen we dezelfde stelling ook nog eens uit het ongerijmde, oftewel we brengen de oorspronkelijke uitdrukking eerst met equivalenties naar de vorm $\cdots \to \mathsf{F}$ en gaan die vervolgens bewijzen.

$$\begin{array}{ll} & \forall x\langle \forall y\langle y > 0 \to x \leq y\rangle \to x \leq 0\rangle \\ \equiv & \neg(\forall x\langle \forall y\langle y > 0 \to x \leq y\rangle \to x \leq 0\rangle) \to \mathsf{F} \\ \equiv & \exists x\langle \neg(\forall y\langle y > 0 \to x \leq y\rangle \to x \leq 0)\rangle \to \mathsf{F} \\ \equiv & \exists x\langle \neg(\neg(\forall y\langle y > 0 \to x \leq y\rangle) \vee x \leq 0)\rangle \to \mathsf{F} \\ \equiv & \exists x\langle \forall y\langle y > 0 \to x \leq y\rangle \wedge \neg(x \leq 0)\rangle \to \mathsf{F} \\ \equiv & \exists x\langle \forall y\langle y > 0 \to x \leq y\rangle \wedge x > 0\rangle \to \mathsf{F} \end{array}$$

Stelling: $\exists x\langle\forall y\langle y > 0 \to x \leq y\rangle \wedge x > 0\rangle \to \mathsf{F}$

BEWIJS:
1 $\exists x\langle\forall y\langle y > 0 \to x \leq y\rangle \wedge x > 0\rangle$ (veronderstelling)
2 $(\forall y\langle y > 0 \to a \leq y\rangle \wedge a > 0) \to \mathsf{F}$
BEWIJS van 2:
2.1 $\forall y\langle y > 0 \to a \leq y\rangle \wedge a > 0$ (veronderstelling)
2.2 $a > 0$ (2.1, eliminatie $\wedge$)
2.3 $a/2 > 0$ (2.2, elementaire rekenkunde)
2.4 $a > a/2$ (2.2, elementaire rekenkunde)
2.5 $\forall y\langle y > 0 \to a \leq y\rangle$ (2.1, eliminatie $\wedge$)
2.6 $\langle y > 0 \to a \leq y\rangle^{y}_{a/2}$ (2.5, elim. $\forall$: subst. $a/2$ voor y)
2.7 $a/2 > 0 \to a \leq a/2$ (betekenis van 2.6)
2.8 $a \leq a/2$ (2.3, 2.7, modus ponens)
2.9 F (2.4, 2.8, introd. F)
EINDE BEWIJS van 2 (deductie)
3 F (1, 2, eliminatie $\exists$)
EINDE BEWIJS (deductie)

In bovenstaand bewijs hebben we de eliminatie van $\exists$ toegepast. Inderdaad is a op regel 2 een nieuwe variabele, en bovendien komt a niet voor in F.

Aan deze bewijzen zien we dat er soms heel verschillende manieren zijn om een bewijs te geven van dezelfde bewering, door die bewering te vervangen door een equivalente bewering. Dit is iets wat altijd correct is, en het is een goed principe te proberen om een te bewijzen bewering eerst in een zodanige equivalente vorm op te schrijven dat het bewijs zo eenvoudig mogelijk verloopt.

Vanaf nu zullen we vaak bewijzen in minder detail opschrijven, en vaak ook nummering van regels achterwege laten.

4.5 Opgaven

Opgave 4.1

Maak gebruik van de afkortingen

$M(x)$	:	x is mannelijk
$V(x)$	:	x is vrouwelijk
$J(x, y)$	:	x is jonger dan y
$K(x, y)$	:	x is een kind van y
$G(x, y)$	:	x en y zijn met elkaar getrouwd

Schrijf, gebruik makend van bovenstaande afkortingen, met als universum de verzameling van alle mensen, in predikatentaal:

a. Iedereen heeft een vader.

b. Iedereen is jonger dan zijn moeder.

c. Er is een man met een schoondochter die ouder is dan hij.

d. x is grootvader van y.

e. x is een zuster van y.

f. x is een oom van y van moeders kant.

Opgave 4.2

Gebruik de notatie $K(x, y)$ voor: x is een kind van y. Schrijf in predicaat-logische notatie: x heeft precies één kind.

Opgave 4.3

Als universum kiezen we de verzameling der reële getallen.
Schrijf de volgende proposities op in gewoon nederlands, en ga na of ze waar zijn:

a. $\forall x \exists y \langle x + y = 3 \rangle$

b. $\exists x \forall y \langle x + y = 3 \rangle$

c. $\exists x \exists y \langle x + y = 3 \rangle$

d. $\forall x \forall y \langle x + y = 3 \rangle$

Opgave 4.4

Neem de natuurlijke getallen als universum, en schrijf op in logische taal: p is een priemgetal.

Opgave 4.5

We bekijken de propositie

$$\forall x \forall t \langle P(x,t) \rightarrow (\exists x \langle Q(x,t) \rangle \wedge \forall t \langle R(x,t) \rangle) \rangle$$

waarin $P(x,t)$, $Q(x,t)$ en $R(x,t)$ predikaten zijn.

a. Geef voor elke voorkomende variabele met een pijl aan door welke quantor hij wordt gebonden.

b. Zorg er door het vervangen van variabelen voor dat eenzelfde letter niet in verschillende scopes optreedt.

Opgave 4.6

Maak gebruik van de volgende afkortingen:
Gxy betekent 'x is getrouwd met y',
en $Kxyz$ is 'z is kind van x en y'.

a. Schrijf als predikaatlogische formule: 'alle kinderen hebben twee ouders'

b. Idem: 'niet alle getrouwde mensen hebben kinderen, maar alle kinderen hebben getrouwde ouders'

c. Schrijf in goed Nederlands (gebruik geen variabelen)
$\forall z[(\exists x \exists y(Kxyz \wedge \neg Gxy)) \rightarrow (\exists u \exists v(Kuvz \rightarrow \forall t(Kuvt \rightarrow t = z)))]$

Opgave 4.7

Herleid de volgende predicaten naar prenex normaalvorm.

a. $(\neg(\forall x\langle P(x)\rangle)) \vee \forall x\langle R(x)\rangle$

b. $\forall x\langle P(x) \rightarrow \neg(\exists y\langle R(x,y)\rangle)\rangle$

c. $(\forall x \exists y\langle P(x,y)\rangle) \leftrightarrow \exists x \forall y\langle R(x,y)\rangle$

Opgave 4.8

Voer de volgende substituties uit, rekening houdend met de regels voor substitutie in bewijzen (alle variabelen zijn van eenzelfde type)

a. $(P(x) \vee \exists x\langle\neg P(x)\rangle)^x_t$

b. $(\forall y\langle(P(x,y) \wedge P(y,z)) \rightarrow P(x,z)\rangle)^x_y$

c. $(\forall y\langle(P(x,y) \wedge P(y,z)) \rightarrow P(x,z)\rangle)^y_x$

Opgave 4.9

a. Geef een voorbeeld van een predikaat P, en expressies t en s zo dat

$$(P^x_t)^y_s \quad \text{en} \quad (P^y_s)^x_t$$

verschillende betekenissen hebben.

b. Bedenk een voorwaarde waaronder verwisseling van de volgorde van twee substituties de betekenis niet aantast.

Opgave 4.10

Beschouw het volgende predikaat P:

$$\forall x \exists y(W(x) \rightarrow R(x,y,z)) \rightarrow \forall x \exists u \exists v(W(x) \vee S(x,y) \vee R(z,u,x))$$

a. Omcirkel alle vrije voorkomens van variabelen en geef met een pijl aan door welke quantor de gebonden variabelen gebonden worden.

b. Zoals je weet is $A(x)$ niet equivalent aan $A(y)$ (vanwege de vrije variabele) maar is $\exists x A(x)$ wel equivalent aan $\exists y A(y)$ (beide drukken uit dat er een object is met eigenschap A).

Geef nu een P' met de eigenschap:

- P en P' zijn equivalent
- in P' komt geen variabele zowel vrij als gebonden voor
- elke quantor in P' bindt een unieke variabele

Hoofdstuk 5

Verzamelingen

In de meest uiteenlopende omstandigheden kan het handig zijn om een stel objecten, elementen, of wat dan ook, samen een naam te geven. Het resultaat noemen we dan een *verzameling*. Zo'n verzameling bestaat alleen maar bij de gratie van de elementen die erin zitten.

Het fundamentele verband tussen een verzameling en objecten is dat van elk object vast ligt of het behoort tot die verzameling of niet. Synoniemen van "behoren tot" zijn "lid zijn van" en "element zijn van".

We gebruiken het *esti-teken* $\in$ als afkorting van "is lid van" of "behoort tot" of "is element van", zoals in $x \in A$.

Als x geen element is van A schrijven we $x \notin A$, wat we kunnen zien als afkorting voor $\neg(x \in A)$.

Een verzameling is volledig bepaald door de objecten die er lid van zijn, door zijn elementen.

Heeft een verzameling slechts eindig veel elementen, dan kunnen we die elementen allemaal *opsommen*, en daardoor de verzameling definiëren. De standaardnotatie die we daarvoor gebruiken is het achter elkaar opschrijven van de elementen, gescheiden door komma's, en het geheel afsluiten met accoladen. Bijvoorbeeld

$$V = \{3, 4, 9, 1\}$$

$$W = \{\text{maandag, dinsdag, woensdag, donderdag, vrijdag, zaterdag}\}$$

Merk op dat het er niet toe doet in welke volgorde de elementen tussen de accoladen staan. Ook mogen elementen herhaald worden:

$$\{3, 4, 9, 1\} = \{1, 3, 4, 9\} = \{3, 4, 9, 3, 1\}.$$

Soms gebruiken we ook een suggestieve notatie, zoals in

$$A = \{1, 2, \ldots, 10\} \qquad B = \{3, 4, 5, \ldots\}$$

Een waarschuwing is hier wel op zijn plaats: in zijn algemeenheid is het niet precies duidelijk wat '...' betekent, en is het aan te raden dit alleen te gebruiken als iedereen er dezelfde betekenis aan hecht. Wat zou bijvoorbeeld

$$\{1, 2, 4, 8, 16, \ldots\}$$

betekenen? De meeste mensen zullen dit rijtje wel voortgezet denken op de manier waarin elk getal door verdubbelen uit het vorige verkregen is, maar het zou met het eerste voorbeeld uit Hoofdstuk 1 in gedachten ook de verzameling van mogelijke aantal stukken kunnen zijn waarin een cirkel verdeeld kan worden door een aantal randpunten met elkaar te verbinden.

Voor grotere verzamelingen, waarbij de neiging bestaat om puntjes te gebruiken hebben we behoefte aan een andere notatie.

Om te beginnen, spreken we voor een aantal veel gebruikte verzamelingen af dat we ze altijd met een vast teken zullen aanduiden. Zo kennen we de standaard notaties

$\emptyset$	voor de *lege verzameling*, zonder elementen.
$\mathbf{N}$	voor de verzameling van alle *natuurlijke getallen*,
$\mathbf{Z}$	voor de verzameling van alle *gehele getallen*,
$\mathbf{Q}$	voor de verzameling van alle *rationale getallen*,
$\mathbf{R}$	voor de verzameling van alle *reële getallen*,
$\mathbf{C}$	voor de verzameling van alle *complexe getallen*.

De keuze van de letters $\mathbf{N}$, $\mathbf{R}$ en $\mathbf{C}$ spreken voor zich, de keuze van de letter $\mathbf{Q}$ is ontleend aan 'quotiënt', terwijl de keuze van de letter $\mathbf{Z}$ afkomstig van het Duitse woord 'Zahlen'.

Bij $\mathbf{N}$ en $\mathbf{Z}$ zouden we voor een redelijk ervaren lezer ook de puntjes-notatie

$$\mathbf{N} = \{0, 1, 2, 3, 4, 5, \ldots\} \text{ en } \mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

kunnen gebruiken. Voor $\mathbf{Q}$, $\mathbf{R}$ en $\mathbf{C}$ kan dat niet.

Merk op dat we hier 0 rekenen tot de natuurlijke getallen. Het is alleen een kwestie van afspraak om dat wel of niet te doen; voor beide is wat te zeggen. Helaas is er op dat gebied niet een uniform gebruik: in de diverse leerboeken kom je zowel definities van natuurlijke getallen tegen waarbij 0 er niet bij hoort als waarbij 0 er wel bij hoort.

Vaak stoppen we objecten in een verzameling omdat ze alle een specifieke eigenschap hebben die ons interesseert. Zo schrijven we bijvoorbeeld

$$A = \{x \in \mathbf{Z} |\ 1 \leq x \wedge x \leq 10\},$$

daarmee aangevend dat A bestaat uit alle gehele getallen die voldoen aan de eigenschap dat ze tussen (inclusief) 1 en 10 zitten. Dit is dus dezelfde verzameling als

$$A = \{1, 2, 3, \ldots, 10\},$$

maar we behoeven niet te raden wat de puntjes betekenen, en we hoeven ook niet alle elementen op te sommen. In zijn algemeenheid kunnen we altijd eigenschappen gebruiken om een verzameling te definiëren. Eigenschappen zijn te verwoorden in predikaten, en zo

gaan de predikaten dus een rol vervullen bij het definiëren van verzamelingen. Algemeen bedoelen we met

$$\{x \in U |\ E(x)\}$$

de verzameling die bestaat uit alle objecten uit de verzameling U die de eigenschap E hebben. Als de verzameling U steeds dezelfde is (het *universum*) en het is duidelijk wat U is, wordt ook wel kortweg geschreven $\{x|E(x)\}$, analoog aan de manier waarop ook bij predicaten het universum wel wordt weggelaten.

Voor de lege verzameling geldt

$$\emptyset = \{x |\ \mathsf{F}\}.$$

Hierin hebben we het universum weggelaten omdat dit er toch niet toe doet. De lege verzameling is de verzameling zonder elementen die we als deelverzameling van elk gewenst universum op willen kunnen vatten.

Een verzameling A heet *deelverzameling* van een verzameling B als elk element van A ook element van B is. We gebruiken hiervoor de notatie $A \subseteq B$, en soms ook wel $B \supseteq A$. Dus:

$$A \subseteq B \text{ betekent } \forall x \langle x \in A \rightarrow x \in B \rangle.$$

De relatie $\subseteq$ tussen verzamelingen heet ook wel *inclusie*. Een verzameling A heet een *echte deelverzameling* van een verzameling B als $A \subseteq B$ en er een element van B is dat niet een element van A is. Hiervoor wordt wel de notatie $A \subset B$ gebruikt, en soms ook wel $B \supset A$, wij zullen deze notatie niet veel tegenkomen.

Twee verzamelingen A en B zijn *gelijk* (notatie $A = B$) als ze dezelfde elementen bevatten, dus precies dan als $A \subseteq B$ en $B \subseteq A$.

$$A = B \text{ betekent } \forall x \langle x \in A \leftrightarrow x \in B \rangle$$

Als $P(x)$ en $Q(x)$ equivalente predicaten zijn, dan zijn de verzamelingen $\{x|P(x)\}$ en $\{x|Q(x)\}$ gelijk. Omgekeerd als $\{x|P(x)\}$ en $\{x|Q(x)\}$ gelijk zijn, dan zijn $P(x)$ en $Q(x)$ equivalent. Dit vatten we als volgt samen:

$$P(x) \equiv Q(x) \iff \{x|P(x)\} = \{x|Q(x)\}.$$

5.1 Operatoren op verzamelingen

Bij twee verzamelingen A en B die niet gelijk zijn, kunnen we een hele serie nieuwe verzamelingen definiëren. Dat is wat we nu gaan doen.

Met $A \cap B$ duiden we de *doorsnede* van A en B aan: de verzameling die bestaat uit alle objecten die zowel in A als in B zitten, oftewel

$$A \cap B = \{x |\ x \in A \wedge x \in B\},$$

ook te schrijven als

$$A \cap B = \{x \in A |\ x \in B\},$$

en ook als

$$A \cap B = \{x \in B |\ x \in A\}.$$

Een belangrijke equivalentie die direct volgt uit deze definitie is

$$x \in A \cap B \quad \Leftrightarrow \quad x \in A \wedge x \in B.$$

Twee verzamelingen heten *disjunct* als hun doorsnede leeg is.

Met $A \cup B$ duiden we de *vereniging* van A en B aan: de verzameling die bestaat uit alle objecten van A en alle objecten van B, oftewel

$$A \cup B = \{x |\ x \in A \vee x \in B\}.$$

Een belangrijke equivalentie die direct volgt uit deze definitie is

$$x \in A \cup B \quad \Leftrightarrow \quad x \in A \vee x \in B.$$

Met $A - B$, het *verschil* van A met B, bedoelen we de verzameling bestaande uit alle objecten die wel tot A behoren, maar niet tot B, oftewel

$$A - B = \{x \in A | x \notin B\}.$$

Een belangrijke equivalentie die direct volgt uit deze definitie is

$$x \in A - B \quad \Leftrightarrow \quad x \in A \wedge x \notin B.$$

De verzameling $(A \cup B) - (A \cap B)$ staat bekend als het *symmetrische verschil* van A en B. Deze is gelijk aan $(A - B) \cup (B - A)$ zoals we later nog zullen zien. Hiervoor wordt wel de notatie $A \Delta B$ gebruikt.

Het komt vaak voor dat we het uitsluitend willen hebben over objecten in een vast *universum* U.

Dat houdt tevens in dat alle verzamelingen waarover we dan kunnen spreken deelverzamelingen zijn van U. Is U het universum, dan heet $U - A$ het *complement* van A, ook wel korter genoteerd als A^c:

$$A^c = \{x |\ x \notin A\}.$$

Bij de begrippen die we tot nu toe (maar dat geldt ook voor het vervolg) hebben behandeld, is het nuttig om plaatjes te tekenen. Daartoe worden verzamelingen vaak voorgesteld als elkaar overlappende (cirkel)schijfjes. Zo'n plaatje heet een *Venn-diagram*. Plaatjes verhelderen vaak de betekenis van een definitie. Bovendien zijn plaatjes nuttig bij het ontdekken van vermoedens, die men vervolgens kan proberen te bewijzen (want een plaatje geldt niet als bewijs). Ook is het tekenen van een plaatje soms de snelste manier om te laten zien dat iets niet waar is.

Het wordt nu tijd om de voorgaande grote hoeveelheid van definities (die hopelijk niet allemaal nieuw zijn) te laten figureren in een aantal belangrijke rekenregels voor verzamelingen.

Stelling 5.1 Voor alle verzamelingen A, B en C gelden de volgende regels

1. $A \cup \emptyset = A$
2. $A \cap \emptyset = \emptyset$
3. $A \cup B = B \cup A$
4. $A \cap B = B \cap A$
5. $(A \cup B) \cup C = A \cup (B \cup C)$
6. $(A \cap B) \cap C = A \cap (B \cap C)$
7. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
8. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Hierin drukt regel 1 uit dat $\emptyset$ een *neutraal element* is met betrekking tot de vereniging. Regels 3 en 4 geven aan dat vereniging en doorsnede *commutatief* zijn. Regels 5 en 6 geven aan dat vereniging en doorsnede *associatief* zijn. Regel 7 geeft aan dat doorsnede *distribueert over* vereniging en regel 8 geeft aan dat vereniging distribueert over doorsnede.

Hoe kunnen we deze stelling bewijzen? We moeten een aantal keren een bewijs geven dat twee verzamelingen V en W gelijk aan elkaar zijn. Per definitie betekent dat dat elk element van V in W moet zitten en omgekeerd. Dit zouden we volgens de regel 'introductie $\forall$' kunnen bewijzen door twee 'halve bewijzen' te geven:

- kies een willekeurig element in V en bewijs dat die in W zit;
- kies een willekeurig element in W en bewijs dat die in V zit.

Vaak kunnen we zo'n bewijs echter korter opschrijven: als we voor een willekeurig element x een reeks equivalenties kunnen vinden van de vorm

$$x \in V \Leftrightarrow \cdots \Leftrightarrow \cdots\cdots\cdots \Leftrightarrow x \in W$$

dan hebben we daarmee het eerste halve bewijs gegeven door deze reeks van links naar rechts te lezen, en hebben we het tweede halve bewijs gegeven door deze reeks van rechts naar links te lezen. We geven enkele voorbeelden van dergelijke bewijzen. Steeds schrijven we voor elke stap de motivatie voor de geldigheid tussen haakjes er achter, in dezelfde stijl als we dat bij het herleiden van een predicaat naar prenex normaalvorm ook al deden. Equivalenties in deze redeneringen noteren we met $\Leftrightarrow$; deze notatie geeft de twee richtingen al aan waarin we het bewijs kunnen lezen. We beginnen met het bewijs van regel 1 van Stelling 5.1.

$$\begin{array}{lcll} x \in A \cup \emptyset & \Leftrightarrow & x \in A \vee x \in \emptyset & \text{(definitie } \cup\text{)} \\ & \Leftrightarrow & x \in A \vee \mathsf{F} & \text{(definitie } \emptyset\text{)} \\ & \Leftrightarrow & x \in A & \text{(propositierekening).} \end{array}$$

Vanwege $x \in A \cup \emptyset \Leftrightarrow x \in A$ geldt nu $A \cup \emptyset = A$ en is regel 1 van Stelling 5.1 bewezen.

We bewijzen nu regel 8 van Stelling 5.1.

$$\begin{array}{lll} x \in (A \cap B) \cup C & \Leftrightarrow & x \in (A \cap B) \vee x \in C \qquad \text{(definitie } \cup\text{)} \\ & \Leftrightarrow & (x \in A \wedge x \in B) \vee x \in C \qquad \text{(definitie } \cap\text{)} \\ & \Leftrightarrow & (x \in A \vee x \in C) \wedge (x \in B \vee x \in C) \qquad \text{(propositierekening)} \\ & \Leftrightarrow & (x \in A \cup C) \wedge (x \in B \vee x \in C) \qquad \text{(definitie } \cup\text{)} \\ & \Leftrightarrow & (x \in A \cup C) \wedge (x \in B \cup C) \qquad \text{(definitie } \cup\text{)} \\ & \Leftrightarrow & x \in (A \cup C) \cap (B \cup C) \qquad \text{(definitie } \cap\text{)} \end{array}$$

Vanwege $x \in (A \cap B) \cup C \Leftrightarrow x \in (A \cup C) \cap (B \cup C)$ geldt nu $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$, en is dus ook regel 8 van Stelling 5.1 bewezen. De bewijzen van de overige regels van Stelling 5.1 gaan geheel analoog. We zien ook dat het geen toeval is dat dat dezelfde regels die we in de propositierekening tegenkwamen voor $\vee$ en $\wedge$ hier precies zo gelden voor $\cup$ en $\cap$: bij het toepassen van de definities van $\cup$ en $\cap$ vertaalt elk $\cup$-symbool naar $\vee$, elk $\cap$-symbool naar $\wedge$ en $\emptyset$ naar F, waarna de bijbehorende regel uit de propositierekening toegepast wordt, en vervolgens nog een aantal keren de definities van $\cup$ en $\cap$ tot het gewenste resultaat is bereikt.

Aan de ene kant is deze analogie heel handig, aan de andere kant is een waarschuwing hier ook op zijn plaats: $\cup$ en $\cap$ zijn operatoren die altijd op verzamelingen werken, en $\vee$ en $\wedge$ zijn operatoren die altijd op proposities / beweringen / predicaten werken. Haal ze dus niet door elkaar!

Stelling 5.2 Voor alle verzamelingen A, B en C gelden de volgende regels

1. $\emptyset \subseteq A$
2. $A \subseteq (A \cup B)$
3. $(A \cap B) \subseteq A$
4. als $A \subseteq B$, dan $(A \cup C) \subseteq (B \cup C)$
5. als $A \subseteq B$, dan $(A \cap C) \subseteq (B \cap C)$
6. als $A \subseteq C$ en $B \subseteq C$, dan $(A \cup B) \subseteq C$
7. als $A \subseteq B$ en $A \subseteq C$, dan $A \subseteq (B \cap C)$
8. als $A \subseteq B$ en $B \subseteq C$, dan $A \subseteq C$

Regel 8 drukt uit dat inclusie *transitief* is.

Het bewijs van een bewering $V \subseteq W$ gaat vrijwel altijd als volgt: neem een willekeurig element $x \in V$ en bewijs dat $x \in W$.

Als voorbeeld bewijzen we $\emptyset \subseteq A$. Neem een willekeurig element $x \in \emptyset$. Zo'n element bestaat helemaal niet: de aanname is F. Uit F kunnen we alles concluderen, in het bijzonder dat $x \in A$. Hiermee is bewezen $\emptyset \subseteq A$, oftewel regel 1 van Stelling 5.2.

Nu gaan we regel 4 van Stelling 5.2 bewijzen. Volgens het deductieprincipe nemen we aan dat $A \subseteq B$, en moeten op grond daarvan bewijzen dat $(A \cup C) \subseteq (B \cup C)$. Kies daartoe een willekeurig element $x \in A \cup C$. Per definitie geldt dan $x \in A \vee x \in C$. Om

deze disjunctie te gebruiken hebben we *eliminatie* $\vee$ nodig. We schrijven het bewijs nog maar eens in detail in stappen op:

1	$x \in A \cup C$	(aanname)
2	$x \in A \vee x \in C$	(1, definitie $\cup$)
3	$x \in A \rightarrow x \in B \cup C$	
	bewijs van 3:	
	3.1 $x \in A$	(veronderstelling)
	3.2 $x \in B$	(3.1, aanname $A \subseteq B$)
	3.3 $x \in B \vee x \in C$	(3.2, introductie $\vee$)
	3.4 $x \in B \cup C$	(3.3, definitie $\cup$)
	einde bewijs van 3 (deductie)	
4	$x \in C \rightarrow x \in B \cup C$	
	bewijs van 4:	
	4.1 $x \in C$	(veronderstelling)
	4.2 $x \in B \vee x \in C$	(4.1, introductie $\vee$)
	4.3 $x \in B \cup C$	(4.2, definitie $\cup$)
	einde bewijs van 4 (deductie)	
5	$x \in B \cup C$	(2, 3, 4, eliminatie $\vee$)

Hiermee hebben we bewezen dat $x \in B \cup C$ voor elk willekeurig element $x \in A \cup C$, oftewel $(A \cup C) \subseteq (B \cup C)$. Daarmee is regel 4 van Stelling 5.2 bewezen.

In woorden zouden we ditzelfde bewijs ook iets slordiger zo op kunnen schrijven:

> We weten $x \in A \vee x \in C$ en maken nu een gevalsonderscheid tussen $x \in A$ en $x \in C$. Als $x \in A$ dan $x \in A \subseteq B \subseteq B \cup C$. Als $x \in C$ dan $x \in C \subseteq B \cup C$. In beide gevallen hebben we $x \in B \cup C$, dus geldt $x \in B \cup C$.

De slordigheid in dit bewijs zit hem in het weglaten van details als nummertjes en namen van regels; maar afgezien daarvan is het precies hetzelfde, en is elk detail weer desgewenst in te vullen. Als daaraan voldaan is, zullen we ook dit soort 'slordige' bewijzen toestaan. Met nadruk wijzen we erop dat dit geen water in de wijn doet op het gebied van precisie, en zeker niet gebruikt kan worden om ontbrekende stukken van een redenering onder de tafel te vegen. Het vinden van een een bewijs blijft even moeilijk en de gestelde eisen aan een redenering blijven dezelfde, we staan alleen een beknoptere en misschien begrijpelijkere notatie van het eindresultaat toe.

Het bewijs van de overige regels van Stelling 5.2 laten we aan de lezer over.

We geven nu een aantal gelijkheden met betrekking tot het *complement* van verzamelingen.

Stelling 5.3 In een vast universum U gelden de volgende regels voor verzamelingen

1. $\emptyset^c = U$
2. $U^c = \emptyset$
3. $(A^c)^c = A$
4. $(A \cup B)^c = A^c \cap B^c$
5. $(A \cap B)^c = A^c \cup B^c$
6. als $A \subseteq B$, dan $B^c \subseteq A^c$

We zien dat de bij Stelling 5.1 genoemde analogie tussen operatoren voor proposities en operatoren voor verzamelingen zich nog verder uitbreidt: het complement vertaalt naar $\neg$ en het universum U vertaalt naar T. De basis-regels zijn

$$x \in \emptyset \Leftrightarrow \mathsf{F}, \quad x \in U \Leftrightarrow \mathsf{T}, \quad x \in A^c \Leftrightarrow \neg(x \in A),$$

$$x \in A \cup B \Leftrightarrow (x \in A \ \vee \ x \in B), \qquad x \in A \cap B \Leftrightarrow (x \in A \ \wedge \ x \in B).$$

Samen met de propositierekening kunnen we hiermee rechtstreeks de eerste vijf regels van Stelling 5.3 bewijzen op dezelfde manier als bij Stelling 5.1: $V = W$ bewijs je door voor een willekeurig element x te bewijzen $x \in V \Leftrightarrow x \in W$. Regels 4 en 5 heten wel de wetten van *DeMorgan* omdat ze precies overeenkomen met wetten van DeMorgan in de propositierekening.

Regel 6 komt overeen met *contrapositie* en gaan we nu bewijzen.

Bewijs:

Neem aan dat $A \subseteq B$.

Kies $x \in B^c$ willekeurig.

Dan $\neg(x \in B)$ (definitie complement).

Stel $x \in A$.

Dan $x \in B$ (vanwege $A \subseteq B$).

Tegenspraak met $\neg(x \in B)$.

Dus $\neg(x \in A)$.

Dus $x \in A^c$ (definitie complement).

Hiermee is bewezen dat $B^c \subseteq A^c$.

Einde Bewijs.

Hiermee is bewezen dat $B^c \subseteq A^c$ onder de aanname dat $A \subseteq B$, oftewel regel 6 van Stelling 5.3 is bewezen.

We bewijzen nu de gelijkheid tussen de twee definities van het *symmetrische verschil* van twee verzamelingen A en B:

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

Daarvoor hebben we de volgende regel nodig:

$$(p \vee q) \wedge \neg(p \wedge q) \Leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p) \qquad (*)$$

In principe hebben we drie manieren om deze equivalentie te bewijzen: we kunnen een *waarheidstafel* opstellen, we kunnen aan de slag met de regels uit Stelling 2.9 en we kunnen voor beide richtingen een deductiebewijs geven. Omdat er hier slechts twee atomaire proposities p en q zijn, hebben we te maken met een waarheidstafel van slechts vier regels en is de eerste methode het snelst en laten we die aan de lezer over. Verder korten we $x \in A$ af tot p en korten we $x \in B$ af tot q.
$x \in (A \cup B) - (A \cap B)$

$$\begin{array}{lll}
\Leftrightarrow & x \in (A \cup B) \wedge \neg(x \in A \cap B) & (\text{definitie } -) \\
\Leftrightarrow & (x \in A \vee x \in B) \wedge \neg(x \in A \cap B) & (\text{definitie } \cup) \\
\Leftrightarrow & (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B) & (\text{definitie } \cap) \\
\Leftrightarrow & (p \vee q) \wedge \neg(p \wedge q) & (\text{definitie } p, q) \\
\Leftrightarrow & (p \wedge \neg q) \vee (q \wedge \neg p) & (*) \\
\Leftrightarrow & (x \in A \wedge \neg(x \in B)) \vee (x \in B \wedge \neg(x \in A)) & (\text{definitie } p, q) \\
\Leftrightarrow & (x \in A - B) \vee (x \in B \wedge \neg(x \in A)) & (\text{definitie } -) \\
\Leftrightarrow & (x \in A - B) \vee (x \in B - A) & (\text{definitie } -) \\
\Leftrightarrow & x \in (A - B) \cup (B - A) & (\text{definitie } \cup)
\end{array}$$

Nu is voor een willekeurig element x bewezen dat

$$x \in (A \cup B) - (A \cap B) \Leftrightarrow x \in (A - B) \cup (B - A),$$

waarmee is bewezen dat $(A \cup B) - (A \cap B) = (A - B) \cup (B - A)$.

5.2 Machtsverzameling en cartesisch product

Objecten hoeven geen "ondeelbare" dingen te zijn. Het komt zelfs vaak voor dat we hele verzamelingen als objecten wensen te beschouwen. Denk bijvoorbeeld aan een elftal, een regiment, een mierenkolonie.
Op de middelbare school hebben we iets dergelijks ook gezien bij de kansrekening, waar bijvoorbeeld gevraagd kan worden naar het aantal mogelijkheden waarop men uit een verzameling V met n objecten een greep kan doen. Dat is de vraag naar het aantal deelverzamelingen van V. Dat is het aantal *elementen* van

de verzameling bestaande uit de *deelverzamelingen* van V.

Deze verzameling noemen we de *machtsverzameling* van V. In het Engels heet dit *power set*; we noteren hem dan ook met $\mathcal{P}(V)$:

$$\mathcal{P}(V) = \{A |\ A \subseteq V\}$$

We geven een voorbeeld. Zij V={a,b,c}. Dan is

$$\mathcal{P}(V) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

$\mathcal{P}(V)$ heeft in dit voorbeeld dus 8 ($= 2^3$) elementen. In het algemeen bestaat $\mathcal{P}(V)$ uit 2^n elementen als V uit n elementen bestaat. Dit is als volgt in te zien. Een element van $\mathcal{P}(V)$ is een deelverzameling van V, en die ligt vast door voor elk element aan te geven of die wel of niet in de deelverzameling zit. Als V bestaat uit n elementen heb je hierbij dus n keer een keuze uit twee mogelijkheden. In totaal levert dat 2^n mogelijkheden. Elke mogelijkheid correspondeert met precies één deelverzameling, en elke deelverzameling kan zo worden verkregen, dus heeft $\mathcal{P}(V)$ precies 2^n elementen. Vanwege deze eigenschap wordt de machtsverzameling $\mathcal{P}(V)$ ook wel genoteerd als 2^V; het woord *machtsverzameling* is zo gekozen omdat hier sprake is van *machtsverheffen*.

> Merk op dat we een onderscheid dienen te maken tussen het element a en de verzameling $\{a\}$ die a als enige element heeft.
>
> In het voorbeeld geldt wel $a \in \{a\}$ en $a \in V$ en $\{a\} \in \mathcal{P}(V)$ en $\{a\} \subseteq V$, maar niet $\{a\} \subseteq \mathcal{P}(V)$. Wel geldt $\{\{a\}\} \subseteq \mathcal{P}(V)$.

Onder het *cartesisch product* $A \times B$ van twee verzamelingen A en B verstaan we de verzameling van alle *geordende paren* (x, y) waarvoor $x \in A$ en $y \in B$.
Dat de paren geordende paren zijn, betekent dat (x, y) en (y, x) verschillend zijn als $x \neq y$.

$$A \times B = \{(x, y) |\ x \in A \wedge y \in B\}$$

Een voorbeeld: Zij

$$A = \{a, b, c, d\} \quad \text{en} \quad B = \{a, d, f, e, g\}.$$

Dan is

$$\begin{array}{rcl} A \times B & = & \{ \quad (a,a), \quad (a,d), \quad (a,f), \quad (a,e), \quad (a,g), \\ & & \quad\ (b,a), \quad (b,d), \quad (b,f), \quad (b,e), \quad (b,g), \\ & & \quad\ (c,a), \quad (c,d), \quad (c,f), \quad (c,e), \quad (c,g), \\ & & \quad\ (d,a), \quad (d,d), \quad (d,f), \quad (d,e), \quad (d,g) \quad \} \end{array}$$

Als A en B eindige verzamelingen zijn met respectievelijk n en m elementen, heeft het cartesisch product $A \times B$ precies $n \times m$ elementen: voor elk geordend paar hebben we n mogelijkheden om het eerste argument te kiezen en m mogelijkheden om het tweede argument te kiezen. Dit aantal verklaart dat we dit een *product* noemen. Het voorvoegsel is afgeleid van de wiskundige René *Descartes* (1596-1650), die de punten het platte vlak opvatte als geordende paren van reële getallen: de *coördinaten*.

Een reden dat we de begrippen machtsverzameling en cartesisch produkt als laatste hebben genoemd, is in de eerste plaats omdat ze abstracter (en wellicht onbekender) zijn dan de overige begrippen. Een andere reden is, dat deze constructies ons buiten een gegeven universum kunnen brengen. Men kan gemakkelijk zelf voorbeelden hiervan vinden.

5.3 Vereniging en doorsnede over een indexverzameling

We hebben de doorsnede en de vereniging van twee verzamelingen gedefinieerd, en daarmee kan men ook doorsneden en verenigingen bestuderen van meer dan twee verzamelingen.

Vanwege associativiteit is de betekenis van zo'n doorsnede of vereniging onafhankelijk van de manier waarop haakjes geplaatst worden, en kunnen we de haakjes ook weglaten. Zo geldt bijvoorbeeld

$$A \cup (B \cup (C \cup D)) = (A \cup B) \cup (C \cup D) = ((A \cup B) \cup C) \cup D$$

en kunnen we deze verzameling zonder verwarring schrijven als $A \cup B \cup C \cup D$. Vanwege commutativiteit kunnen we ook nog de volgorde veranderen zonder de betekenis aan te tasten. Let wel dat dit alleen opgaat als er alleen sprake is van vereniging of alleen van doorsnede, maar niet van combinaties van vereniging en doorsnede. Op deze wijze kunnen we bij elke eindige verzameling van verzamelingen spreken van de vereniging en de doorsnede.

We gaan nu een notatie invoeren waarmee ook de vereniging en de doorsnede kan worden genomen van *oneindig veel* verzamelingen. waarvan de doorsnede of de vereniging moet worden bepaald.

In het algemeen is voor een verzameling $\mathcal{A}$ van verzamelingen de vereniging van alle elementen van $\mathcal{A}$ gedefinieerd door

$$\bigcup_{z \in \mathcal{A}} z = \{x |\ \exists z \in \mathcal{A}\ \langle x \in z \rangle\}$$

en de doorsnede van alle elementen van $\mathcal{A}$ door

$$\bigcap_{z \in \mathcal{A}} z = \{x |\ \forall z \in \mathcal{A}\ \langle x \in z \rangle\}$$

Net zoals

$+$ generaliseert tot Σ,

$\vee$ generaliseert tot $\exists$,

$\wedge$ generaliseert tot $\forall$,

kunnen we nu zeggen dat

$\cup$ generaliseert tot $\bigcup$,

$\cap$ generaliseert tot $\bigcap$.

Als voorbeeld kiezen we $\mathcal{A} = \{A, B\}$. Omdat $\exists z \in \mathcal{A}\ \langle x \in z \rangle$ hetzelfde betekent als $x \in A \vee x \in B$, en $\forall z \in \mathcal{A}\ \langle x \in z \rangle$ hetzelfde betekent als $x \in A \wedge x \in B$, geldt in dit geval

$$\bigcup_{z \in \mathcal{A}} z = A \cup B \quad \text{en} \quad \bigcap_{z \in \mathcal{A}} z = A \cap B.$$

Als de verzameling $\mathcal{A}$ van verzamelingen geschreven is als

$$\mathcal{A} = \{A_i | i \in I\}$$

schrijven we ook wel

$$\bigcup_{i \in I} A_i \quad \text{voor} \quad \bigcup_{z \in \mathcal{A}} z, \quad \text{en} \quad \bigcap_{i \in I} A_i \quad \text{voor} \quad \bigcap_{z \in \mathcal{A}} z.$$

In dit geval heet I de *indexverzameling*. In plaats van

$$\bigcup_{i\in\mathbf{N}} \quad \text{en} \quad \bigcap_{i\in\mathbf{N}}$$

wordt ook wel geschreven

$$\bigcup_{i=0}^{\infty} \quad \text{en} \quad \bigcap_{i=0}^{\infty}.$$

Als $I = \{i \in \mathbf{N} | i > 0 \wedge i < 10\}$ hebben we dus

$$\bigcup_{i\in I} A_i \;=\; A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6 \cup A_7 \cup A_8 \cup A_9;$$

zo zien we dat met deze notatie soms ook eindige verenigingen en doorsneden korter kunnen opschrijven dan voorheen.

Als slot van dit hoofdstuk bewijzen we dat

$$\bigcup_{i\in\mathbf{Z}} A_i \;=\; \mathbf{R}$$

waarbij voor iedere $i \in \mathbf{Z}$ de deelverzameling A_i van $\mathbf{R}$ gedefinieerd is door

$$A_i = \{x \in \mathbf{R} | i \leq x \wedge x \leq i + 1\}.$$

We bewijzen dit in twee stappen: $\bigcup_{i\in\mathbf{Z}} A_i \subseteq \mathbf{R}$, afgekort tot '$\subseteq$', en $\bigcup_{i\in\mathbf{Z}} A_i \supseteq \mathbf{R}$, afgekort tot '$\supseteq$'.

Bewijs:

'$\subseteq$':

We kiezen een willekeurig element $x \in \bigcup_{i\in\mathbf{Z}} A_i$ en moeten daarvoor bewijzen dat $x \in \mathbf{R}$. Volgens de definitie van $\bigcup$ is er $i \in \mathbf{Z}$ zodanig dat $x \in A_i$. Vanwege $A_i \subseteq \mathbf{R}$ concluderen we nu $x \in \mathbf{R}$, en hebben we '$\subseteq$' bewezen.

'$\supseteq$':

We kiezen een willekeurig element $x \in \mathbf{R}$ en moeten daarvoor bewijzen dat $x \in \bigcup_{i\in\mathbf{Z}} A_i$. Definieer nu n als het grootste gehele getal waarvoor geldt $n \leq x$. Per definitie geldt dan $n \leq x$. Maar er geldt ook dat $x < n + 1$, want als dat niet zo was, dan was $n + 1 \leq x$, en was er een groter geheel getal, nl. $n + 1$, waarvoor $n + 1 \leq x$. Vanwege $x < n + 1$ geldt zeker $x \leq n + 1$, en vanwege $n \leq x$ geldt nu $n \leq x \wedge x \leq n+1$. Hieruit volgt dat $x \in A_n$. Dus is er een $i \in \mathbf{Z}$ (nl. n) met $x \in A_i$, dus geldt $x \in \bigcup_{i\in\mathbf{Z}} A_i$. Hiermee is '$\supseteq$' bewezen.

Einde Bewijs.

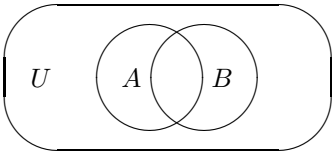
5.4 Opgaven

In de volgende opgaven is $X \Delta Y$ het symmetrische verschil tussen de verzamelingen X en Y.

Opgave 5.1

In onderstaand plaatje is U het universum, en zijn A en B verzamelingen. Teken dit plaatje een aantal malen over, en geef door arcering aan

a. $A \Delta B$ **d.** $A - B$
b. $A^c \Delta B^c$ **e.** $A^c - B$
c. $(A^c - B^c)^c$ **f.** $(A - B)^c$



Opgave 5.2

$P(x)$ en $Q(x)$ zijn predikaten, en x is een variabele over een universum U. We stellen $A = \{x|\ P(x)\}$ en $B = \{x|\ Q(x)\}$. Druk de volgende verzamelingen uit in A en B en de operatoren op verzamelingen.

a. $\{x|\ P(x) \rightarrow Q(x)\}$

b. $\{x|\ P(x) \wedge Q(x)\}$

c. $\{x|\ P(x) \leftrightarrow Q(x)\}$

d. $\{x|\ P(x) \vee Q(x)\}$

Opgave 5.3

Teken de bijbehorende Venn-diagrammen, en bewijs

a. $A - (B - C) = A - (B - (A \cap C))$

b. $(A - B) - C = A - (B \cup C)$

c. $A - B = A - (A \cap B)$

d. $A - B = (A \cup B) - B$

e. $(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$

Opgave 5.4

Bestudeer de volgende uitspraken. Geef in geval van algemene juistheid een bewijs, geef anders een tegenvoorbeeld.

a. $A - B = (A \cup C) - (B \cup C)$

b. $A - B = (A \cap C) - (B \cap C)$

c. $(A - B) \cup C = (A \cup C) - (B \cup C)$

d. $(A - B) \cap C = (A \cap C) - (B \cap C)$

e. $(A \Delta B) \cup C = (A \cup C) \Delta (B \cup C)$

Opgave 5.5

Voor een verzameling X met eindig veel elementen, geven we met $\#X$ het aantal elementen van X aan. Alle in deze opgave voorkomende verzamelingen worden geacht eindig veel elementen te bezitten.

a. Beredeneer dat $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.

b. Gebruik het resultaat van a. om aan te tonen dat

$$\#(A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C).$$

Opgave 5.6

Bewijs dat voor verzamelingen A en B geldt

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B).$$

Opgave 5.7

a. Bewijs dat voor verzamelingen A en B geldt

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B).$$

b. Geef een voorbeeld van twee verzamelingen A en B waarvoor niet geldt dat

$$\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B).$$

Opgave 5.8

Bestudeer de volgende uitspraken. Geef in geval van algemene juistheid een bewijs, geef anders een tegenvoorbeeld.

a. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

b. $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$

Opgave 5.9

Bewijs dat voor verzamelingen A, B en C geldt

a. $A \times (B \cup C) = (A \times B) \cup (A \times C)$

b. $A \times (B \cap C) = (A \times B) \cap (A \times C)$

c. $(A \cup B) \times C = (A \times C) \cup (B \times C)$

d. $(A \cap B) \times C = (A \times C) \cap (B \times C)$

Opgave 5.10

Laten A en B deelverzamelingen van U zijn. Laat $D \subseteq (U \times U)$ gegeven zijn door $D = \{(u, u) |\ u \in U\}$ (D heet de *diagonaal* van $U \times U$).

Bewijs: $A \cap B = \emptyset$ dan en slechts dan als $(A \times B) \cap D = \emptyset$.

Opgave 5.11

Bewijs dat

$$\bigcup_{i \in \mathbf{N}} B_i \ = \ \mathbf{R}$$

waarbij voor iedere $i \in \mathbf{N}$ de deelverzameling B_i van $\mathbf{R}$ gedefinieerd is door

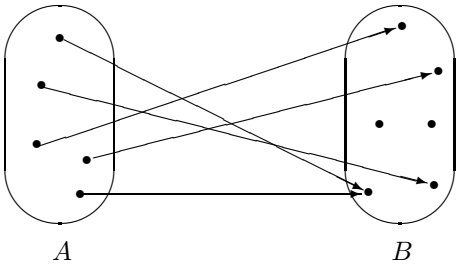
$$B_i = \{x \in \mathbf{R} | -i < x \wedge x < i\}.$$

Hoofdstuk 6

Afbeeldingen

Wanneer we voor twee verzamelingen A en B bij elk element van A precies één element van B vastleggen, dan hebben we een *afbeelding* van A naar B gedefinieerd. In plaats van afbeelding zegt men ook wel *functie*. In het Engels heet een afbeelding een *map* of *function*.

Door middel van een afbeelding van A naar B wijst elk element van A dus een element van B aan. Een element van B kan vaker aangewezen worden. Een element van A kan niet meer dan één element van B aanwijzen. Wij zullen ons meestal bedienen van deze terminologie van aanwijzen. Dit komt ook overeen met een veelgebruikte manier om een afbeelding van A naar B te visualiseren door middel van een tekening waarin vanuit elk punt van een getekende verzameling A een pijl vertrekt die aankomt in een van de punten van de getekende verzameling B.



Zo'n plaatje heet ook wel een *pijlendiagram*.

Een afbeelding bestaat dus uit een drietal: een verzameling A, een verzameling B, en een beschrijving die aangeeft hoe de aanwijzing van elementen van B door de elementen van A er uitziet.

Korten we die beschrijving af door een letter, bijvoorbeeld f, dan is de afbeelding dus het drietal (A, B, f).

A heet het *domein* van f (Engels: *domain*),

B heet het *bereik* van f (Engels: *range*).

Andere gebruikte namen zijn: A is het *brontype* (Engels: *source type*) van f, B is het *bestemmingstype* (Engels: *target type*) of *codomein* (Engels: *codomain*) van f.

Een suggestieve en zeer vaak gebruikte notatie is

$$f : A \to B.$$

Alhoewel de pijl hier verward zou kunnen worden met de logische pijl, staat de context er vrijwel altijd borg voor dat zulks niet gebeurt. De combinatie $A \to B$ van domein er bereik heet wel het *type* van de afbeedling f.

Is x een element van A, dan duidt $f(x)$ het *beeld* van x aan (Engels: *image*), het element van B dat door x wordt aangewezen. Het element x heet dan wel het *argument* van de afbeelding.

Twee afbeeldingen $f : A \to B$ en $g : C \to D$ zijn aan elkaar *gelijk* (zijn dus dezelfde afbeelding), precies dan als aan drie voorwaarden voldaan is:

$$A = C,\ B = D,\ \forall x \in A\ \langle f(x) = g(x)\rangle.$$

Enkele voorbeelden van afbeeldingen zijn

- $A = \mathbf{R}$, $B = \mathbf{R}$, voor alle $x \in \mathbf{R}$ is $f(x) = \sin(x)$
- $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, $f(1) = b$, $f(2) = d$, $f(3) = b$ $\qquad (*)$
- $A = \mathbf{N}$, $B = \{2, 3, 5, 7\}$, voor alle $n \in \mathbf{N}$ is $f(n) = 5$

In het vervolg zullen we het tweede voorbeeld $(*)$ nog een aantal keren aanhalen.
Enkele gevallen waarin we niet met een afbeelding van doen hebben, zijn:

- $A = \mathbf{R}$, $B = \mathbf{R}$, $f(x) = \ln(x)$
  want $\ln(x)$ is niet voor elke $x \in \mathbf{R}$ gedefinieerd
- $A = \mathbf{N}$, $B = \mathbf{Q}$, $f(x) = \sqrt{x}$
  want $\sqrt{2} \notin \mathbf{Q}$

Bij een afbeelding $f : A \to B$ en een deelverzameling X van A kunnen we kijken naar de deelverzameling van B bestaande uit de beelden van alle elementen van X. Deze deelverzameling van B heet het *beeld* van X, en wordt aangeduid met $f(X)$.

$$f(X) = \{y \in B |\ \exists x \in X\ \langle y = f(x)\rangle\}$$

Merk op dat zowel de notatie als de terminologie hiervan overeenkomt met het beeld van een element. Uit de context moet dus worden opgemaakt om welk van de twee begrippen het gaat: als x een element is van A dan is $f(x)$ het bijbehorende element van B; als x een deelverzameling is van A dan is $f(x)$ de deelverzameling van B bestaande uit bij die deelverzameling horende elementen van B.

In voorbeeld $(*)$ hebben we onder andere

$$f(\{1\}) = \{b\},\ f(\{1,2\}) = \{b,d\},\ f(\{1,3\}) = \{b\},\ f(A) = \{b,d\}$$

De verzameling $f(A)$ wordt wel het *beeld* van f genoemd (Engels: *image*).

Ook kunnen we bij een deelverzameling Y van B vragen naar de deelverzameling van A bestaande uit alle x waarvoor $f(x) \in Y$. Deze deelverzameling heet het *volledig origineel* (Engels: *inverse image*) van Y, en wordt aangeduid met $f^{-1}(Y)$.

$$f^{-1}(Y) = \{x \in A|\ f(x) \in Y\}.$$

We kijken weer naar het voorbeeld $(*)$. Hier geldt:

$$\begin{array}{llll} f^{-1}(\{a\}) = \emptyset, & f^{-1}(\{c\}) = \emptyset, & f^{-1}(\{a,b\}) = \{1,3\}, & f^{-1}(\{a,d\}) = \{2\}, \\ f^{-1}(\{b\}) = \{1,3\}, & f^{-1}(\{d\}) = \{2\}, & f^{-1}(\{a,c\}) = \emptyset, & f^{-1}(\{b,d\}) = A \end{array}$$

Wanneer de deelverzameling Y van B bestaat uit slechts één element, schrijft men gewoonlijk $f^{-1}(y)$ in plaats van $f^{-1}(\{y\})$. Dus:

- als x een element is van A dan is $f(x)$ een element van B,
- als X een deelverzameling is van A dan is $f(X)$ een deelverzameling van B,
- als y een element is van B dan is $f^{-1}(y)$ een deelverzameling van A,
- als Y een deelverzameling is van B dan is $f^{-1}(Y)$ een deelverzameling van A.

Een speciale situatie ontstaat als we voor een deelverzameling X van A kijken naar het volledig origineel van het beeld van X, of als we voor een deelverzameling Y van B kijken naar het beeld van het volledig origineel van Y.

Stelling 6.1 Zij $f : A \to B$ een afbeelding. Dan gelden

1. $f^{-1}(B) = A$
2. Als $X \subseteq A$, dan $X \subseteq f^{-1}(f(X))$
3. Als $Y \subseteq B$, dan $f(f^{-1}(Y)) \subseteq Y$

Bewijs:

Bewijs van (1):

Kies $x \in f^{-1}(B)$ willekeurig. Dan geldt $x \in A$. Dus $f^{-1}(B) \subseteq A$.

Kies omgekeerd $x \in A$ willekeurig. Dan $f(x) \in B$, dus $x \in f^{-1}(B)$. Dus $A \subseteq f^{-1}(B)$.

Met beide resultaten samen hebben we $f^{-1}(B) = A$, einde bewijs van (1).

Bewijs van (2):

Kies $x \in X$ willekeurig. Dan $f(x) \in f(X)$. Dus $x \in \{x \in A | f(x) \in f(X)\} = f^{-1}(f(X))$. Dus $X \subseteq f^{-1}(f(X))$, einde bewijs van (2).

Bewijs van (3):

Kies $z \in f(f^{-1}(Y))$ willekeurig. Dan is er een $x \in f^{-1}(Y)$ met $z = f(x)$. Vanwege $x \in f^{-1}(Y)$ geldt $f(x) \in Y$. Vanwege $z = f(x)$ geldt $z \in Y$. Hiermee is bewezen $f(f^{-1}(Y)) \subseteq Y$, einde bewijs van (3).

Einde Bewijs.

Een zeer vaak gemaakte fout is te menen dat

$$f(f^{-1}(Y)) = Y \quad \text{en dat} \quad f^{-1}(f(X)) = X.$$

Dat dit niet waar is illustreren we met behulp van het voorbeeld $(*)$: daarin geldt

$$f(f^{-1}(\{a, d\})) = f(\{2\}) = \{d\} \neq \{a, d\}$$

en

$$f^{-1}(f(\{1\})) = \{1, 3\} \neq \{1\}.$$

6.1 Injectieve, surjectieve en bijectieve afbeeldingen

Vaak bekijkt men afbeeldingen $f : A \to B$ die aan speciale eisen voldoen. We laten een drietal van zulke extra eisen de revue passeren.

Een afbeelding $f : A \to B$ heet *injectief* als geen twee verschillende elementen van A eenzelfde element van B aanwijzen, dus als

$$\neg(\exists x \in A \exists y \in A \ \langle x \neq y \wedge f(x) = f(y) \rangle)$$

oftewel

$$\forall x \in A \forall y \in A \ \langle f(x) = f(y) \to x = y \rangle.$$

Nog weer anders gezegd: voor elk element $z \in B$ bestaat $f^{-1}(z)$ uit hoogstens één element.

Een injectieve afbeelding heet ook wel een *injectie*.

Als je wilt bewijzen dat $f : A \to B$ injectief is, kies je willekeurig twee elementen $x, y \in A$ waarvoor je aanneemt dat $f(x) = f(y)$. Als je dan kunt bewijzen dat $x = y$, heb je volgens 'introductie $\forall$' en deductie bewezen dat

$$\forall x \in A \forall y \in A \ \langle f(x) = f(y) \to x = y \rangle,$$

oftewel dat f injectief is.

Als je daarentegen twee verschillende elementen $x, y \in A$ kunt vinden waarvoor geldt dat $f(x) = f(y)$, dan heb je daarmee juist bewezen dat $f : A \to B$ niet injectief is.

Een afbeelding $f : A \to B$ heet *surjectief* als elk element van B optreedt als beeld, dus als

$$\forall z \in B \exists x \in A \ \langle f(x) = z \rangle.$$

Anders gezegd: voor elk element $z \in B$ bestaat $f^{-1}(z)$ uit minstens één element. Nog korter gezegd: $f(A) = B$.

Een surjectieve afbeelding heet ook wel een *surjectie*.

Als je wilt bewijzen dat $f : A \to B$ surjectief is, kies je een willekeurig element $z \in B$. Als je daarvoor een element $x \in A$ kunt vinden waarvoor geldt $f(x) = z$ heb je volgens 'introductie $\forall$' en 'introductie $\exists$' bewezen dat

$$\forall z \in B \exists x \in A \ \langle f(x) = z \rangle,$$

oftewel dat f surjectief is.

Als je een element $z \in B$ kunt vinden dat voor geen enkel element $x \in A$ te schrijven is als $z = f(x)$, dan heb je daarmee juis bewezen dat f niet surjectief is.

Een afbeelding $f : A \to B$ heet *bijectief* als hij injectief en surjectief is. Dus als elk element van B optreedt als beeld van precies één element van A. Preciezer gezegd: voor elk element $z \in B$ bestaat $f^{-1}(z)$ uit precies één element.

Een bijectieve afbeelding heet ook wel een *bijectie*.

Als voorbeeld beschouwen we de afbeelding $s : \mathbf{N} \to \mathbf{N}$ gedefinieerd door $s(x) = x + 1$ voor alle $x \in \mathbf{N}$. Deze afbeelding heet de *successor*.

Deze afbeelding is injectief, want uit $s(x) = s(y)$ concluderen we $x + 1 = y + 1$ en daaruit volgt $x = y$.

Deze afbeelding is niet surjectief, want voor $0 \in \mathbf{N}$ bestaat er geen $x \in \mathbf{N}$ waarvoor geldt $s(x) = 0$.

Omdat de afbeelding s niet surjectief is, is s ook niet bijectief.

Het voorbeeld $(*)$ is niet injectief, want daar geldt $f(1) = b = f(3)$. Het voorbeeld $(*)$ is ook niet surjectief, want de elementen a en c treden niet op als beeld van f.

Intuïtief betekent injectiviteit dat er bij het toepassen van de afbeelding geen informatie verloren gaat. In de informatica is dit bijvoorbeeld essentieel bij *datacompressie*: je wilt een file in minder geheugen opslaan dan hij zelf beslaat, maar wel zodanig dat de oorspronkelijke file exact te reconstrueren valt uit de gecomprimeerde versie. In feite heb je hier met een afbeelding te maken: datacompressie is het toepassen van een afbeelding op een file. Zowel het domein als het bereik van deze afbeelding is de verzameling van alle mogelijke files. Deze afbeelding is bruikbaar als datacompressie als voor grote files van een veelvoorkomend type geldt dat hun beeld onder deze afbeelding aanzienlijk kleiner is. Maar heel essentieel is ook dat er een *decompressie*-afbeelding bestaat die de oorspronkelijke file exact reconstrueert. Als de afbeelding f die de datacompressie beschrijft niet injectief is zal dit nooit lukken. Dan bestaan er namelijk verschillende files x en y met $f(x) = f(y)$. Aan de hand van de gecomprimeerde versie $f(x) = f(y)$ is het dan onmogelijk vast te stellen of de oorspronkelijke file nou x geweest is of y, of misschien nog wel wat anders.

Precies hetzelfde speelt bij *encryptie*: je wilt een boodschap zodanig versleutelen dat hij voor buitenstaanders niet toegankelijk is. De rechtmatige ontvanger beschikt over een *sleutel* waarmee de oorspronkelijke boodschap weer uit de versleutelde versie te reconstrueren

is. Om precies dezelfde reden als hierboven kan dat alleen als de versleutelingsafbeelding injectief is.

In Stelling 6.1 hebben we twee inclusies gezien die in het algemeen geen gelijkheden waren. We laten nu zien dat ze dat wel zijn als de betreffende afbeeldingen respectievelijk injectief en surjectief zijn.

Stelling 6.2 Als $f : A \to B$ een injectieve afbeelding is, en X een deelverzameling van A is, dan is $f^{-1}(f(X)) = X$.

Bewijs:

In Stelling 6.1 hebben we al bewezen dat $X \subseteq f^{-1}(f(X))$; we hoeven nu alleen nog te bewijzen dat $f^{-1}(f(X)) \subseteq X$.

Kies daartoe $x \in f^{-1}(f(X))$ willekeurig.

Volgens de definitie van f^{-1} geldt dan $f(x) \in f(X)$.

Volgens de definitie van $f(X)$ is er dan een $y \in X$ met $f(x) = f(y)$.

Omdat f injectief is geldt dan $x = y$.

Omdat $y \in X$ is hiermee bewezen dat $x \in X$.

Hiermee is bewezen dat $f^{-1}(f(X)) \subseteq X$.

Einde Bewijs.

Stelling 6.3 Als $f : A \to B$ een surjectieve afbeelding is, en Y een deelverzameling van B is, dan is $f(f^{-1}(Y)) = Y$.

Bewijs:

In Stelling 6.1 hebben we al bewezen dat $f(f^{-1}(Y)) \subseteq Y$; we hoeven nu alleen nog te bewijzen dat $Y \subseteq f(f^{-1}(Y))$.

Kies daartoe $y \in Y$ willekeurig.

Omdat ook $y \in B$ en f surjectief is, is er een $x \in A$ met $f(x) = y$.

Volgens de definitie van f^{-1} geldt dan $x \in f^{-1}(Y)$.

Daaruit volgt dat $f(x) \in f(f^{-1}(Y))$.

Omdat $f(x) = y$ geldt nu $y \in f(f^{-1}(Y))$.

Hiermee is bewezen dat $Y \subseteq f(f^{-1}(Y))$.

Einde Bewijs.

6.2 Enkele speciale afbeeldingen

Bij elke verzameling A bestaat er een afbeelding van A naar A waarbij elk element van A zichzelf aanwijst. Men noemt deze afbeelding de *identieke afbeelding* of kortweg de *identiteit* op A en noteert haar door $\mathrm{id}_A : A \to A$. Voor elk element x van A geldt dus $\mathrm{id}_A(x) = x$.
Soms gebruikt men ook wel de notatie 1_A inplaats van id_A. Als er geen verwarring kan bestaan over wat de verzameling A is, wordt ook wel alleen maar 'id' geschreven.

Is A een deelverzameling van de verzameling B, dan heeft men de afbeelding van A naar B waarbij elk element van A zichzelf aanwijst. Deze afbeelding heet de *inclusie-afbeelding* van A in B, en wordt aangegeven met de notatie $\mathrm{i}_{AB} : A \to B$.

In het bijzonder geldt $\mathrm{i}_{AA} = \mathrm{id}_A$, maar als $A = B$ gebruiken we bij voorkeur de notatie id_A.

Werkend in een universum U beschrijft men een verzameling A wel door zijn *karakteristieke functie* $\chi_A : U \to \{0, 1\}$, die gedefinieerd is door:

$$\text{voor elke } x \in A \text{ is } \chi_A(x) = 1 \text{ en voor elke } x \notin A \text{ is } \chi_A(x) = 0.$$

Omgekeerd kan men iedere afbeelding $f : U \to \{0, 1\}$ zien als karakteristieke functie, namelijk $f = \chi_{f^{-1}(1)}$.
Dus bij f hoort de verzameling $A = \{x|\ f(x) = 1\}$.

Een zeer speciale situatie ontstaat wanneer men wil spreken over een afbeelding $f : A \to B$ in het geval dat $A = \emptyset$ of $B = \emptyset$.

Is $A \neq \emptyset$ en $B = \emptyset$, dan bestaat er geen afbeelding van A naar B, immers men kan bij een element van A geen element van B aanwijzen.

Is echter $A = \emptyset$, dan spreekt men wel over de *lege afbeelding* van A naar B. Hierbij mag B een willekeurige verzameling zijn.

De lege afbeelding is een abstract concept, dat wordt gebruikt om allerlei regels door te laten gaan, zoals bijvoorbeeld in de nu volgende sectie.

6.3 Afbeeldigen op eindige verzamelingen

We gaan nu het geval bekijken waarin de verzamelingen A en B beide
eindig veel elementen hebben. We zeggen dan dat A en B *eindige verzamelingen* zijn. Het aantal elementen van A, respectievelijk van B duiden we aan met $\#A$ en $\#B$. Andere notaties hiervoor zijn $|A|$ en $|B|$. Om aan te geven dat A eindig is wordt wel geschreven $\#A < \infty$.

Dan kan men een afbeelding van A naar B volledig vastleggen door de elementen van A op een rij te zetten, en onder elk element te schrijven welk element van B erdoor wordt aangewezen. Op deze manier opgeschreven ziet het inmiddels beroemde voorbeeld $(*)$ er als volgt uit

$$\begin{pmatrix} 1 & 2 & 3 \\ b & d & b \end{pmatrix} \text{ of bijvoorbeeld als } \begin{pmatrix} 2 & 1 & 3 \\ d & b & b \end{pmatrix}$$

Als we een of andere vaste volgorde voor de bovenste rij (van alle elementen van A) kiezen, dan zien we aan de onderste rij dat een afbeelding $f : A \to B$ eigenlijk neerkomt op het *met terugleggen* kiezen van $\#A$ elementen uit de verzameling B. Als $\#A = m$ en $\#B = n$, kan dit op n^m manieren, en dat is dus ook het aantal afbeeldingen van A naar B. De *verzameling van afbeeldingen* van A naar B wordt wel genoteerd met B^A; deze notatie is gekozen omdat dan blijkbaar geldt

$$\#(B^A) = (\#B)^{\#A}.$$

Hier zien we ook dat het handig is om de *lege afbeelding* wel als afbeelding op te vatten. Dan geldt namelijk deze formule ook als $A = \emptyset$, immers dan is $\#A = 0$, en de formule zegt dat er één afbeelding zou moeten zijn, want $(\#B)^0 = 1$. Inderdaad: de lege afbeelding.

Strict genomen geldt dit laatste alleen wanneer $B \neq \emptyset$, want 0^0 is niet gedefinieerd. In allerlei telproblemen, dus wanneer alleen natuurlijke getallen in het geding zijn, heeft men echter de gewoonte om $0^0 = 1$ te stellen.

In de voorstelling van afbeeldingen als twee rijen waarden is een afbeelding van A naar B injectief als alle elementen in de onderste rij (van elementen van B) verschillend zijn. Dat kan natuurlijk alleen als B tenminste m ($= \#A$) elementen heeft, en dan kiezen we dus eigenlijk *zonder terugleggen* m elementen uit de verzameling B van n elementen. Dat kan op $n!/(n-m)!$ manieren (n.b.: $0! = 1$); het aantal injectieve afbeeldingen van een verzameling met m elementen naar een verzameling met n elementen is dus precies $n!/(n-m)!$ als $n \geq m$, en 0 als $n < m$.

De surjectiviteit van een afbeelding van A naar B kenmerkt zich in deze voorstelling door het voorkomen van alle elementen van B in de onderste rij. Dat kan vanzelfsprekend alleen als er genoeg plaatsen zijn voor alle elementen van B, dus als $\#A \geq \#B$. Het is niet zo gemakkelijk uit te rekenen hoeveel surjectieve afbeeldingen $f : A \to B$ er zijn. Dat laten we hier dan ook maar schieten.

We kunnen wel uit het voorgaande concluderen dat er alleen mogelijkheden kunnen zijn voor bijectieve afbeeldingen $f : A \to B$ als $\#A = \#B$ (want injectiviteit vereist $\#A \leq \#B$ en surjectiviteit vereist $\#A \geq \#B$). Het aantal bijectieve afbeeldingen is dan het aantal mogelijkheden om de n elementen van B op een rij te zetten. Dat is $n!$. Een bijectieve afbeelding van een eindige verzameling naar zichzelf heet ook wel een *permutatie*. Het aantal permutaties op n elementen is dus precies $n!$.

Stelling 6.4 Laat A en B beide eindige verzamelingen zijn en $f : A \to B$. Dan geldt altijd

$$\#(f(A)) \leq \#A \quad \text{en} \quad \#(f(A)) \leq \#B.$$

Verder geldt

$$f \text{ is injectief} \iff \#(f(A)) = \#A,$$

en

$$f \text{ is surjectief} \iff \#(f(A)) = \#B.$$

Als bovendien geldt $\#A = \#B$, dan geldt

$$f \text{ is injectief} \iff f \text{ is bijectief} \iff f \text{ is surjectief}.$$

De geldigheid van de laatste bewering volgt direct uit de karakteriseringen van injectief en surjectief. De geldigheid van de overige beweringen is eenvoudig in te zien; wij ontwikkelen geen verdere notaties om dit in meer detail op te kunnen schrijven.

In het bijzonder geldt dus dat voor eindige verzamelingen A voor afbeeldingen $f : A \to A$ de begrippen injectief, surjectief en bijectief samenvallen. Voor oneindige verzamelingen is dat niet meer het geval, zo is $f : \mathbf{N} \to \mathbf{N}$ gedefinieerd door $f(x) = x + 1$ voor alle $x \in \mathbf{N}$ wel injectief maar niet surjectief.

Bij het redeneren over eindige verzamelingen speelt het *duiventilprincipe* (Engels: *pigeon hole principle*) vaak een belangrijke rol; in het eerste hoofdstuk is het ook al aan de orde geweest. Wij formuleren dit in een stelling:

Stelling 6.5 (Pigeon hole principle)
Laat n, k een natuurlijke getallen ongelijk aan 0 zijn.
Als de vereniging van n verzamelingen meer dan $k * n$ elementen bevat, dan moet tenminste een van die verzamelingen $k + 1$ of meer elementen bevatten.

Immers, als elke verzameling hoogstens k elementen bevat, dan is het totale aantal elementen hoogstens $k * n$.

6.4 Samenstellen van afbeeldingen

Laten $f : A \to B$ en $g : B \to C$ afbeeldingen zijn. Let er goed op dat het bereik van f tevens het domein van g is. Dan kan men voor elke $x \in A$ een element in C aanwijzen door $g(f(x))$. Zo wijzen we voor elke $x \in A$ één element in C aan, dus is er sprake van een afbeelding van A naar C.

Deze afbeelding heet de *samenstelling* van f gevolgd door g, en wordt genoteerd met $g \circ f : A \to C$.

Merk op dat $g \circ f$ alleen gedefinieerd is als

$$(\text{bereik van } f) = (\text{domein van } g).$$

Om aan te geven hoe $g \circ f$ ontstaan is, gebruikt men wel het diagram

$$A \xrightarrow{f} B \xrightarrow{g} C$$

De volgorde in de notatie is precies omgekeerd aan de volgorde in de omschrijving "f gevolgd door g". Dat is bewust zo gekozen, omdat we altijd $(g \circ f)(x)$ schrijven voor het beeld van x, en dan is het gemakkelijk als we voor de definitie van $(g \circ f)(x)$ kunnen opschrijven $(g \circ f)(x) = g(f(x))$.

Als $f : B \to C$ een afbeelding is, en A is een deelverzameling van B dan heet de samenstelling $f \circ \mathrm{i}_{AB} : A \to C$ de afbeelding f *beperkt tot* A. Men heeft dan het domein van f beperkt tot A. Dit komt zo vaak voor, dat er een speciale notatie voor is: $f_{|A}$.

Evenzo kan men, als $f : A \to B$ een afbeelding is en B een deelverzameling van C is, de samenstelling $\mathrm{i}_{BC} \circ f : A \to C$ bekijken. Men heeft dan het bereik van f uitgebreid tot C. Deze constructie is minder vaak noodzakelijk, zodat er geen speciale notatie voor is bedacht.

Ook merken we hier nog op dat voor de samenstellingen van een afbeelding $f : A \to B$ met de identiteiten $\mathrm{id}_A : A \to A$ en $\mathrm{id}_B : B \to B$ geldt

$$f \circ \mathrm{id}_A = f \quad \text{en} \quad \mathrm{id}_B \circ f = f$$

We zeggen dat de identiteit een *neutraal element* is met betrekking tot de samenstelling, net zoals

0 een neutraal element is met betrekking tot optelling,

1 een neutraal element is met betrekking tot vermenigvuldiging,

T een neutraal element is met betrekking tot conjunctie,

F een neutraal element is met betrekking tot disjunctie.

Stelling 6.6

- De samenstelling van twee injectieve afbeeldingen is weer een injectieve afbeelding.
- De samenstelling van twee surjectieve afbeeldingen is weer een surjectieve afbeelding.
- De samenstelling van twee bijectieve afbeeldingen is weer een bijectieve afbeelding.

Bewijs:

- Laten $f : A \to B$ en $g : B \to C$ injectieve afbeeldingen zijn.
  Kies willekeurige $x, x' \in A$.
  Stel dat $(g \circ f)(x) = (g \circ f)(x')$.
  Dan geldt $g(f(x)) = g(f(x'))$.
  Omdat g injectief is geldt dan $f(x) = f(x')$.
  Omdat f injectief is geldt dan $x = x'$.
  We hebben nu bewezen: $\forall x, x' \in A \, \langle (g \circ f)(x) = (g \circ f)(x') \to x = x' \rangle$.
  Hiermee is bewezen dat $g \circ f$ injectief is.
- Laten $f : A \to B$ en $g : B \to C$ surjectieve afbeeldingen zijn.
  Kies $z \in C$ willekeurig.
  Omdat g surjectief is, is er een $y \in B$ met $z = g(y)$.
  Omdat f surjectief is, is er een $x \in A$ met $y = f(x)$.
  Nu geldt $z = g(y) = g(f(x)) = (g \circ f)(x)$.
  We hebben nu bewezen: $\forall z \in C \exists x \in A \, \langle z = (g \circ f)(x) \rangle$.
  Hiermee is bewezen dat $g \circ f$ surjectief is.

- Laten $f : A \to B$ en $g : B \to C$ bijectieve afbeeldingen zijn.
  Omdat f en g injectief zijn is volgens bovenstaande ook $g \circ f$ injectief.
  Omdat f en g surjectief zijn is volgens bovenstaande ook $g \circ f$ surjectief.
  Hiermee is bewezen dat $g \circ f$ bijectief is.

Einde Bewijs.

Stelling 6.7 Laten $f : A \to B$ en $g : B \to C$ en $h : C \to D$ afbeeldingen zijn. Dan zijn $(h \circ g) \circ f : A \to D$ en $h \circ (g \circ f) : A \to D$ dezelfde afbeeldingen.

Bewijs:

Beide afbeeldingen hebben inderdaad A als domein en D als bereik.

Kies $x \in A$ willekeurig. Dan geldt:

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

Einde Bewijs.

Stelling 6.7 zegt dat samenstelling *associatief* is, daar waar de samenstelling goed gedefinieerd is.

Samenstelling is echter niet *commutatief*. Als voorbeeld beschouwen we $f, g : \mathbf{N} \to \mathbf{N}$, gedefinieerd door

$$f(x) = x + 1 \quad \text{en} \quad g(x) = 2x$$

voor alle $x \in \mathbf{N}$. Dan zijn $f \circ g$ en $g \circ f$ beide gedefinieerd, maar niet gelijk, want

$$(f \circ g)(1) = f(g(1)) = f(2) = 3 \neq 4 = g(2) = g(f(1)) = (g \circ f)(1).$$

Om een afbeelding $f : A \to B$ samen te stellen met een afbeelding $g : C \to D$ tot een nieuwe afbeelding $g \circ f : A \to D$, hebben we $B = C$ geëist. Het gaat er om dat $g(f(x))$ voor iedere $x \in A$ gedefinieerd is. Dat is het geval als $B \subseteq C$.

Men zou dus eigenlijk al de samenstelling $g \circ f : A \to D$ kunnen maken als $B \subseteq C$.

Toch laten we dat niet toe. Wat in zo'n geval wel het gewenste resultaat oplevert is de samenstelling $g \circ \mathrm{i}_{BC} \circ f$ met diagram

$$A \xrightarrow{f} B \xrightarrow{\mathrm{i}_{BC}} C \xrightarrow{g} D$$

In feite is dit dus de samenstelling $g_{|B} \circ f$.

Het samenstellen van afbeeldingen is een van de pijlers van *functioneel programmeren*. Dat is een manier van programmeren met behulp van een *functionele programmeertaal* waarin je er naar streeft om alle operaties die je doet als *functie* te beschrijven. Daarbij is een functie een afbeelding die gedefinieerd is op een manier waarmee je het resultaat ook kunt berekenen. Het domein en het bereik vormen dan het *type* van de functie. Een

element van het domein waar je een functie op los kunt laten heet dan een *parameter*. De verzameling B^A van afbeeldingen van een verzameling A naar een verzameling B kan zelf weer het domein of het bereik van een andere afbeelding zijn. Op soortgelijke wijze kun je in een functionele programmeertaal functies beschrijven waarvan een parameter zelf weer een functie is, of waarvan het resultaat een functie is.

We komen nog even terug op *datacompressie*: je wilt een file in veel gevallen in minder geheugen opslaan dan hij zelf beslaat, maar wel zodanig dat de oorspronkelijke file exact te reconstrueren valt uit de gecomprimeerde versie. Deze reconstructie noemen we *decompressie*. Als we de afbeelding die de datacompressie beschrijft f noemen en de afbeelding die de decompressie beschrijft g, dan is de hierboven geformuleerde eis compact op te schrijven als

$$g \circ f = \mathrm{id}.$$

We hadden al eerder opgemerkt dat zo'n datacompressie-afbeelding f injectief moet zijn. Dit kunnen we nu inderdaad uit deze eis afleiden. Neem twee willekeurige files x en y en stel dat $f(x) = f(y)$. Met gebruikmaking van de eis leiden we nu af

$$x = \mathrm{id}(x) = (g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y) = \mathrm{id}(y) = y.$$

Hiermee is bewezen dat f injectief is.

Omgekeerd is de decompressie altijd surjectief. Neem namelijk een willekeurige file x. Dan geldt

$$x = \mathrm{id}(x) = (g \circ f)(x) = g(f(x)),$$

oftewel er is een file y met $x = g(y)$. Hiermee is bewezen dat g surjectief is.

Precies hetzelfde geldt voor *encryptie* en *decryptie*: de encryptie-afbeelding f die een willekeurige boodschap versleuteld tot iets wat buitenstaanders niet kunnen ontcijferen is altijd injectief; de decryptie-afbeelding g die alleen bij de rechtmatige ontvanger bekend is en de versleutelde boodschap ontcijfert tot de oorspronkelijke boodschap, is altijd surjectief.

6.5 Inverse afbeeldingen en dekpunten

Als een afbeelding $f : A \to B$ bijectief is, dan kan men een speciale afbeelding maken van B naar A, door bij elke $y \in B$ de $x \in A$ aan te wijzen waarvoor geldt $y = f(x)$.

Deze uniek bepaalde afbeelding heet de *inverse* van f en wordt wel genoteerd met $f^{-1} : B \to A$.

Ook $f^{-1} : B \to A$ is een bijectieve afbeelding, want bij elke $x \in A$ is er precies één $y \in B$ met $f^{-1}(y) = x$, namelijk $y = f(x)$.

Men kan f en f^{-1} op twee manieren samenstellen:

$$f^{-1} \circ f : A \to A \quad \text{en} \quad f \circ f^{-1} : B \to B.$$

Volgens de definitie geldt

$$f^{-1} \circ f = \mathrm{id}_A \quad \text{en} \quad f \circ f^{-1} = \mathrm{id}_B.$$

Dit verklaart ook het gebruik van het woord *inverse*: algemener wordt dit woord gebruikt voor elke situatie waarin een operator losgelaten op een element en zijn inverse als resultaat het neutrale element geeft. Zo is $-x$ de inverse van een willekeurig reëel getal x met betrekking tot de optelling, en is $1/x$ de inverse van een willekeurig reëel getal $x \neq 0$ met betrekking tot de vermenigvuldiging.

Eerder in dit hoofdstuk zijn we dezelfde notatie f^{-1} tegengekomen in een geheel andere betekenis, namelijk om het *volledig origineel* van een deelverzameling van het bereik van f aan te duiden. Uit de context blijkt meestal wel wat met f^{-1} wordt bedoeld. In het geval dat $f : A \to B$ een bijectieve afbeelding is en $Y \subseteq B$ hebben we echter twee verschillende definities van $f^{-1}(Y)$ gegeven:

vroeger: $f^{-1}(Y) = \{x \in A | f(x) \in Y\}$,

nu: $f^{-1}(Y) = \{x \in A | \exists y \in Y \langle x = f^{-1}(y)\rangle\}$.

Gelukkig zijn beide verzamelingen gelijk vanwege

$$f(x) \in Y \;\Leftrightarrow\; \exists y \in Y \langle f(x) = y\rangle \;\Leftrightarrow\; \exists y \in Y \langle x = f^{-1}(y)\rangle.$$

Een speciale situatie ontstaat, wanneer we afbeeldingen bekijken van een verzameling A naar A zelf. In dit geval kunnen we elke twee afbeeldingen $f : A \to A$ en $g : A \to A$ samenstellen, en wel op twee manieren, namelijk tot $f \circ g : A \to A$ en tot $g \circ f : A \to A$. We hebben al gezien dat in het algemeen deze samenstellingen een verschillend resultaat geven: samenstelling is niet commutatief.

Ook kan men een afbeelding $f : A \to A$ meervoudig met zichzelf samenstellen. Dan gebruiken we de notatie f^2 voor $f \circ f$, f^3 voor $f \circ f \circ f$, en in het algemeen f^m voor de m-voudige samenstelling van f met zichzelf. Ook komt men wel eens f^1 en f^0 tegen, in de betekenis van respectievelijk f en id_A.

Bij een afbeelding $f : A \to A$ zijn er soms elementen a van A waarvoor $f(a) = a$. Zo'n element heet een *dekpunt* van f, in het Engels *fixed point*.

We geven een paar voorbeelden.

Voorbeeld:
$A = \mathbf{R}$, $f(x) = x + 1$. Hier zijn geen dekpunten, want de vergelijking $f(x) = x$, dus $x + 1 = x$, heeft geen oplossingen.

Voorbeeld:
$A = \mathbf{R}$, $f(x) = x^2 - 1$. Hier zijn twee dekpunten, namelijk de twee oplossingen van de vergelijking $x = x^2 - 1$: $a = (1 + \sqrt{5})/2$ en $b = (1 - \sqrt{5})/2$.

Voorbeeld:
$A = \mathbf{Z}$, $f(x) = x^2 - 1$. Hier zijn geen dekpunten, want de enige reële oplossingen van de vergelijking $x = x^2 - 1$ zijn de a en b uit het vorige voorbeeld, maar dat zijn geen gehele getallen.

Voorbeeld:
$A = \mathbf{Z} \times \mathbf{Z}$, $f(m, n) = (m - m * n,\ n - m)$. Dekpunten zijn hier alle paren $(0, n)$.

Dekpunten kunnen soms worden gebruikt om ingewikkelder dingen te definiëren dan wat je aan kunt. Stel je voor dat je de afbeelding $p : \mathbf{N} \to \mathbf{N}$ wilt definiëren waarvoor $p(x) = 2^x$ voor alle $x \in \mathbf{N}$, maar dan zonder gebruik te maken van machtsverheffen. De cruciale eigenschap van p is dat $p(0) = 1$ en $p(x+1) = 2 * p(x)$ voor alle $x \in \mathbf{N}$. Met deze eigenschap in gedachten definiëren we een afbeelding

$$\Phi : \mathbf{N}^{\mathbf{N}} \to \mathbf{N}^{\mathbf{N}}.$$

De afbeelding Φ wordt gedefinieerd door een willekeurige afbeelding $f : \mathbf{N} \to \mathbf{N}$ te nemen en daarvoor te definiëren wat $\Phi(f)$ is. Dat moet zelf ook weer een afbeelding van $\mathbf{N}$ naar $\mathbf{N}$ worden, die op haar beurt gedefinieerd wordt door er een willekeurig natuurlijk getal in te stoppen. Zo'n natuurlijk getal is altijd òf 0, òf van de vorm $x + 1$. Met de eigenschap van p in gedachten definiëren we

$$\begin{array}{lcl} (\Phi(f))(0) & = & 1 \\ (\Phi(f))(x+1) & = & 2 * (\Phi(f))(x) \quad \text{voor alle } x \in \mathbf{N}. \end{array}$$

Hiermee is voor elke $f : \mathbf{N} \to \mathbf{N}$ een afbeelding $\Phi(f) : \mathbf{N} \to \mathbf{N}$ gedefinieerd, waarmee inderdaad

$$\Phi : \mathbf{N}^{\mathbf{N}} \to \mathbf{N}^{\mathbf{N}}.$$

We hebben dit zo gedaan dat de beoogde afbeelding p een dekpunt is van Φ: volgens de eigenschap van p geldt $\Phi(p) = p$. Met theorie die we hier niet verder zullen behandelen kun je bewijzen dat een op een dergelijke manier gedefinieerde afbeelding Φ altijd precies één dekpunt heeft. Met die theorie kunnen we nu dus p definiëren als het enige dekpunt van Φ. Op deze wijze hebben we een definitie van de beoogde afbeelding p gegeven zonder daarbij gebruik te maken van machtsverheffen. Dit kunnen we zien als een *inductieve definitie* zoals we die in sectie 7.1 nader zullen beschouwen.

Dit ziet er op het eerste gezicht erg ingewikkeld uit, en onnodig omslachtig omdat iedereen toch al vertrouwd is met machtsverheffen. In diverse takken van de theoretische informatica zijn soortgelijke methoden om ingewikkelde dingen te definiëren door middel van dekpunten, echter zeer vruchtbaar gebleken. In het bijzonder noemen we in dit verband het definiëren van de precieze betekenis van een programmeertaal: de *semantiek*.

6.6 Opgaven

Opgave 6.1

Laat $f, g : \mathbf{N} \to \mathbf{N}$ gedefinieerd zijn door

$$f(2x) = x \quad \text{en} \quad f(2x+1) = x \quad \text{en} \quad g(x) = 2x$$

voor alle $x \in \mathbf{N}$.

a. Is f injectief?

b. Is f surjectief?

c. Is g injectief?

d. Is g surjectief?

Geef voor alle vier antwoorden een bewijs.

Opgave 6.2

Laat $f : A \to B$ een afbeelding zijn, en X en Y deelverzamelingen van A.

a. Bewijs: $f(X \cup Y) = f(X) \cup f(Y)$.

b. Bewijs: $f(X \cap Y) \subseteq f(X) \cap f(Y)$.

c. Geef een voorbeeld waaruit blijkt dat $f(X \cap Y) = f(X) \cap f(Y)$ niet altijd juist is, en geef een voorwaarde voor f waaronder dit wel geldt.

Opgave 6.3

Laat $f : A \to B$ een afbeelding zijn, en Y een deelverzameling van B met $f(A) \subseteq Y$. Laat $g : A \to Y$ de afbeelding zijn waarvoor $g(x) = f(x)$ voor alle $x \in A$. Gegeven is dat g surjectief is. Bewijs dat $f(A) = Y$.

Opgave 6.4

Laat $f : A \to B$ een afbeelding zijn, en U en V deelverzamelingen van B. Bewijs:

a. $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$

b. $f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$

c. $f^{-1}(B - U) = A - f^{-1}(U)$

Opgave 6.5

a. Is een inclusie-afbeelding altijd injectief?

b. Is een inclusie-afbeelding altijd surjectief?

c. Is een identieke afbeelding altijd injectief?

d. Is een identieke afbeelding altijd surjectief?

Geef voor alle vier antwoorden een bewijs.

Opgave 6.6

Laat $f : A \to B$ een afbeelding zijn. Bewijs:

a. Voor $X \subseteq A$ geldt $f(f^{-1}(f(X))) = f(X)$

b. Voor $Y \subseteq B$ geldt $f^{-1}(f(f^{-1}(Y))) = f^{-1}(Y)$

Opgave 6.7

Laat $f, g : \mathbf{N} \to \mathbf{N}$ gedefinieerd zijn door

$$f(x) = x + 1 \quad \text{en} \quad g(x) = 2x$$

voor alle $x \in \mathbf{N}$. Bewijs dat

$$f \circ f \circ g = g \circ f.$$

Opgave 6.8

Gegeven zijn $A = \{1, 2, 3, 4\}$ en $B = \{a, b, c\}$. De afbeelding $f : A \to B$ is gegeven door $f(1) = a$, $f(2) = b$, $f(3) = c$, $f(4) = b$.

Geef een opsomming van alle afbeeldingen $g : B \to A$ waarvoor geldt dat $f \circ g = id_B$, en bereken voor elk van die afbeeldingen de samenstelling $g \circ f$.

Opgave 6.9

Gegeven zijn $A = \{1, 2, 3, 4\}$ en $B = \{a, b, c\}$. De afbeelding $f : B \to A$ is gegeven door $f(a) = 1$, $f(b) = 2$, $f(c) = 3$.

Geef een opsomming van alle afbeeldingen $g : A \to B$ waarvoor geldt dat $g \circ f = id_B$, en bereken voor elk van die afbeeldingen de samenstelling $f \circ g$.

Opgave 6.10

Laat $f, g : \mathbf{N} \to \mathbf{N}$ gedefinieerd zijn door

$$f(2x) = x \quad \text{en} \quad f(2x + 1) = x \quad \text{en} \quad g(x) = 2x$$

voor alle $x \in \mathbf{N}$.

a. Geldt $f \circ g = id_{\mathbf{N}}$?

b. Geldt $g \circ f = id_{\mathbf{N}}$?

Geef voor beide antwoorden een bewijs.

Opgave 6.11

Gegeven zijn afbeeldingen $f : A \to B$ en $g : B \to C$. Bewijs:

a. Als $g \circ f$ surjectief is, dan is g surjectief.

b. Als $g \circ f$ injectief is, dan is f injectief.

Opgave 6.12

Gegeven zijn afbeeldingen $f, g : A \to B$ en $h, k : B \to C$.

a. Mag men uit $h \circ f = k \circ f$ concluderen dat $h = k$? Geef een bewijs of een tegenvoorbeeld.

Bewijs dat het zeker mag als f surjectief is.

b. Mag men uit $h \circ f = h \circ g$ concluderen dat $f = g$? Geef een bewijs of een tegenvoorbeeld.

Bewijs dat het zeker mag als h injectief is.

Opgave 6.13

Gegeven is $A = \{1, 2, 3, 4, 5\}$, en $f : A \to A$ is een afbeelding.
Bereken f^n voor $n = 0, 1, 2, 3, 4, 5$ en vergelijk ze met elkaar in de volgende gevallen:

a. $f(1) = 2$, $f(2) = 3$, $f(3) = 4$, $f(4) = 5$, $f(5) = 1$;

b. $f(1) = 2$, $f(2) = 1$, $f(3) = 4$, $f(4) = 5$, $f(5) = 3$;

c. $f(1) = 1$, $f(2) = 2$, $f(3) = 3$, $f(4) = 1$, $f(5) = 2$.

Opgave 6.14

Een afbeelding $f : A \to B$ bepaalt afbeeldingen $F_f : \mathcal{P}(A) \to \mathcal{P}(B)$ en $G_f : \mathcal{P}(B) \to \mathcal{P}(A)$ door voor $X \subseteq A$ en $Y \subseteq B$ te definiëren

$$F_f(X) = f(X) \quad \text{en} \quad G_f(Y) = f^{-1}(Y)$$

a. Bewijs: F_f is injectief dan en slechts dan als f injectief is.

b. Bewijs: F_f is surjectief dan en slechts dan als f surjectief is.

c. Bewijs: G_f is injectief dan en slechts dan als f surjectief is.

d. Bewijs: G_f is surjectief dan en slechts dan als f injectief is.

e. Laat aan de hand van een voorbeeld zien dat F_f en G_f in het algemeen niet elkaars inversen zijn.

Hoofdstuk 7

Volledige inductie

Van een deelverzameling V van de verzameling $\mathbf{N}$ van alle natuurlijke getallen veronderstellen we het volgende:

(i) $0 \in V$
(ii) $\forall k \in \mathbf{N}\langle k \in V \to k+1 \in V\rangle$

Dan is $V = \mathbf{N}$. Men ziet dit als volgt in:

$0 \in V$, want dat is gegeven in (i).
Dan ook $1 \in V$ wegens (ii).
Dan ook $2 \in V$ wegens (ii).
Dan ook $3 \in V$ wegens (ii).
En zo voort.

Hiermee is bewezen dat 1, 2 en 3 elementen van V zijn, verder nog niets. Maar ik zal ongetwijfeld zo voortgaand kunnen bewijzen dat 1000 een element van V is. Als iemand mij een getal noemt, kan ik (misschien moet ik het aan mijn opvolgers overlaten) laten zien dat dat getal tot V behoort. Daarmee is echter nog niet bewezen dat $V = \mathbf{N}$.

Daarvoor is nodig dat $\forall n \in \mathbf{N}\langle n \in V\rangle$ wordt bewezen. Maar dit is onmogelijk met de ons bekende bewijsmethoden: we willen gebruik maken van de nog niet geformuleerde eigenschap dat elk natuurlijk getal te bereiken is door te beginnen met 0 en vanaf daar een eindig aantal keren de opvolger te nemen. Omdat we dit principe willen gebruiken om de geldigheid van predicaten over natuurlijke getallen te bewijzen, formuleren we dit principe in de taal van predicaten. We noemen dit het *principe van volledige inductie*, en vatten dit op als een *axioma*, een basisprincipe waarvan we de geldigheid aannemen en dat we altijd mogen gebruiken. Het gebruik van dit principe noemen we *volledige inductie*, of kortweg *inductie*.

Principe van volledige inductie:
Zij P een predikaat, gedefinieerd op $\mathbf{N}$, waarvoor geldig zijn:

- $P(0)$, en
- $\forall k \in \mathbf{N}\langle P(k) \rightarrow P(k+1)\rangle$.

Dan geldt $\forall n \in \mathbf{N}\langle P(n)\rangle$.

Om hiermee te bewijzen dat een bewering $P(n)$ waar is voor alle $n \in \mathbf{N}$ moet je dus twee dingen doen:

- bewijs dat $P(0)$ waar is, en
- neem voor willekeurige $k \in \mathbf{N}$ aan dat $P(k)$ waar is, en bewijs dat dan ook $P(k+1)$ waar is.

De eerste stap heet wel de *basisstap*, de tweede stap de *inductiestap*. De aanname dat $P(k)$ waar is heet de *inductiehypothese*.

Als eerste voorbeeld bewijzen we met behulp van dit principe van volledige inductie dat inderdaad $V = \mathbf{N}$ voor een verzameling V die voldoet aan (i) en (ii). We definiëren

$$P(n) \equiv (n \in V).$$

Vanwege (i) geldt nu $P(0)$ en is aan de basisstap voldaan. Neem voor willekeurige $k \in \mathbf{N}$ aan dat $P(k)$ waar is, oftewel dat $k \in V$. Volgens (ii) geldt dan $k+1 \in V$, oftewel $P(k+1)$. Hiermee is de inductiestap bewezen. Volgens het principe van volledige inductie is nu inderdaad bewezen dat $P(n)$ waar is voor alle $n \in \mathbf{N}$, oftewel dat $\forall n \in \mathbf{N}\langle n \in V\rangle$. Hieruit concluderen we dat inderdaad $V = \mathbf{N}$.

Bij de volgende stellingen gaat het niet alleen om de stelling zelf, maar vooral om de manier waarop het bewijs gegeven wordt met behulp van het principe van volledige inductie.

Stelling 7.1 Voor elk natuurlijk getal n geldt $\displaystyle\sum_{m=0}^{n} m = n(n+1)/2$

Bewijs:

Zij $P(n)$ de uitspraak $\displaystyle\sum_{m=0}^{n} m = n(n+1)/2$.

Basisstap:

Voor $n = 0$ staat er $0 = (0 * 1)/2$, en dit is waar.

Dus $P(0)$ is waar, en de basisstap is voltooid.

Inductiestap:

Neem nu aan dat $P(k)$ waar is (de inductiehypothese).

Dat wil zeggen $\sum_{m=0}^{k} m = k(k+1)/2$.

Volgens de betekenis van notatie $\sum$ en de inductiehypothese is nu

$$\sum_{m=0}^{k+1} m = (\sum_{m=0}^{k} m) + k + 1 = k(k+1)/2 + k + 1.$$

Dit is gelijk aan $(k+1)(k+2)/2$ zodat inderdaad $P(k+1)$ geldt.

Hiermee is de inductiestap voltooid.

Nu is voldaan aan beide eisen van het principe van volledige inductie, zodat we mogen concluderen dat $P(n)$ geldt voor alle natuurlijke getallen n.

Einde Bewijs.

Stelling 7.2 Zij r een reëel getal waarvoor $r > -1$. Dan geldt voor elk natuurlijk getal n de ongelijkheid $(1+r)^n \geq 1 + n \cdot r$.

Bewijs:

Zij $P(n)$ de uitspraak $((1+r)^n \geq 1 + n \cdot r)$

1 $1 + r > 0$ wegens $r > -1$
2 $P(0)$ is waar, immers $(1+r)^0 = 1$ en $1 + 0 \cdot r = 1$
3 $P(k) \rightarrow P(k+1)$, immers
  3.1 Stel $P(k)$ is waar
  3.2 $(1+r)^{k+1} = (1+r)^k(1+r)$ (betekenis van machten)
  3.3 $(1+r)^k(1+r) \geq (1+kr)(1+r)$ wegens 1 en 3.1
  3.4 $(1+kr)(1+r) \geq 1 + (k+1)r$ want
    $(1+kr)(1+r) = 1 + kr + r + kr^2 =$
    $1 + (k+1)r + kr^2 \geq 1 + (k+1)r$
  3.5 $(1+r)^{k+1} \geq 1 + (k+1)r$ wegens 3.2, 3.3 en 3.4
  3.6 regel 3.5 is precies de uitspraak $P(k+1)$, dus regel 3 is waar

Met het principe van volledige inductie volgt nu uit 2 en 3 dat voor iedere n in $\mathbf{N}$ de uitspraak $P(n)$ waar is, dus is de stelling waar.

Einde Bewijs.

In het inleidende hoofdstuk hebben we aantal voorbeelden gezien van bewijzen met behulp van een *invariant*. Zo'n invariant is een bepaalde eigenschap. Daarbij was de aanname dat

- de invariant aan het begin geldt, en dat

- als de invariant geldt en er wordt vervolgens een stap gedaan, dan geldt na afloop van die stap de invariant weer.

De conclusie die we dan trokken was dat de invariant na het uitvoeren van een willekeurig eindig aantal stappen altijd geldt. Destijds hebben we dat als principe geformuleerd en aannemelijk gemaakt; nu kunnen we de geldigheid van dit invariantenprincipe bewijzen met volledige inductie. We gaan met inductie naar n bewijzen dat na n stappen de invariant geldig is. Voor $n = 0$ geldt dit volgens de eerste aanname, daarmee is de basisstap bewezen. Vervolgens vragen we ons af of de invariant geldt na $n + 1$ stappen. Het uitvoeren van $n + 1$ stappen kunnen we zien als het uitvoeren van n stappen en daarna nog één stap. Volgens de inductiehypothese moge we aannemen dat na n stappen inderdaad de invariant geldt. Volgens de tweede aanname geldt dan dat na het uitvoeren van nog één stap, dus na in totaal $n + 1$ stappen, de invariant weer geldt. Volgens het principe van volledige inductie is hiermee bewezen dat voor elke n geldt dat de invariant na het uitvoeren van n stappen geldt, precies wat we wilden bewijzen.

We gaan nu met volledige inductie een bekende stelling bewijzen over priemgetallen.

Een natuurlijk getal $p \geq 2$ heet een *priemgetal* als zijn enige delers 1 en p zelf zijn.

Stelling 7.3 Ieder natuurlijk getal $q \geq 2$ is een priemgetal, of is een produkt van priemgetallen.

Bewijs:

Zij $P(n)$ de uitspraak: voor alle natuurlijke getallen k die voldoen aan $2 \leq k \leq n + 2$ geldt dat k een priemgetal of een produkt van priemgetallen is.

Basisstap: $P(0)$ is waar, want het enige getal k dat voldoet aan $2 \leq k \leq 0 + 2$ is $k = 2$ en dat is een priemgetal.

Inductiestap:

Neem aan dat $P(x)$ waar is.

We moeten bewijzen dat $P(x + 1)$ waar is, oftewel dat voor alle natuurlijke getallen k die voldoen aan $2 \leq k \leq x + 3$ geldt dat k een priemgetal of een produkt van priemgetallen is.

Vanwege $P(x)$ hoeven we dit alleen maar te bewijzen voor $k = x + 3$.

Neem dus aan dat $P(x)$ geldt, we moeten nu bewijzen dat $x+3$ een priemgetal of een produkt van priemgetallen is.

Stel dat $x + 3$ geen priemgetal is.

Dan heeft $x + 3$ een deler y die ongelijk is aan 1 en ongelijk aan $x + 3$.

Dan is dus $x + 3 = y * z$ waarbij $y \neq 1$ en $y \neq x + 3$.

Dus geldt $2 \leq y \leq x + 2$.

Vanwege $x + 3 = y * z$ geldt dan ook $2 \leq z \leq x + 2$.

Nu weten we door de inductiehypothese $P(x)$ dat y en z beide priemgetallen of produkten van priemgetallen zijn.

Dus is $x + 3 = y * z$ ook een produkt van priemgetallen.

Uit het voorgaande concluderen we dat $x + 3$ een priemgetal of een produkt van priemgetallen is, hetgeen precies is wat we wilden bewijzen.

Einde Bewijs.

Merk op dat we het bovenstaande bewijs ook kunnen interpreteren als een andere vorm van volledige inductie op de uitspraak $Q(n)$ die luidt: "$n + 2$ is een priemgetal of een produkt van priemgetallen", namelijk via het principe

Zij Q een predikaat, gedefinieerd op $\mathbf{N}$, waarvoor:

- $Q(0)$ is waar, en
- voor elke $k \in \mathbf{N}$ geldt:
  als $Q(x)$ waar is voor alle $x \leq k$ dan is $Q(k + 1)$ waar.

Dan geldt $\forall n \in \mathbf{N}\langle Q(n)\rangle$.

Men noemt dit wel *sterke volledige inductie*, alhoewel daar geen enkele reden voor bestaat, immers dit komt neer op "gewone" volledige inductie voor de uitspraak $P(n)$, luidend "voor alle $k \leq n$ geldt $Q(k)$".

Ook kent men *volledige inductie vanaf* m via het principe

Zij R een predikaat, gedefinieerd op natuurlijke getallen $\geq m$, waarvoor

- $R(m)$ is waar, en
- voor elke $k \geq m$ geldt:
  als $Q(k)$ waar is dan is ook $Q(k + 1)$ waar.

Dan is $R(y)$ waar voor alle natuurlijke getallen $y \geq m$.

Dit principe spaart alleen wat schrijfwerk en doet daarmee een bewijs eenvoudiger ogen. Je kunt echter altijd hetzelfde bewijs geven met 'gewone' volledige inductie waarbij $P(n)$ gedefinieerd is als $R(n + m)$. Toch zijn dit soort hulpmiddelen waarmee je bewijzen wat korter kunt maken of stroomlijnen zeer waardevol: bij het zoeken naar een bewijs wil je je kunnen concentreren op het echte probleem, en niet op de notatie er om heen.

Er zijn mensen die er de voorkeur aan geven niet de stap van n naar $n+1$ te maken maar van $n-1$ naar n. De inductiestap ziet er dan als volgt uit:

> Neem voor willekeurige $n > 0$ aan dat $P(n-1)$ geldt.
>
> Bewijs dat dan ook $P(n)$ geldt.

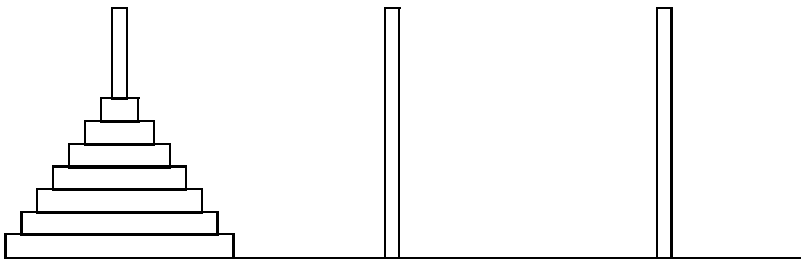
De sterke variant hiervan luidt:

> Neem aan dat $P(k)$ geldt voor elke $k \in \mathbf{N}$ met $k < n$.
>
> Bewijs dat dan ook $P(n)$ geldt.

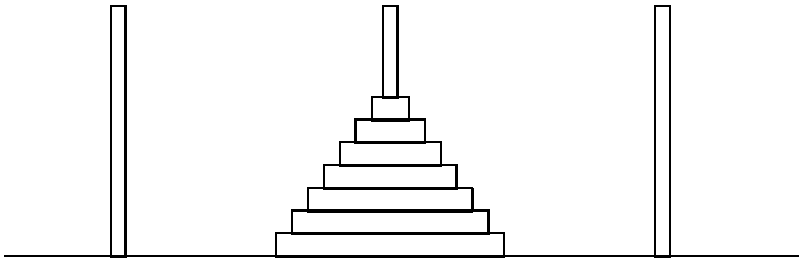
Het aardige van deze laatste vorm is dat je de basisstap niet meer afzonderlijk na hoeft te gaan: dit is namelijk het speciale geval van de inductiestap waarbij $n = 0$. In dat geval is er geen enkele aanname, want er is geen enkele $k \in \mathbf{N}$ met $k < n$, maar je moet wel bewijzen dat $P(n)$ oftewel $P(0)$ geldt. Dat is precies de basistap.

Ruwweg kunnen we zeggen dat inductie betekent dat als je wilt bewijzen dat een eigenschap voor elk natuurlijk getal geldt, je bij het bewijs daarvan desgewenst gebruik mag maken van de aanname dat diezelfde eigenschap voor kleinere getallen al geldt.

De verschijningsvormen kunnen heel verschillend zijn. In de meeste opgaven bij dit hoofdstuk wordt gevraagd: 'Bewijs dat voor elk natuurlijk getal $n \cdots$' en gaat dit het handigst met inductie naar n. Soms moet je iets bewijzen over n zonder dat je verder iets over n weet en moet je het ook voor elke n doen zonder dat dat er heel expliciet bij staat. Als je bijvoorbeeld iets over eindige verzamelingen moet bewijzen, kan het handig zijn om dat te doen door met inductie naar n te bewijzen dat de gewenste eigenschap voor elke verzameling met n elementen geldt. Het kan zelfs voorkomen dat inductie een handige methode is om iets te bewijzen wat slechts over één specifiek getal n gaat. Het kan makkelijker zijn om de algemene bewering voor elke willekeurige n te bewijzen met inductie dan alleen maar de bewering over dat ene specifieke getal rechtstreeks te bewijzen. We gaan hier nu een voorbeeld van geven: de *torens van Hanoi*.



Er zijn hier drie palen, en er zijn zeven schijven in oplopende grootte met een gat in het midden, die precies over de palen geschoven kunnen worden. In het begin liggen alle zeven schijven om de meest linkse paal, van onder naar boven gerangschikt van groot naar klein, zoals in het plaatje is aangegeven. De bedoeling is nu om deze hele stapel van schijven over te hevelen naar de middelste paal, zoals in het volgende plaatje is aangegeven:



Hierbij moeten de volgende spelregels in acht worden genomen:

- per stap kan slechts één schijf verplaatst worden, en wel de bovenste schijf van de stapel rond de ene paal naar een andere paal;
- een schijf mag nooit op een kleinere schijf worden gelegd.

De opdracht is nu om te laten zien dat

- je in 127 stappen de hele stapel rond de linkerpaal kunt overhevelen naar de middelste paal, en
- dat het niet in minder dan 127 stappen kan.

Hoewel deze opdracht betrekking heeft op de gegeven situatie met zeven schijven, ligt het voor de hand om eerst eenvoudiger instanties te bekijken met minder schijven. Hierbij volgen we een heel algemeen principe voor het aanpakken van een moeilijk probleem: probeer eerst eenvoudiger instanties van het probleem goed te begrijpen.

Laten we dus eens beginnen met één schijf. Die kunnen we in één stap van de linkerpaal naar de middelste paal overhevelen. Dat is wel erg makkelijk: na één stap zijn we klaar. Ietsje lastiger wordt het met twee schijven. Als eerste stap moeten we dan de bovenste schijf van de linkerpaal naar de middelste of rechterpaal verplaatsen. Laten we de rechterpaal kiezen. Vervolgens kunnen we de onderste schijf van de linkerpaal naar de middelste paal verplaatsen, en tenslotte kunnen we de kleinste schijf die we rond de rechterpaal geparkeerd hadden naar het midden brengen, en zijn we klaar. Hier hebben we drie stappen voor nodig gehad. Als we nu gaan spelen met drie of vier schijven beginnen we het volgende patroon te ontdekken: als ik een stapel van n van links naar het midden wil verplaatsen, moet ik eerst de bovenste $n-1$ naar de rechterpaal overhevelen, dan de onderste schijf naar het midden verplaatsen, en tenslotte de hele stapel van $n-1$ op de rechterpaal naar het midden overhevelen. Als ik het aantal stappen dat ik voor het verplaatsen van n schijven nodig heb $f(n)$ noem, zie ik uit deze observatie dat $f(1) = 1$ en $f(n) = f(n-1) + 1 + f(n-1)$. Invullen van kleine waarden: $f(1) = 1, f(2) = 3, f(3) = 7, f(4) = 15, f(5) = 31, f(6) = 63, \ldots$ doet het patroon opdoemen dat $f(n) = 2^n - 1$. Op grond hiervan proberen we het volgende met inductie naar n te bewijzen:

> Als we volgens bovenstaande spelregels een stapel van n schijven rond de linkerpaal willen overhevelen naar de middelste paal, kan dat in $2^n - 1$ stappen, en kan het niet in minder dan $2^n - 1$ stappen.

Bewijs:

Basisstap:

Voor $n = 1$ kun je die ene schijf in $2^n - 1 = 1$ stap naar het midden verplaatsen, en het kan niet in minder stappen. De bewering is dus waar voor $n = 1$.

Inductiestap:

We moeten twee dingen bewijzen: dat het kan in $2^n - 1$ stappen, en dat het niet kan in minder dan $2^n - 1$ stappen.

Dat het kan is als volgt in te zien.

Verplaats eerst de bovenste $n - 1$ schijven van de linkerpaal naar de rechterpaal in $2^{n-1} - 1$ stappen. Volgens de inductiehypothese is een dergelijke verplaatsing mogelijk naar de middelste paal, maar door de rechterpaal en de middelste paal elkaars rol in te laten nemen is dit ook mogelijk van de linkerpaal naar de rechterpaal. Vervolgens wordt de onderste schijf van links naar het midden verplaatst. Tenslotte worden de $n - 1$ schijven van de rechterpaal naar de middelste paal verplaatst in $2^{n-1} - 1$ stappen. Dit kan volgens de inductiehypothese door daarin de linkerpaal en de rechterpaal van rol te laten verwisselen. Op deze wijze is de volledige stapel van n schijven van links naar het midden verplaatst; het hiervoor benodigde aantal stappen was $(2^{n-1} - 1) + 1 + (2^{n-1} - 1) = 2 * 2^{n-1} - 1 = 2^n - 1$.

We moeten nog laten zien dat het niet in minder stappen kan. Het is duidelijk dat de grootste schijf tenminste één keer verplaatst zal moeten worden. Deze kan alleen maar verplaatst worden volgens de spelregels als alle andere schijven rond de paal geplaatst zijn waar de grootste schijf niet vandaan komt en ook niet naar toe gaat. Volgens de inductiehypothese zijn voor het verplaatsen van de andere $n-1$ schijven naar een andere paal tenminste $2^{n-1}-1$ stappen nodig. Tenslotte zal na de laatste keer dat de grootste schijf verplaatst wordt, de hele stapel van $n - 1$ kleinere weer naar het midden moeten worden overgeheveld. Ook hier zijn volgens de inductiehypothese tenminste $2^{n-1} - 1$ stappen nodig. In totaal is het minimale aantal hiervoor benodigde stappen dus $(2^{n-1} - 1) + 1 + (2^{n-1} - 1) = 2^n - 1$.

Einde Bewijs.

Het oorspronkelijke probleem voor zeven schijven is nu opgelost door deze bewering die we net hebben bewezen voor elke $n \geq 1$, toe te passen voor $n = 7$.

Het is zelfs met deze redenering in te zien dat het verplaatsen van de hele stapel van n schijven van de linkerpaal naar de middelste paal slechts op precies één manier kan in $2^n - 1$ stappen, en wel volgens de manier die in het bewijs is aangegeven en eenvoudig in een algoritme kan worden omgezet.

7.1 Inductieve definities

Tot nu toe hebben we inductie gebruikt om uitspraken over natuurlijke getallen te bewijzen. De achterliggende gedachte is dat elk natuurlijk getal te bereiken is door te beginnen

met 0 en vanaf daar een eindig aantal keer de opvolger te nemen. Ditzelfde principe kunnen we ook gebruiken om afbeeldingen f van $\mathbf{N}$ naar een verzameling A te definiëren. Daartoe definiëren we $f(0)$ apart, en geven we een definitie van $f(n+1)$ waarin gebruikt mag worden van $f(n)$. Volgens bovenstaand principe is daarmee $f(n)$ vastgelegd voor elk natuurlijk getal n, en is de afbeelding f daarmee geheel gedefinieerd. Een dergelijke definitie van een afbeelding noemen we een *inductieve definitie*. Op deze manier wordt bij het definiëren van $f(n+1)$ de definitie van dezelfde afbeelding f aangeroepen. Een dergelijke definitie die zichzelf weer aanroept heet ook wel een *recursieve definitie*, net zoals in een programmeertaal een methode of procedure die zichzelf aanroept ook *recursief* heet.

We geven een aantal voorbeelden.

Wanneer we x^n willen definiëren voor natuurlijke getallen n, dan kan dat het duidelijkst door te stellen

$$x^0 = 1 \text{ en voor elk natuurlijk getal } n \text{ is } x^{n+1} = x^n x.$$

Een ander voorbeeld:

$$0! = 1 \text{ en voor elk natuurlijk getal } n \text{ is } (n+1)! = (n+1)(n!).$$

Met dit laatste is voor elk natuurlijk getal n de waarde $n!$ gedefinieerd, uitgesproken als n *faculteit* (Engels: n *factorial*).

Omdat een afbeelding f van $\mathbf{N}$ naar een verzameling A gegeven wordt door het definiëren van een rij van waarden $f(0), f(1), f(2), \ldots$, wordt een afbeelding waarvan het domein $\mathbf{N}$ is ook wel een (oneindige) *rij* genoemd (Engels: *sequence*); een afbeelding waarvan het domein $\{0, 1, 2, \ldots, n\}$ is voor zekere $n \in \mathbf{N}$ wordt wel een *eindige rij* genoemd. Voor eindige en oneindige rijen wordt vaak de notatie f_n gekozen in plaats van $f(n)$, waarmee minder haakjes hoeven te worden geschreven.

Net zoals we bij het geven van bewijzen met volledige inductie een 'sterke' variant hadden waarbij we de geldigheid van $P(k)$ mogen aannemen voor elke k met $k < n+1$, mogen bij het geven van de definitie van $f(n+1)$ niet alleen de waarde van $f(n)$ bekend veronderstellen, maar ook de waarde van $f(k)$ voor elke k met $k < n+1$. Het komt er op neer dat we bij het definiëren van een afbeedling toegepast op een willekeurig natuurlijk getal gebruik mogen maken van diezelfde afbeelding toegepast op kleinere getallen.

Een zeer bekende, op deze manier inductief gedefinieerde rij getallen is de zogenaamde *rij van Fibonacci*, die gedefinieerd is door

$$a_0 = 1, \quad a_1 = 1, \text{ en } a_{n+2} = a_{n+1} + a_n \text{ voor } n \in \mathbf{N}.$$

Na de twee eerste elementen die beide de waarde 1 hebben is elk element in deze rij dus de som van zijn twee voorgangers. Het verhaal gaat dat dit proces geïnspireerd is door de manier waarop konijnen zich vermenigvuldigen, maar je moet wel enige weinig realistische aanames doen om met konijnenpopulaties precies op deze getallen uit te komen.

We schrijven het beginstuk van deze rij op in een tabel:

n:	0	1	2	3	4	5	6	7	8	9	10	11	12	13
a_n:	1	1	2	3	5	8	13	21	34	55	89	144	233	377

n:	14	15	16	17	18	19	20	21	22
a_n:	610	987	1597	2584	4181	6765	10946	17711	28657

De waarden in deze rij heten wel *fibonaccigetallen*. Hiervan zijn bijzonder veel eigenschappen bekend, waarvan we in de volgende stelling een noemen. Weer gaat het hier meer om de manier waarop het bewijs wordt gegeven dan om het resultaat op zich.

Stelling 7.4 Voor elk natuurlijk getal n geldt

$$a_{n+1}^2 - a_n * a_{n+2} = (-1)^{n+1}.$$

Bewijs:

We schrijven $P(n)$ voor de bewering

$$a_{n+1}^2 - a_n * a_{n+2} = (-1)^{n+1},$$

en gaan met volledige inductie bewijzen dat $P(n)$ geldt voor elk natuurlijk getal n.

Basisstap: $a_1^2 - a_0 * a_2 = 1^2 - 1 * 2 = -1 = (-1)^1$, dus $P(0)$ geldt.

Inductiestap: Stel dat $P(n)$ geldt. We moeten bewijzen dat $P(n+1)$ geldt, oftewel

$$a_{n+2}^2 - a_{n+1} * a_{n+3} = (-1)^{n+2}.$$

Door het tweemaal toepassen van de definitie van de rij van Fibonacci krijgen we:

$$\begin{array}{lll} a_{n+2}^2 - a_{n+1} * a_{n+3} & & \\ \quad = \quad a_{n+2}^2 - a_{n+1} * (a_{n+2} + a_{n+1}) & & (\text{want } a_{n+3} = a_{n+2} + a_{n+1}) \\ \quad = \quad a_{n+2} * (a_{n+1} + a_n) - a_{n+1} * (a_{n+2} + a_{n+1}) & & (\text{want } a_{n+2} = a_{n+1} + a_n) \\ \quad = \quad a_{n+2} * a_n - a_{n+1} * a_{n+1} & & (\text{rekenen}) \\ \quad = \quad -(a_{n+1}^2 - a_{n+2} * a_n) & & (\text{rekenen}) \\ \quad = \quad -((-1)^{n+1}) & & (\text{inductiehypothese}) \\ \quad = \quad (-1)^{n+2} & & (\text{rekenen}). \end{array}$$

Hiermee is het gevraagde bewezen.

Einde Bewijs.

Bij het vinden van een dergelijk bewijs is het de kunst om zodanig de inductieve definitie in te vullen (in dit geval dus twee keer), dat een uitdrukking verkregen wordt waarop de inductiehypothese toegepast kan worden.

De volgende stelling geeft een *gesloten uitdrukking* voor de fibonaccigetallen, dat wil zeggen een uitdrukking waarmee de fibonaccigetallen helemaal vast liggen zonder een beroep op inductie te doen. De uitdrukking ziet er nogal ingewikkeld uit, daarom geven we eerst de afleiding en dan pas de uitdrukking zelf.

We proberen oplossingen te vinden van het type $a_n = s^n$. Vullen we dit in in de vergelijking $a_{n+2} = a_{n+1} + a_n$, zonder ons te bekommeren om a_0 en a_1, dan vinden we

$$s^{n+2} = s^{n+1} + s^n.$$

Delen we (let op de mogelijkheid $s = 0$) door s^n, dan komt er

$$s^2 = s + 1, \quad \text{oftewel} \quad s^2 - s - 1 = 0.$$

Deze vierkantsvergelijking in s kunnen we oplossen met de bekende *abc*-formule, en we vinden voor s twee mogelijkheden:

$$s_1 = \frac{1+\sqrt{5}}{2} \quad \text{en} \quad s_2 = \frac{1-\sqrt{5}}{2}$$

We zien nu dat $a_n = s_1^n$ oplevert $a_0 = 1$ en $a_1 = s_1$,
en dat $a_n = s_2^n$ oplevert $a_0 = 1$ en $a_1 = s_2$.

Geen van beide mogelijkheden geeft dus wat we willen, namelijk $a_0 = 1$ en $a_1 = 1$.
Maar we hebben nog een pijl op onze boog: we kunnen proberen om de twee mogelijkheden te combineren tot

$$a_n = c \cdot s_1^n + d \cdot s_2^n,$$

waarin c en d constanten zijn.
Immers dan blijft voldaan aan $a_{n+2} = a_{n+1} + a_n$.
Om nu $a_0 = 1$ en $a_1 = 1$ te krijgen, moeten c en d voldoen aan het stelsel lineaire vergelijkingen

$$\begin{array}{lcll} c & + & d & = & 1 \\ c \cdot s_1 & + & d \cdot s_2 & = & 1 \end{array}$$

Zoals men gemakkelijk narekent, wordt de oplossing van dit stelsel gegeven door

$$c = -\frac{s_1}{s_2 - s_1} \quad \text{en} \quad d = \frac{s_2}{s_2 - s_1},$$

en aangezien $s_2 - s_1 = -\sqrt{5}$, krijgen we uit deze rekenpartij

$$a_n = c \cdot s_1^n + d \cdot s_2^n = \frac{s_1^{n+1} - s_2^{n+1}}{\sqrt{5}}.$$

Door hierin weer de definities van s_1 en s_2 in te vullen en te schrijven $\frac{1}{\sqrt{5}} = \frac{1}{5}\sqrt{5}$ krijgen we de volgende stelling.

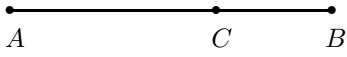
Stelling 7.5 Voor elk natuurlijk getal n geldt

$$a_n = \frac{1}{5}\sqrt{5}((\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}).$$

Van deze stelling kan een bewijs met volledige inductie worden gegeven, gebruik makend van $(\frac{1+\sqrt{5}}{2})^2 = \frac{1+\sqrt{5}}{2} + 1$ en $(\frac{1-\sqrt{5}}{2})^2 = \frac{1-\sqrt{5}}{2} + 1$. Dit laten we aan de lezer over.

Voor grote waarden van n ligt s_2^{n+1} heel dicht bij 0, want $s_2 = -0{,}618034\ldots$. In dat geval is $\frac{1}{5}\sqrt{5} * s_1^{n+1}$ dus al een goede benadering van a_n. Zo is bijvoorbeeld $a_9 = 55$, en afgerond op 5 cijfers na de komma is $\frac{1}{5}\sqrt{5} * s_1^{10} = 55{,}00364$.

Het getal $s_1 = 1{,}618034\ldots$ staat bekend als de *gulden snede*, en wordt wel aangeduid door de griekse letter τ. Meetkundig is het bijzondere eraan, dat een verdeling van een segment in twee stukken die zich verhouden als $\tau : 1$ de eigenschap heeft dat ook de verhouding van het hele segment tot het grootste stuk $\tau : 1$ is:



$AC : CB = AB : AC$ geeft $\tau : 1 = (\tau + 1) : \tau$, dus $\tau^2 = \tau + 1$.

Deze zelfde verhouding komen we bij benadering tegen als verhouding van twee opeenvolgende fibonaccigetallen.

7.2 Binomiaalcoëfficiënten

Als n en m natuurlijke getallen zijn met $m \leq n$, op hoeveel manieren kun je dan een uit m elementen bestaande deelverzameling maken van een verzameling met n elementen? Het antwoord op deze vraag schrijven we als $\binom{n}{m}$, uit te spreken als n *over* m of n *boven* m. Deze getallen heten *binomiaalcoëfficiënten*, en zijn het onderwerp van deze sectie.

Als $m = 0$ is er maar één zo'n deelverzameling, namelijk de lege verzameling. Ook als $m = n$ is er maar één zo'n deelverzameling, namelijk de hele verzameling. We hebben dus voor elk natuurlijk getal n:

$$\binom{n}{0} = 1 \quad \text{en} \quad \binom{n}{n} = 1.$$

Veronderstel nu dat we $\binom{k}{m}$ kennen voor zekere k en alle m met $0 \leq m \leq k$. Om dan $\binom{k+1}{r+1}$ te berekenen voor zekere r met $0 \leq r < k$ kunnen we de volgende redenering houden.

> Neem een verzameling van $k + 1$ elementen. Neem daarin een element e apart (dit kan, want $k + 1 \geq 1$), en kijk naar de deelverzamelingen die e bevatten en naar de deelverzamelingen die e niet bevatten.
>
> Het aantal uit $r+1$ elementen bestaande deelverzamelingen dat e wel bevat is precies $\binom{k}{r}$, er zijn immers precies k elementen ongelijk aan e en elke gevraagde deelverzameling wordt verkregen door daar precies r elementen uit te kiezen.
>
> Het aantal uit $r+1$ elementen bestaande deelverzamelingen dat e niet bevat is precies $\binom{k}{r+1}$, want zo'n verzameling wordt verkregen door precies $r+1$ elementen te kiezen uit de k elementen ongelijk aan e.
>
> In totaal heeft de verzameling van $k + 1$ elementen dus precies $\binom{k}{r} + \binom{k}{r+1}$ deelverzamelingen met precies $r + 1$ elementen, we hebben dus laten zien dat
>
> $$\binom{k+1}{r+1} = \binom{k}{r} + \binom{k}{r+1}.$$

Samenvattend kunnen we de volgende stelling formuleren.

Stelling 7.6 Voor elk natuurlijk getal n geldt:

$$\binom{n}{0} = 1 \quad \text{en} \quad \binom{n}{n} = 1.$$

Voor natuurlijke getallen n, m met $m < n$ geldt:

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

Het aardige van deze stelling is dat we dit nu ook als de definitie van binomiaalcoëfficiënten kunnen opvatten: als we de oorspronkelijke definitie vergeten, en we hebben alleen maar Stelling 7.6, dan ligt daarmee voor elk tweetal natuurlijke getallen n, m met $m < n$ de waarde van $\binom{n}{m}$ vast. We kunnen de volgende tabel opstellen:

m / n	0	1	2	3	4	5	.	.
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
.	.	.	.	.	.	.	.	
.	.	.	.	.	.	.	.	.

Door in deze tabel de rijen ten opzichte van elkaar te verschuiven wordt de symmetrie beter zichtbaar en krijgt men een driehoekige tabel, de bekende *driehoek van Pascal*:

```
                    1
                  1   1
                1   2   1
              1   3   3   1
            1   4   6   4   1
          1   5  10  10   5   1
        .   .   .   .   .   .   .
```

Op de rand van de driehoek staat steeds het getal 1, elk ander getal is de som van de twee er onmiddellijk boven staande getallen. Voor $0 \leq m \leq n$ vinden we $\binom{n}{m}$ in de driehoek op de $(n+1)$-ste rij van boven en daarvan het $(m+1)$-ste getal van links. Naar onderen breidt de driehoek zich onbeperkt uit.

Er is nog een andere manier om $\binom{n}{m}$ te berekenen, rechtstreeks uit de oorspronkelijke definitie.

Veronderstel dat $1 \leq m \leq n$. Uit de verzameling met n elementen kunnen we m elementen een voor een pakken. Voor het eerste element zijn er n mogelijkheden, voor het tweede element nog $n-1$, voor het derde nog $n-2$, ... , voor het m-de element blijven er tenslotte $n-m+1$ mogelijkheden over, zodat het totale aantal mogelijkheden om achtereenvolgens m elementen te pakken gelijk is aan

$$n(n-1)(n-2)\cdots(n-m+1).$$

We kunnen deze uitdrukking ook compacter schrijven als $n!/(n-m)!$.
We hebben nu uitgerekend hoe groot het aantal mogelijkheden is, als we op de volgorde van de elementen letten. Voor een verzameling doet de volgorde van zijn elementen er echter niet toe, zodat we het berekende aantal nog moeten delen door $m!$, zijnde het aantal mogelijkheden om m elementen op een rij te zetten. Deze redenering leidt ons dus tot de uitkomst

$$\text{Als } 0 \leq m \leq n, \text{ dan is } \binom{n}{m} = \frac{n!}{m!(n-m)!}$$

Het is eenvoudig na te gaan dat deze formule ook klopt met de feiten als $m = 0$ of $n = 0$.

Bovenstaand resultaat is gemakkelijk te toetsen aan de eerder afgeleide betrekking in Stelling 7.6. Daarvoor is geen volledige inductie nodig, het komt simpelweg neer op het gelijknamig maken van breuken die moeten worden opgeteld:

$$\begin{array}{rcl}
\binom{n+1}{m+1} & = & \frac{(n+1)!}{(m+1)!(n-m)!} \\
& = & \frac{n!*(n+1)}{(m+1)!(n-m)!} \\
& = & \frac{n!*(m+1)}{(m+1)!(n-m)!} + \frac{n!*(n-m)}{(m+1)!(n-m)!} \\
& = & \frac{n!}{m!(n-m)!} + \frac{n!}{(m+1)!(n-m-1)!} \\
& = & \binom{n}{m} + \binom{n}{m+1}.
\end{array}$$

De binomiaalcoëfficiënten zijn van bijzonder nut bij allerlei rekenwerk. Zo geldt bijvoorbeeld het *binomium van Newton*: voor elk natuurlijk getal n geldt

$$(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m},$$

te bewijzen met volledige inductie naar n, gebruikmakend van Stelling 7.6. Hieruit zien we dan weer door $x = 1$ en $y = 1$ te nemen dat

$$2^n = \sum_{m=0}^{n} \binom{n}{m},$$

iets wat ons niet zal verbazen, omdat we nu eigenlijk met de som in het rechterlid tellen hoeveel deelverzamelingen een verzameling met n elementen heeft. In sectie 5.2 hebben we al gezien dat dat precies 2^n is.

7.3 Opgaven

In de volgende opgaven slaat de variabele n op natuurlijke getallen.

Opgave 7.1

Bewijs dat voor iedere n geldt $\sum_{k=0}^{n} 4k^3 = n^4 + 2n^3 + n^2$.

Opgave 7.2

Bewijs dat voor iedere $n \geq 1$ en iedere reële $a \neq 1$ geldt

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

Opgave 7.3

Bewijs dat voor iedere n het getal $n^3 + 2n$ deelbaar is door 3.

Opgave 7.4

Gegeven is een natuurlijk getal n. Bewijs dat $\sum_{k=0}^{n} k \cdot k! = (n+1)! - 1$

Opgave 7.5

Gegeven is een natuurlijk getal n. Bewijs dat $\sum_{k=0}^{n} k^3 = (\sum_{k=0}^{n} k)^2$

Opgave 7.6

Gegeven is een natuurlijk getal $n > 1$. Bewijs dat $\sum_{k=1}^{n} \frac{1}{\sqrt{k}} > \sqrt{n}$

(Aanwijzing: gebruik $(\sqrt{n+1} + \sqrt{n}) * (\sqrt{n+1} - \sqrt{n}) = 1$.)

Opgave 7.7

Gegeven is een natuurlijk getal $n > 0$. Bewijs dat $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$

Opgave 7.8

Gegeven is een natuurlijk getal n. Bewijs dat $\sum_{k=0}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1)$

Opgave 7.9

Laat a_k het k-de Fibonaccigetal zijn. Bewijs dat

$$\sum_{k=0}^{n} a_k = a_{n+2} - 1$$

voor elk natuurlijk getal n.

Opgave 7.10

Laat a_k het k-de Fibonaccigetal zijn. Bewijs dat

$$\sum_{k=0}^{n} a_{2k} = a_{2n+1}$$

voor elk natuurlijk getal n.

Opgave 7.11

Gegeven zijn de getallen $b_0, b_1, b_2, \ldots$ die voldoen aan

$$b_0 = 2, \;\; b_1 = 1,$$

$$b_{n+2} = b_{n+1} + 2b_n \;\text{ voor elke } n \geq 0.$$

Bewijs dat voor ieder natuurlijk getal n geldt dat

$$b_n = 2^n + (-1)^n.$$

Opgave 7.12

Bewijs Stelling 7.5.

Opgave 7.13

Bewijs dat

$$n\binom{n-1}{k} = (k+1)\binom{n}{k+1}$$

voor natuurlijke getallen n, k met $n > k$.

Opgave 7.14

Bewijs dat

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$$

voor natuurlijke getallen n, k, r met $n \geq r \geq k$.

Opgave 7.15

Bewijs het binomium van Newton met behulp van Stelling 7.6.

Opgave 7.16

Gegeven zijn twee gehele getallen a_0 en a_1 met $a_1 > 0$ en $a_1 > a_0$. Voor $i = 0, \ldots, 98$ is gedefinieerd $a_{i+2} = 3a_{i+1} - 2a_i$. Bewijs dat $a_100 \geq 2^{100} - 1$.

(Aanwijzing: bewijs dat voor elke $n \geq 0$ geldt: $a_{n+1} \geq 2^{n+1} - 1 \wedge a_{n+1} \geq a_n + 2^n$.)

Hoofdstuk 8

Relaties en grafen

8.1 Relaties

We zijn gewend aan het gebruik van de notaties $=$, $>$, $<$, $\leq$, $\geq$, maar wat zijn dat nu eigenlijk voor dingen? We noemen dit een *relatie*, en voor elke relatie R en elk tweetal elementen x, y is xRy een bewering die wel of niet waar kan zijn. Zo'n relatie laat zich dus beschrijven met de verzameling paren (x, y) waarvoor xRy waar is. Dit geven we dan ook als definitie voor het begrip relatie:

Definitie 8.1 Laten A en B verzamelingen zijn.
Een relatie R van A naar B is een deelverzameling van het cartesisch produkt $A \times B$.
A heet het *domein* van R, en B heet het *bereik* van R.

De notatie xRy beschouwen we als afkorting voor de bewering $(x, y) \in R$. Zo kunnen we de relatie $\leq$ van $\mathbf{R}$ naar $\mathbf{R}$ zien als de verzameling

$$\leq \; = \; \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x \leq y\},$$

waarmee inderdaad $x \leq y$ precies hetzelfde betekent als $(x, y) \in \leq$. Geheel analoog kunnen we ook $=$, $>$, $<$ en $\geq$ als deelverzamelingen van $\mathbf{R} \times \mathbf{R}$ zien.

Een belangrijke rol wordt gespeeld door relaties van een verzameling A naar diezelfde verzameling A, dus door relaties waarvoor domein en bereik samenvallen. In dit geval zegt men wel *relatie op* A in plaats van relatie van A naar A.

Als voorbeeld van een relatie waarin domein en bereik verschillende verzamelingen zijn noemen we de relatie $\in$. Bij een universum U kunnen we dit zien als een relatie waarvan het domein U is en het bereik $\mathcal{P}(U)$:

$$\in \; = \; \{(x, y) \in U \times \mathcal{P}(U) \mid x \in y\}.$$

De relatie $\subseteq$ heeft als domein en als bereik allebei $\mathcal{P}(U)$.

Bij elke afbeelding $f : A \to B$ hoort een relatie van A naar B, namelijk de *grafiek* van f:

$$\{(x, y) \in A \times B \mid y = f(x)\}.$$

Een relatie R van A naar B is de grafiek van een afbeelding van A naar B dan en slechts dan als er bij elke $x \in A$ er precies één $y \in B$ bestaat waarvoor xRy.

Bij elke relatie R van A naar B bestaat er ook een *inverse* R^{-1}. Dit is een relatie van B naar A, en is gedefinieerd door

$$R^{-1} \;=\; \{(y, x) \in B \times A \mid xRy\}.$$

Bij elke verzameling A bestaat er een *identiteit* van A naar A, gewoonlijk genoteerd met $=$:

$$\{(x, y) \in A \times A \mid x = y\}.$$

De identiteit is precies de grafiek van de identieke afbeelding van A naar A. Als we dit als een plaatje tekenen beschrijft deze grafiek precies de *diagonaal*, zo wordt deze relatie dan ook wel genoemd.

Net als bij afbeeldingen kunnen we ook relaties samenstellen. Als $R \subseteq A \times B$ en $S \subseteq B \times C$ relaties zijn, dan verstaan we onder de *samenstelling* R *gevolgd door* S de relatie $(S \circ R) \subseteq A \times C$ bepaald door

$$(S \circ R) = \{(a, c) \in A \times C \mid \; \exists b \in B \langle aRb \wedge bSc \rangle\}.$$

Let erop dat het domein van S gelijk moet zijn aan het bereik van R, net zoals bij het samenstellen van afbeeldingen.

Als voorbeeld noemen we de relatie R van A naar A waarin A de verzameling van alle mensen is, en xRy precies dan geldt als x een kind is van y. Dan geldt $x(R \circ R)y$ precies dan als x een kleinkind is van y.

De definitie van het samenstellen van relaties is in overeenstemming met de definitie van het samenstellen van afbeeldingen: $(S \circ R) \subseteq (A \times C)$ is precies de grafiek van $s \circ r : A \to C$ als $R \subseteq A \times B$ en $S \subseteq B \times C$ de grafieken zijn van afbeeldingen $r : A \to B$ en $s : B \to C$.

Net zoals bij het samenstellen van afbeeldingen is ook het samenstellen van relaties *associatief*: $S \circ (R \circ T) = (S \circ R) \circ T$ als beide samenstellingen goed gedefinieerd zijn. Ook is de identiteit een *neutraal element* met betrekking tot de samenstelling:

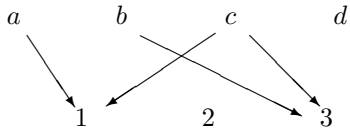
$$(= \circ R) \;=\; R \;=\; (R \circ =),$$

waarbij de eerste '$=$' de identiteit op het bereik van R is en de laatste '$=$' de identiteit op het domein van R.

Voor een relatie R van een eindige verzameling A naar een eindige verzameling B zijn er verschillende manieren om R in een schema voor te stellen.

De eerste manier waarop we de aandacht willen vestigen is het *pijlendiagram* van R. Daarbij stelt men de elementen van A en van B voor door punten en trekt een pijl van

van punt x naar punt y als xRy. Zo geeft voor $A = \{a, b, c, d\}$ en $B = \{1, 2, 3\}$ het pijlen-diagram



de relatie $R = \{(a, 1), (b, 3), (c, 1), (c, 3)\}$ van A naar B aan.

Merk op dat dit overeenkomt met het pijlendiagram van een afbeelding, het enige verschil is dat de eis dat er vanuit elk element van A precies één pijl moet uitgaan is komen te vervallen.

Een andere manier is de *matrixvoorstelling*. Daarbij tekent men een voorstelling van $A \times B$ in tabelvorm (horizontaal de elementen van A, vertikaal de elementen van B) en zet men in het veld (x, y) het cijfer 1 als xRy, en het cijfer 0 als niet xRy. Voor het bovenstaande voorbeeld is de matrixvoorstelling

	a	b	c	d
1	1	0	1	0
2	0	0	0	0
3	0	1	1	0

8.2 Grafen

In allerlei toepassingen kom je grafen tegen: aantallen punten waarvan sommige tweetallen met elkaar verbonden zijn. Denk maar eens aan:

- plaatsen op een kaart, met verbindingswegen ertussen,
- computers in een netwerk,
- leidingen van electriciteit, water, gas, kabeltelevisie.

In feite is zo'n serie verbindingen niet meer en niet minder dan een relatie op de verzameling punten. Dit rechtvaardigt de volgende definitie.

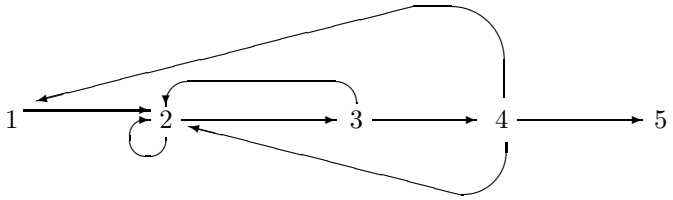
Definitie 8.2 Een relatie R op een eindige verzameling A heet een *gerichte graaf*, of kortweg *graaf*.

Een element van A heet dan een *knoop* van de graaf, in het Engels *node* of *vertex*. Een element van R heet dan een *kant* of *pijl* van de graaf, in het Engels *edge* of *arc*. Een kant is dus een paar van knopen, en een graaf is een verzameling van kanten.

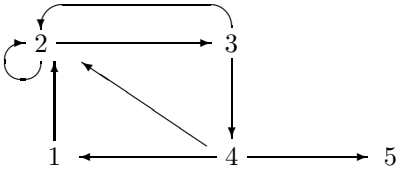
Een graaf wordt meestal getekend door een pijlendiagram waarbij elk element van A één keer wordt getekend, dus niet twee keer zoals we dat bij een relatie van A naar A deden. Als voorbeeld tekenen we de relatie

$$\{(1, 2), (2, 2), (2, 3), (3, 2), (3, 4), (4, 2), (4, 1), (4, 5)\}$$

op de verzameling $\{1, 2, 3, 4, 5\}$:

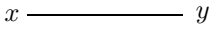


Het op deze manier weergegeven pijlendiagram van een graaf wordt zelf ook vaak graaf genoemd. In ons voorbeeld hebben we alle knopen op een rechte lijn getekend. Dit is echter niet noodzakelijk, precies dezelfde graaf kun je ook tekenen als

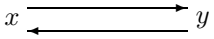


In het algemeen mag je een graaf tekenen zoals je wilt, als de knopen er maar allemaal staan en er voor elke kant (x, y) een pijl van knoop x naar knoop y is getekend.

In veel toepassingen speelt de richting van de pijl geen rol. Dit kunnen we in hetzelfde formalisme houden door zowel de kant (x, y) als (y, x) aanwezig te denken. Een relatie R op A heet *symmetrisch* als voor elke x, y met xRy ook geldt yRx. Een graaf waarvan de bijbehorende relatie symmetrisch is heet een *ongerichte graaf*. Voor elke kant (x, y) van een ongerichte graaf is dus (y, x) ook een kant. In plaats van dan zowel een pijl van x naar y als van y naar x te tekenen is het handiger om alleen maar een lijntje tussen x en y te tekenen. Dus



in plaats van



In onze benadering zien we een ongerichte graaf als een speciaal geval van een gerichte graaf. Omgekeerd kun je bij een gerichte graaf ook een ongerichte graaf maken door de richting van de kanten te 'vergeten': als R een gerichte graaf op A is, dan is

$$\{(x, y) \in A \times A \mid (x, y) \in R \vee (y, x) \in R\}$$

de bijbehorende ongerichte graaf.

Grafen modelleren op natuurlijke wijze alle mogelijke soorten netwerken, bijvoorbeeld wegen, computers, telefoon. Een veel voorkomend probleem daarin is het bepalen van verbindingen: op een wegenkaart wil je een kortste verbinding van plaats A naar plaats B bepalen, en bij een computernetwerk of telefoonnetwerk wil je een verbinding maken

tussen het ene ene het andere aangesloten apparaat. In termen van grafen heet zo'n verbinding een *pad* (Engels: *path* of *walk*): een pad van knoop a naar knoop b is een rij kanten $e_1, e_2, \ldots, e_n$ in die graaf waarvoor steeds de eindknoop van elke kant overeenkomt met de beginknoop van van zijn opvolger, dus

$$\begin{array}{rcl} e_1 & = & (a, a_1) \\ e_2 & = & (a_1, a_2) \\ e_3 & = & (a_2, a_3) \\ \vdots & \vdots & \vdots \\ e_{n-1} & = & (a_{n-2}, a_{n-1}) \\ e_n & = & (a_{n-1}, b). \end{array}$$

Eén enkele kant (a, b) beschouwen we ook als een pad van a naar b, voor elke knoop a beschouwen we zelfs een *leeg pad* van a naar a. Dit wordt gemotiveerd door de bedoeling van een pad: een pad beschrijft een manier om van een knoop a naar een knoop b te komen; als a en b gelijk zijn kan dit altijd door domweg in a te blijven.

In het bovenstaande voorbeeld is

$$(1,2), (2,2), (2,3), (3,2), (2,3), (3,4), (4,2), (2,3), (3,4), (4,5)$$

een pad van 1 naar 5, en is

$$(1,2), (2,3), (3,4), (4,5)$$

een korter pad van 1 naar 5.

Een graaf heet *samenhangend* (Engels: *connected*) als voor elk tweetal knopen a, b van de graaf er een pad van a naar b bestaat.

Het bovenstaande voorbeeld is niet samenhangend, want er is geen pad van 5 naar een andere knoop.

Stelling 8.3 Gegeven zijn twee samenhangende grafen $R_1 \subseteq A_1 \times A_1$ en $R_2 \subseteq A_2 \times A_2$ waarvoor $A_1 \cap A_2 \neq \emptyset$.
Dan is $R_1 \cup R_2 \subseteq (A_1 \cup A_2) \times (A_1 \cup A_2)$ ook samenhangend.

Bewijs:

Kies $a, b \in A_1 \cup A_2$ willekeurig.

Dan $a \in A_i$ en $b \in A_j$ voor zekere $i, j \in \{1, 2\}$.

Omdat $A_1 \cap A_2 \neq \emptyset$ is er een $c \in A_1 \cap A_2$, dus $c \in A_1$ en $c \in A_2$.

Omdat R_i samenhangend is, is er een pad van a naar c in R_i.

Omdat R_j samenhangend is, is er een pad van c naar b in R_j.

Deze twee paden achter elkaar geeft een pad van a naar b in $R_1 \cup R_2$.

Omdat er geen enkele aanname over $a, b \in A_1 \cup A_2$ is gemaakt, is er nu voor elke $a, b \in A_1 \cup A_2$ een pad van a naar b in $R_1 \cup R_2$.

Dus is $R_1 \cup R_2 \subseteq (A_1 \cup A_2) \times (A_1 \cup A_2)$ samenhangend.

Einde Bewijs.

Grafen hebben vaak ook toepassingen op problemen die op het eerste gezicht niets met grafen te maken lijken te hebben. Als voorbeeld hiervan geven we twee problemen die allebei opgelost kunnen worden met een stelling over grafen die we vervolgens gaan bewijzen.

- Landen op een kaart moeten gekleurd worden zodanig dat aangrenzende landen een verschillende kleur hebben.

  Bewering:

  Als elk land aan hoogstens k andere landen grenst, dan kan dit met $k+1$ kleuren.

- Studenten willen in een aantal vakken tentamen doen. Twee vakken conflicteren als er een student is die in beide vakken tentamen wil doen.

  Bewering:

  Als elk vak met hoogstens k andere vakken conflicteert, dan kunnen de tentamens in $k+1$ dagdelen worden ingeroosterd.

Beide beweringen volgen direct uit de volgende stelling als we voor het eerste probleem definiëren

$$A = \text{ verzameling landen, en}$$

$$R = \{(a,b) \in A \times A \mid a \neq b \ \wedge \ a \ \text{ grenst aan } \ b\ \},$$

en voor het tweede probleem definiëren

$$A = \text{ verzameling vakken, en}$$

$$R = \{(a,b) \in A \times A \mid a \neq b \ \wedge \ a \ \text{ conflicteert met } \ b\ \}.$$

Stelling 8.4 Gegeven is een ongerichte graaf R op een verzameling A zodanig dat voor elke $a \in A$ geldt dat

$$(a,a) \notin R$$

en

$$\#\{b \in A \mid (a,b) \in R\ \} \ \leq \ k.$$

Dan is er een afbeelding

$$f : A \to \{1, 2, \ldots, k+1\}$$

zodanig dat $f(a) \neq f(b)$ voor elke $(a,b) \in R$.

Bewijs:

We bewijzen dit met inductie naar $\#A$.

Basisstap:

$\#A = 1$, dan is $A = \{a\}$, definieer $f(a) = 1$.

Inductiestap:

Kies $a_0 \in A$.

Definieer $A' = A - \{a_0\}$.

Definieer

$$R' = \{(a, b) \in R \mid a \neq a_0 \wedge b \neq a_0\}.$$

Volgens de inductiehypothese is er een

$$f' : A' \to \{1, 2, \ldots, k+1\}$$

zodanig dat $f'(a) \neq f'(b)$ voor elke $(a, b) \in R'$.

Volgens het gegeven is nu

$$\#\{b \in A \mid (a_0, b) \in R\} \leq k.$$

Kies $n \in \{1, 2, \ldots, k+1\}$ met $n \neq f'(b)$ voor alle b met $(a_0, b) \in R$; dit kan omdat er hoogstens k dergelijke b's zijn.

Definieer $f(x) = f'(x)$ als $x \neq a_0$, en $f(a_0) = n$.

Stel $(a, b) \in R$. Dan is $a \neq b$.

- Als $a = a_0$ dan $f(a) = f(a_0) = n \neq f'(b) = f(b)$.
- Als $b = a_0$ dan $(a_0, a) \in R$ omdat R ongericht is. Dan geldt $f(a) = f'(a) \neq n = f(a_0) = f(b)$.
- Als $a \neq a_0$ en $b \neq a_0$ dan $(a, b) \in R'$, en geldt $f(a) \neq f(b)$ volgens de inductiehypothese.

Dus voldoet $f : A \to \{1, 2, \ldots, k+1\}$ aan de eis dat $f(a) \neq f(b)$ voor elke $(a, b) \in R$.

Hiermee is de stelling bewezen.

Einde Bewijs.

8.3 Equivalentierelaties en partities

We gaan nu een speciaal soort relaties beschouwen die een zeker begrip van *equivalentie* beschrijven, waarbij twee elementen equivalent genoemd worden als ze bijvoorbeeld een bepaalde eigenschap gemeenschappelijk hebben. Altijd geldt natuurlijk dat een element dezelfde eigenschap heeft als zichzelf. Verder geldt dat als x dezelfde eigenschap heeft als y dan heeft ook y dezelfde eigenschap heeft als x. Tenslotte geldt dat als x dezelfde eigenschap heeft als y en als y dezelfde eigenschap heeft als z dan heeft ook x dezelfde

eigenschap als z. Deze drie zeer voor de hand liggende eigenschappen beschouwen we nu als het fundament van het equivalentiebegrip en zetten we om in de volgende definitie.

Definitie 8.5 Zij A een verzameling. Een relatie E van A naar A heet

- *reflexief* als geldt: $\forall x\langle xEx\rangle$,
- *symmetrisch* als geldt: $\forall x\forall y\langle xEy \to yEx\rangle$,
- *transitief* als geldt: $\forall x\forall y\forall z\langle(xEy \wedge yEz) \to xEz\rangle$,
- een *equivalentierelatie* als E zowel reflexief, symmetrisch als transitief is.

Zonder quantoren te gebruiken kunnen we ook definiëren:

- E heet reflexief als $=\subseteq E$,
- E heet symmetrisch als $E^{-1} \subseteq E$,
- E heet transitief als $E \circ E \subseteq E$.

Hierin is '=' de identiteit op A en is E^{-1} de inverse van E. Hoewel deze versie korter is, vinden de meeste mensen de versie met quantoren toch prettiger om mee te werken.

Als we van een relatie R moeten bewijzen dat het equivalentierelatie is, moeten we dus bewijzen R reflexief, symmetrisch en transitief is. Soms zijn deze eigenschappen triviaal in te zien, met name reflexiviteit en symmetrie, maar voor het geven van het bewijs is het toch essentieel om dan tenminste op te schrijven dat je dit hebt ingezien, en liefst de betekenis van de eigenschappen in het specifieke geval van R uit te schrijven. We geven een aantal voorbeelden.

Voorbeeld 1.
Op elke verzameling A is de identiteit $=$ op A een equivalentierelatie, want er geldt:

- $=$ is reflexief want voor elke $x \in A$ geldt $x = x$;
- $=$ is symmetrisch want voor elke $x, y \in A$ geldt als $x = y$, dan geldt ook $y = x$;
- $=$ is transitief want voor elke $x, y, z \in A$ geldt als $x = y$ en $y = z$, dan geldt ook $x = z$.

Voorbeeld 2.
Op elke verzameling A is de relatie $A \times A$ een equivalentierelatie, want er geldt:

- $A \times A$ is reflexief want voor elke $x \in A$ geldt $(x, x) \in A \times A$;
- $A \times A$ is symmetrisch want voor elke $x, y \in A$ geldt als $(x, y) \in A \times A$ dan geldt ook $(y, x) \in A \times A$;
- $A \times A$ is transitief want voor elke $x, y, z \in A$ geldt als $(x, y) \in A \times A$ en $(y, z) \in A \times A$ dan geldt ook $(x, z) \in A \times A$.

Voorbeeld 3.
Een interessant voorbeeld van een equivalentierelatie krijgen we door voor A de verzameling van natuurlijke getallen of van gehele getallen te kiezen, en een vast natuurlijk getal $n > 1$ te kiezen. Voor $x, y \in A$ definiëren we

$$x \equiv y \iff \exists k \in \mathbf{Z}\langle x - y = n * k\rangle.$$

Om expliciet aan te geven om welke n het gaat wordt ook wel $x \equiv y \pmod{n}$ genoteerd in plaats van $x \equiv y$; de getallen x en y heten dan equivalent *modulo* n. De relatie $\equiv$ is inderdaad een equivalentierelatie, want er geldt:

- $\equiv$ is reflexief want voor elke $x \in A$ geldt $x - x = n * 0$, dus $\exists k \in \mathbf{Z}\langle x - x = n * k\rangle$, dus $x \equiv x$;
- $\equiv$ is symmetrisch want als $x \equiv y$ dan is $x - y = n * k$ voor zekere $k \in \mathbf{Z}$, dan geldt ook $-k \in \mathbf{Z}$ en $y - x = n * (-k)$, dus $y \equiv x$;
- $\equiv$ is transitief want als $x \equiv y$ en $y \equiv z$ dan zijn er $k, k' \in \mathbf{Z}$ met $x - y = n * k$ en $y - z = n * k'$ en dan geldt $k - k' \in \mathbf{Z}$ en $x - z = (x - y) + (y - z) = n * (k - k')$, dus $x \equiv z$.

Stelling 8.6 Voor alle verzamelingen A en B en elke afbeelding $f : A \to B$ is

$$\simeq_f \;=\; \{(x, y) \in A \times A \mid f(x) = f(y)\}$$

een equivalentierelatie op A.

Bewijs:

- $\simeq_f$ is reflexief want voor elke $x \in A$ geldt $f(x) = f(x)$, dus geldt $x \simeq_f x$;
- $\simeq_f$ is symmetrisch want voor elke $x, y \in A$ geldt als $x \simeq_f y$, dan geldt $f(x) = f(y)$, dus ook $f(y) = f(x)$, dus $y \simeq_f x$;
- $\simeq_f$ is transitief want voor elke $x, y, z \in A$ geldt als $x \simeq_f y$ en $y \simeq_f z$, dan geldt $f(x) = f(y)$ en $f(y) = f(z)$, dus $f(x) = f(z)$, dus $x \simeq_f z$.

Einde Bewijs.

De relatie $\simeq_f$ is een heel algemene manier om equivalentierelaties te beschrijven. Zo is de identiteit $=$ op A (voorbeeld 1) een speciaal geval van $\simeq_f$, namelijk het geval waarbij f de identieke afbeelding van A naar A is. Ook $A \times A$ (voorbeeld 2) is een speciaal geval van $\simeq_f$, namelijk het geval waarbij f de afbeelding van A naar B is waarbij B slechts uit één element bestaat.

Ook equivalentie modulo n (voorbeeld 3) kunnen we beschrijven als de relatie $\simeq_f$ voor een geschikt gekozen f. Voor A kiezen we de verzameling van natuurlijke getallen of van gehele getallen. Voor B kiezen we

$$B \;=\; \{0, 1, 2, \ldots, n - 1\}.$$

Voor elk getal $x \in A$ is er precies een $r \in B$ zodat er een $q \in \mathbf{Z}$ bestaat met $x = n * q + r$, dit is feite *delen met rest*, waarbij q het quotiënt is en r de rest. We definiëren nu $f(x) = r$, waarmee f een afbeelding van A naar B is geworden. Het is eenvoudig in te zien dat

$$x \equiv y \pmod{n} \iff x \simeq_f y;$$

twee getallen zijn namelijk precies dan equivalent modulo n als ze bij deling door n dezelfde rest opleveren.

In de volgende definitie en stelling wordt aangegeven hoe bij een equivalentierelatie op een verzameling, deze verzameling wordt opgesplitst in disjuncte stukken.

Definitie 8.7 Zij E een equivalentierelatie op een verzameling A. Voor een element x van A verstaan we onder de *equivalentieklasse* $[x]$ van x de deelverzameling

$$[x] = \{y \in A |\ xEy\}$$

van A.

Stelling 8.8 Zij E een equivalentierelatie op een verzameling A. Voor elke twee elementen x en y van A geldt:

- als xEy dan $[x] = [y]$;
- als $\neg(xEy)$ dan $[x] \cap [y] = \emptyset$.

Bewijs:

- Stel xEy, we gaan bewijzen dat $[x] = [y]$.
  - Stel $z \in [x]$.
    Dan geldt xEz volgens de definitie van $[x]$.
    Dan geldt zEx volgens symmetrie van E.
    Dan geldt zEy omdat xEy geldt en E transitief is.
    Dan geldt yEz volgens symmetrie van E.
    Dan geldt $z \in [y]$ volgens de definitie van $[y]$.
    We hebben dus bewezen $[x] \subseteq [y]$.
  - Stel omgekeerd $z \in [y]$.
    Dan geldt yEz volgens de definitie van $[y]$.
    Dan geldt xEz omdat xEy geldt en E transitief is.
    Dan geldt $z \in [x]$ volgens de definitie van $[x]$.
    We hebben dus bewezen $[y] \subseteq [x]$.

  Dit levert de gevraagde bewering $[x] = [y]$.
- Nu moeten we nog de tweede bewering van de stelling bewijzen: als $\neg(xEy)$ dan $[x] \cap [y] = \emptyset$.

Volgens contrapositie is dit equivalent aan:
als $[x] \cap [y] \neq \emptyset$ dan xEy.
Stel dat $[x] \cap [y] \neq \emptyset$.
Dan is er een $z \in [x] \cap [y]$.
Dan $z \in [x]$ en $z \in [y]$.
Dan xEz en yEz volgens de definitie van $[x]$ en $[y]$.
Dan xEz en zEy volgens symmetrie van E.
Dan xEy vanwege transitiviteit van E.
Dit is precies wat we moesten bewijzen.

Einde Bewijs.

Omdat E reflexief is geldt dat $x \in [x]$ voor elke $x \in A$. Samen met bovenstaande stelling concluderen we:

Voor elke equivalentierelatie op A zit elke $x \in A$ in precies één equivalentieklasse.

We hadden het begrip equivalentieklasse ook voor een willekeurige relatie kunnen definiëren, maar om te kunnen concluderen dat elke $x \in A$ in precies één equivalentieklasse zit hebben we precies de drie eigenschappen nodig die samen de definitie van equivalentierelatie vormen.

In het geval van de equivalentierelatie $=$ (voorbeeld 1) bestaat elke equivalentieklasse uit één element, en is ook elke verzameling van één element een equivalentieklasse.

In het geval van de equivalentierelatie $A \times A$ (voorbeeld 2) is er maar één equivalentieklasse, namelijk de hele verzameling A.

In het geval van equivalentie modulo n (voorbeeld 3) zijn er precies n equivalentieklassen:

$$\begin{array}{rcccl}
[0] & = & \{\ldots, -n, 0, n, 2n, \ldots\} & = & \{k * n \mid k \in \mathbf{Z}\} \\
[1] & = & \{\ldots, -n+1, 1, n+1, 2n+1, \ldots\} & = & \{k * n + 1 \mid k \in \mathbf{Z}\} \\
[2] & = & \{\ldots, -n+2, 2, n+2, 2n+2, \ldots\} & = & \{k * n + 2 \mid k \in \mathbf{Z}\} \\
\vdots & \vdots & \vdots & & \\
[n-1] & = & \{\ldots, -n-1, -1, n-1, 2n-1, \ldots\} & = & \{k * n + (n-1) \mid k \in \mathbf{Z}\}.
\end{array}$$

Bij de equivalentierelatie $\simeq_f$ uit Stelling 8.6 is de equivalentieklasse $[x]$ van een element x gelijk aan de verzameling $f^{-1}(f(x))$.

Uit Stelling 8.8 en de observatie dat $x \in [x]$ voor elke $x \in A$ concluderen we dat voor elke equivalentierelatie op A geldt:

Elke equivalentieklasse is een niet lege deelverzameling van A.

Ongelijke equivalentieklassen zijn disjunct.

Elk element x van A behoort tot een unieke equivalentieklasse.

Zo'n systeem van deelverzamelingen noemen we een partitie, preciezer geformuleerd in de volgende definitie.

Definitie 8.9 Zij A een verzameling. Een deelverzameling Z van $\mathcal{P}(A)$ heet een *partitie* van A als

- de lege verzameling is geen element van Z: $\emptyset \notin Z$.
- ongelijke elementen van Z zijn disjunct (als deelverzamelingen van A): $\forall u, v \in Z\ \langle u \neq v \rightarrow u \cap v = \emptyset \rangle$.
- elk element x van A behoort tot een element van Z:
  $\forall x \in A\ \exists z \in Z\ \langle x \in z \rangle$.

We kunnen ook zeggen: een partitie van A is een verzameling van niet-lege, disjuncte deelverzamelingen van A, waarvan de vereniging de hele verzameling A is.

Merk op dat er voor een partitie Z van A bij elk element x van A precies één element $p_Z(x)$ van Z is zo dat x tot $p_Z(x)$ behoort, omdat ongelijke elementen van Z disjunct zijn. Zo kunnen we p_Z opvatten als een afbeelding van A naar Z.

We hebben dus gezien dat de equivalentieklassen van een equivalentierelatie op A een partitie van A vormen. Hiervan geldt ook een omgekeerde, zoals we in de volgende stelling zien.

Stelling 8.10 Zij de deelverzameling Z van $\mathcal{P}(A)$ een partitie van A. Dan is de relatie E_Z op A, gedefinieerd door

$$x\ E_Z\ y \iff p_Z(x) = p_Z(y)$$

een equivalentierelatie op A.

Bewijs:

Pas Stelling 8.6 toe op de afbeelding $p_Z : A \rightarrow Z$.

Einde Bewijs.

Voor elke equivalentierelatie geldt dat als voor Z de partitie van de bijbehorende equivalentieklassen gekozen wordt, de equivalentierelatie E_Z gelijk is aan de oorspronkelijke equivalentierelatie.

Omgekeerd geldt voor elke partitie Z dat de partitie gevormd door de equivalentieklassen van de equivalentierelatie E_Z gelijk is aan de oorspronkelijke partitie Z.

Zo kunnen we dus naar willekeur equivalentierelaties vertalen in partities en omgekeerd.

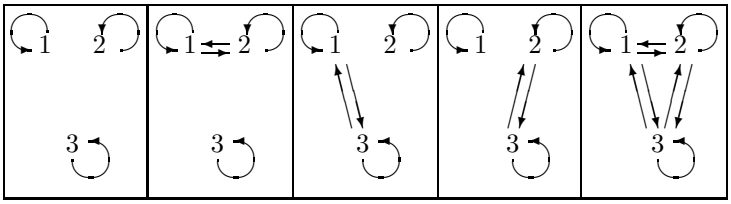
Als voorbeeld bekijken we alle partities van $A = \{1, 2, 3\}$.

$$Z_1 = \{\{1\}, \{2\}, \{3\}\}$$
$$Z_2 = \{\{1, 2\}, \{3\}\} \qquad Z_3 = \{\{1, 3\}, \{2\}\} \quad Z_4 = \{\{2, 3\}, \{1\}\}$$
$$Z_5 = \{A\}$$

De bijbehorende equivalentierelaties op A zijn

$$E_1 = \{(1, 1), (2, 2), (3, 3)\} \text{ (de diagonaal van } A \times A)$$
$$E_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$$
$$E_3 = \{(1, 1), (1, 3), (3, 1), (3, 3), (2, 2)\}$$
$$E_4 = \{(2, 2), (2, 3), (3, 2), (3, 3), (1, 1)\}$$
$$E_5 = A \times A$$

Als graaf weergegeven zien deze relaties er als volgt uit:



E_1 E_2 E_3 E_4 E_5

Een als graaf weergegeven equivalentierelatie op een eindige verzameling kenmerkt zich door de volgende drie eigenschappen:

- Elke knoop heeft een kant naar zichzelf (een *lus*).
- Als er een kant is van a naar b, dan ook een van b naar a: het is een *ongerichte graaf*.
- De verzameling knopen valt uiteen in stukken.
  Voor elk tweetal knopen a, b in een stuk is er een kant van a naar b.
  Voor elk tweetal knopen a, b in verschillende stukken is er geen kant van a naar b.

De verschillende stukken vormen juist de partitie van A die bij de equivalentierelatie hoort.

We sluiten dit hoofdstuk af met een interessante equivalentierelatie op een ongerichte graaf.

Stelling 8.11 In een ongerichte graaf is de relatie $\simeq$ gedefinieerd door

$$x \simeq y \iff \text{er is een pad van } x \text{ naar } y \text{ in de graaf}$$

een equivalentierelatie op de verzameling knopen van de graaf.

Bewijs:

De relatie $\simeq$ is reflexief, want voor elke knoop x is er een pad van x naar x: het lege pad.

De relatie $\simeq$ is symmetrisch, want als er een pad is van x naar y is er ook een pad van y naar x, namelijk hetzelfde in omgekeerde volgorde. Dit geldt omdat de graaf ongericht is.

De relatie $\simeq$ is symmetrisch, want als er een pad is van x naar y is en een pad van y naar z, dan kunnen die aan elkaar worden geknoopt tot een pad van x naar z.

Einde Bewijs.

Een equivalentieklasse van deze equivalentierelatie heet een *samenhangscomponent*, of kortweg *component* van de ongerichte graaf. Een ongerichte graaf is samenhangend dan en slechts dan als hij uit precies één samenhangscomponent bestaat. Bij een telefoonnetwerk is dat iets wat je graag wilt: dan kun je vanuit elke aangesloten telefoon naar elke andere aangesloten telefoon bellen.

8.4 Opgaven

Opgave 8.1

Ga van elk van de volgende relaties na of ze reflexief, symmetrisch of transitief zijn.

a. $\leq$ op $\mathbf{N}$;

b. $>$ op $\mathbf{N}$;

c. $\neq$ op $\mathbf{N}$;

d. $\emptyset$ op $\mathbf{N}$;

e. $\{(a,b),(b,a)\}$ op $\{a,b\}$;

f. $\{(a,b),(b,c)\}$ op $\{a,b,c\}$;

g. $\{(a,a),(a,b),(b,b),(b,c),(c,c)\}$ op $\{a,b,c\}$;

h. R op $\mathbf{N}$ gedefinieerd door

$$xRy \iff y < x+3 \wedge x < y+3;$$

Opgave 8.2

Beschouw de graaf bestaande uit vijf knopen a, b, c, d en e en vijf kanten (a,b), (a,e), (b,d), (c,b) en (d,c). Bepaal alle vijftien paren knopen (x,y) waarvoor er een pad van x naar y bestaat.

Opgave 8.3

a. Toon aan dat er voor elke $n \in \mathbf{N}$ een samenhangende gerichte graaf bestaat met precies n knopen en precies n kanten.

b. Gegeven is $n \in \mathbf{N}$ met $n > 1$. Toon aan dat er geen samenhangende gerichte graaf bestaat met precies n knopen en precies $n - 1$ kanten.

Opgave 8.4

Zij R de relatie op $\mathbf{Z}$, gegeven door $xRy \Leftrightarrow |x| = |y|$.

a. Bewijs dat R een equivalentierelatie is.

b. Hoe zien de equivalentieklassen er in dit geval uit?

Opgave 8.5

We bekijken de relatie R op $\mathbf{R}$ gegeven door $xRy \Leftrightarrow x = \cos y$.

a. Is R de grafiek van een afbeelding $f : \mathbf{R} \to \mathbf{R}$?

b. Bepaal de relatie R^{-1}.

c. Is R^{-1} de grafiek van een afbeelding $f : \mathbf{R} \to \mathbf{R}$?

Opgave 8.6

Gegeven is een relatie R van X naar Y die de grafiek is van een afbeelding $f : X \to Y$. Bewijs dat $R^{-1} \circ R$ een equivalentierelatie op X is. Geef duidelijk aan waar gebruik gemaakt wordt van de veronderstelling dat R de grafiek is van een afbeelding.

Opgave 8.7

Op $\mathbf{R} \times \mathbf{R} - \{(0, 0)\}$ definiëren we de relatie Q door

$$(x, y)Q(u, v) \Leftrightarrow xv = uy.$$

a. Toon aan dat Q een equivalentierelatie is.

b. Bepaal de equivalentieklassen van $(x, 0)$, van $(0, x)$, van (x, x), van (x, y). Neem hierbij aan dat x en y beide ongelijk aan nul zijn.

c. Geef in een plaatje van $\mathbf{R} \times \mathbf{R} - \{(0, 0)\}$ een indruk van de door Q bepaalde partitie.

Opgave 8.8

Zij R de relatie op $\mathbf{N}$, gegeven door $xRy \Leftrightarrow x|y$. Hierin betekent $x|y$ dat x een *deler* is van y, oftewel dat er een $z \in \mathbf{N}$ bestaat met $x * z = y$.

a. Laat zien dat $R \circ R = R$.

b. Geef een voorbeeld van een relatie S op $\mathbf{N}$ waarvoor niet geldt dat $S \circ S = S$.

Opgave 8.9

Gegeven zijn eindige verzamelingen A, B en C. De relaties R van A naar B en S van B naar C zijn gegeven door hun matrixvoorstellingen (hierbij nemen we een vaste volgorde voor de elementen van respectievelijk A, B, C).

a. Beschrijf een procedure om de matrixvoorstelling van $S \circ R$ te bepalen.

b. Beschrijf een procedure om de matrixvoorstelling van de relatie R^{-1} van B naar A te bepalen.

c. G is de relatie $xGy \Leftrightarrow x > y$ op $\{1, 2, 3, 4, 5\}$. Geef de matrixvoorstelling van G, van $G \circ G$, van $G \circ G \circ G$ etc.

Opgave 8.10

Zij G de relatie op $\mathbf{N} \times \mathbf{N}$ gegeven door $(m, n)G(r, s) \Leftrightarrow m + s = n + r$.

a. Bewijs dat G een equivalentierelatie is.

b. Teken in een plaatje van $\mathbf{N} \times \mathbf{N}$ een aantal equivalentieklassen van G.

Hoofdstuk 9

Ordeningen

In het vorige hoofdstuk hebben we algemene relaties van een verzameling naar een (andere) verzameling bekeken, en meer speciaal equivalentierelaties op een verzameling. Behalve de equivalentierelaties is er nog een andere belangrijke klasse van relaties op een verzameling, namelijk de zogenaamde partiële ordeningen. Zoals een equivalentierelatie een soort van gelijkheid beschrijft, bijvoorbeeld het hebben van een gemeenschappelijke eigenschap, zo beschrijft een partiële ordening een notie van groter en kleiner, waarbij ook gelijkheid is toegestaan. Reflexiviteit en transitiviteit zijn voor dat soort relaties net zo natuurlijk en wenselijk als bij equivalentierelaties, maar symmetrie juist niet: als a groter of gelijk is aan b hebben we juist niet dat b groter of gelijk is aan a. Integendeel: de twee eigenschappen 'a groter of gelijk b' en 'b groter of gelijk a' kunnen alleen maar samengaan als a en b aan elkaar gelijk zijn. Dit verschijnsel is in zekere zin het tegenovergestelde van symmetrie, en zullen we dan ook *antisymmetrie* noemen. Met herhaling van de definities van reflexiviteit en transitiviteit krijgen we dan de volgende definitie:

Definitie 9.1 Zij A een verzameling. Een relatie R van A naar A heet

- *reflexief* als geldt: $\forall x\langle xRx\rangle$;
- *antisymmetrisch* als geldt: $\forall x\forall y\langle(xRy \wedge yRx) \rightarrow x = y\rangle$;
- *transitief* als geldt: $\forall x\forall y\forall z\langle(xRy \wedge yRz) \rightarrow xRz\rangle$,
- een *partiële ordening*, of kortweg *ordening* als R zowel reflexief, antisymmetrisch als transitief is.

Een verzameling A samen met een partiële ordening daarop heet wel een *partieel geordende verzameling*, of kortweg *poset*, hetgeen een afkorting is van *partially ordered set*.

De relatie $\leq$ op $\mathbf{N}$ is een partiële ordening, want voor elke $x, y, z \in \mathbf{N}$ geldt:

- $x \leq x$, dus $\leq$ is reflexief;
- als $x \leq y$ en $y \leq x$ dan geldt $x = y$, dus $\leq$ is antisymmetrisch;

- als $x \leq y$ en $y \leq z$ dan geldt $x \leq z$, dus $\leq$ is transitief.

Net zo is de relatie $\geq$ op $\mathbf{N}$ een partiële ordening, en zijn de relaties $\leq$ en $\geq$ op elke andere deelverzameling van $\mathbf{R}$ partiële ordeningen. De relaties $<$ en $>$ op $\mathbf{N}$ zijn geen partiële ordeningen, deze relaties zijn niet reflexief: er geldt niet dat $x < x$ of $x > x$.

Definitie 9.2 Een partiële ordening R op A heet een *totale ordening* of *lineaire ordening* als voor elk tweetal elementen x en y van A geldt xRy of yRx.

De partiële ordeningen $\leq$ en $\geq$ op $\mathbf{N}$ of een andere deelverzameling van $\mathbf{R}$ zijn inderdaad totale ordeningen, want voor elk tweetal getallen x en y geldt $x \leq y$ of $y \leq x$.

We geven nu een aantal voorbeelden van partiële ordeningen die niet totaal zijn. Als eerste nemen we de relatie $\subseteq$ op $A = \mathcal{P}(X)$ voor een verzameling X. Er geldt inderdaad

- $Y \subseteq Y$ voor elke $Y \in \mathcal{P}(X)$, dus $\subseteq$ is reflexief;
- als $Y \subseteq Y'$ en $Y' \subseteq Y$ voor $Y, Y' \in \mathcal{P}(X)$, dan geldt $Y = Y'$, dit was namelijk de definitie van gelijkheid van verzamelingen, dus $\subseteq$ is antisymmetrisch;
- als $Y \subseteq Y'$ en $Y' \subseteq Y''$ voor $Y, Y', Y'' \in \mathcal{P}(X)$, dan geldt $Y \subseteq Y''$, dus $\subseteq$ is transitief.

Hiermee is aangetoond dat $\subseteq$ een partiële ordening is. Als X minstens twee elementen bevat is het echter niet een totale ordening, want als we twee verschillende elementen $x, y \in X$ kiezen, zijn $\{x\}$ en $\{y\}$ elementen van $A = \mathcal{P}(X)$, terwijl niet geldt $\{x\} \subseteq \{y\}$ en ook niet $\{y\} \subseteq \{x\}$.

Het tweede voorbeeld van partiële ordening die niet totaal is de *deelbaarheidsrelatie* $|$ op $\mathbf{N}$. Deze is gedefinieerd door

$$x|y \quad \Leftrightarrow \quad \exists k \in \mathbf{N}\, \langle x * k = y \rangle.$$

Als $x|y$ zeggen we dat y *deelbaar* is door x, of dat x een *deler* is van y. We gaan nu bewijzen dat de deelbaarheidsrelatie inderdaad een partiële ordening is.

- Voor elke $x \in \mathbf{N}$ geldt $x * 1 = x$, dus $\exists k \in \mathbf{N}\, \langle x * k = x \rangle$, dus $x|x$.

  Hiermee is bewezen dat $|$ reflexief is.

- Stel dat $x|y$ en $y|x$.

  Dan zijn er $k, k' \in \mathbf{N}$ met $x * k = y$ en $y * k' = x$.

  We onderscheiden twee gevallen: $x = 0$ en $x \neq 0$.

  Stel $x = 0$, dan is $y = x * k = 0$, dus $x = y$.

  Stel $x \neq 0$, dan is $x = y * k' = x * k * k'$. Vanwege $x \neq 0$ kunnen we delen door x, dus $k * k' = 1$. Vanwege $k, k' \in \mathbf{N}$ kan dit alleen als $k = k' = 1$. Hieruit volgt $x = y * k' = y$.

In beide gevallen hebben we bewezen dat $x = y$ voor willekeurige x, y met $x|y$ en $y|x$.

Hiermee is bewezen dat $|$ antisymmetrisch is.

- Stel dat $x|y$ en $y|z$.

  Dan zijn er $k, k' \in \mathbf{N}$ met $x * k = y$ en $y * k' = z$.

  Dan geldt $x * (k * k') = (x * k) * k' = y * k' = z$.

  Dus geldt $x|z$.

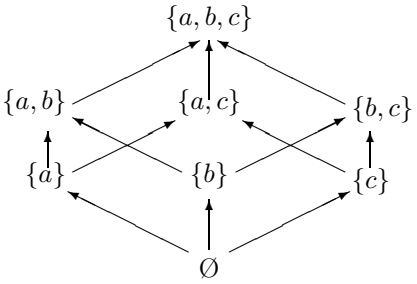
  Hiermee is bewezen dat $|$ transitief is.

Hiermee is bewezen dat $|$ een partiële ordening is. Het is echter geen totale ordening, want er geldt bijvoorbeeld niet $2|3$ en ook niet $3|2$.

Als een partiële ordening op een eindige verzameling als graaf weergegeven wordt, worden vaak een aantal overbodige pijlen weggelaten. Zo wordt elke *lus* (pijl van een knoop naar zichzelf) weggelaten, want vanwege reflexiviteit bestaat die voor elke knoop. Verder tekent men alleen de hoogst noodzakelijke pijlen. Hiermee bedoelen we dat men die pijlen weglaat waarvan de existentie op grond van transitiviteit uit reeds getekende pijlen volgt. Tenslotte wordt alles zo getekend dat alle pijlen omhoog of schuin omhoog wijzen. Met behulp van antisymmetrie kan worden aangetoond dat dit altijd mogelijk is. Een dergelijk uitgebeend pijlendiagram van een partiële ordening heet het *Hasse-diagram* van die partiële ordening.

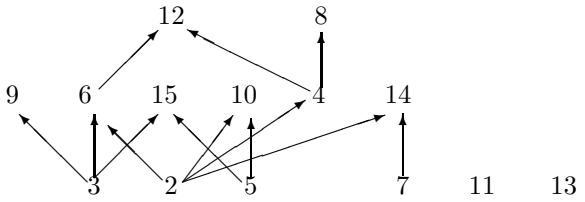
Ter illustratie tekenen we het Hasse-diagram voor de partiële ordening $x \subseteq y$ op $\mathcal{P}(X)$, waarbij $X = \{a, b, c\}$.

Dit is dus de partiële ordening R waarvoor geldt $xRy \leftrightarrow x \subseteq y$.



We zien hieruit bijvoorbeeld dat $\emptyset R\{a, b, c\}$ en $\emptyset R\{a, b\}$ en $\{a\}R\{a, b, c\}$, alhoewel de bijbehorende pijlen niet getekend zijn.

We tekenen ook het Hasse-diagram van de partiële ordening $|$ op $A = \{x \in \mathbf{N} | \ 2 \leq x \leq 15\}$.



Omdat alle pijlen omhoog of schuin omhoog wijzen zouden we ook nog de punten van de pijlen weg kunnen laten in een Hasse-diagram. In elk geval is een Hasse-diagram een gerichte graaf waarvoor geen enkel niet-leeg *pad* van een knoop naar zichzelf bestaat. Een niet-leeg pad van een knoop naar zichzelf wordt wel een *cykel* genoemd. Een gerichte graaf waarin geen cykels bestaan heet in het Engels *directed acyclic graph*, afgekort tot *dag*. In het Nederlands noemen we dit ook 'dag', maar houden wel de Engelse uitspraak aan. Een partiële ordening op een eindige verzameling definieert dus een dag: het Hasse-diagram. Omgekeerd definieert een dag als volgt een partiële ordening op de verzameling knopen. We definiëren voor een dag de relatie R op de verzameling knopen door

$$aRb \iff \text{er is een pad van } a \text{ naar } b.$$

De relatie R is

- reflexief, want van elke knoop is er een leeg pad naar zichzelf;
- antisymmetrisch, want als aRb en bRa voor $a \neq b$ dan geeft het aan elkaar knopen van de paden van a naar b en van b naar a een cykel van a;
- transitief, want als aRb en bRc dan geeft het aan elkaar knopen van de paden van a naar b en van b naar c een pad van a naar c.

Dus is R een partiële ordening op de verzameling knopen.

9.1 Maxima en minima, boven- en ondergrenzen

Partiële ordeningen spelen een grote rol in de wiskunde en de informatica. Er is een aantal begrippen mee verbonden die we nu de revue zullen laten passeren. Om de begrippen groot en klein hun betekenis te laten houden, denken we bij een partiële ordening R steeds aan: kleiner of gelijk aan. Je zou in deze definities ook elke 'R' kunnen vervangen door '$\leq$', als je daarbij in gedachten houdt dat dit slaat op een willekeurige partiéle ordening en niet alleen op de gebruikelijke ordening $\leq$ op getallen. Als A bestaat uit getallen en we willen iets zeggen over een andere ordening dan de gewone $\leq$ is het juist heel verwarrend om daar de notatie $\leq$ voor te gebruiken. Notaties die er wat op lijken, zoals $\preceq$ of $\sqsubseteq$, zijn nog wel bruikbaar.

Definitie 9.3 Laat R een partiële ordening op een verzameling A zijn, en B een deelverzameling van A.

- Een element b van B heet een *maximaal element* van B als er geen van b verschillend element x van B is zo dat bRx.
- Een element b van B heet een *minimaal element* van B als er geen van b verschillend element x van B is zo dat xRb.
- Een element b van B heet het *grootste element* of *maximum* van B als voor alle elementen x van B geldt xRb.
- Een element b van B heet het *kleinste element* of *minimum* van B als voor alle elementen x van B geldt bRx.
- Een element a van A heet een *bovengrens* of *majorant* van B als voor alle elementen x van B geldt xRa. De Engelse term voor bovengrens is *upper bound*.
- Een element a van A heet een *ondergrens* of *minorant* van B als voor alle elementen x van B geldt aRx. De Engelse term voor bovengrens is *lower bound*.
- Een bovengrens a van B heet de *kleinste bovengrens* of het *supremum* van B als voor elke bovengrens y van B geldt aRy. De Engelse term voor kleinste bovengrens is *least upper bound*.
- Een ondergrens a van B heet de *grootste ondergrens* of het *infimum* van B als voor elke ondergrens y van B geldt yRa. De Engelse term voor grootste ondergrens is *greatest lower bound*.

Merk op dat er een wezenlijk verschil is tussen “maximaal” en “grootste” en evenzo tussen “minimaal” en “kleinste”.
Ruwweg gezegd:

Maximaal :	niet kleiner dan een andere (geen andere is groter).
Grootste :	alle andere zijn kleiner (groter dan alle andere).
Minimaal :	er is geen andere die kleiner is.
Kleinste :	kleiner dan alle andere.

Voor een relatie R op een verzameling A is het eenvoudig in te zien dat

- als R reflexief is, dan is ook R^{-1} reflexief;
- als R antisymmetrisch is, dan is ook R^{-1} antisymmetrisch;
- als R transitief is, dan is ook R^{-1} transitief.

Als R een partiële ordening op A is, is R^{-1} dat dus ook. Een maximaal element met betrekking tot R is per definitie een minimaal element met betrekking tot R^{-1}, en omgekeerd. Net zo geldt voor elk van deze begrippen dat alles wat over R gezegd kan worden, ook over R^{-1} gezegd kan worden waarbij ‘groot’, ‘max’ en ‘boven’ vervangen wordt door respectievelijk ‘klein’, ‘min’ en ‘onder’, en omgekeerd. Als we een bewering bewijzen over

een willekeurige partiële ordening R, kunnen we deze bewering ook toepassen op R^{-1}, en daarmee hebben we een nieuwe bewering over R bewezen, namelijk dezelfde bewering maar dan met 'groot', 'max' en 'boven' vervangen door respectievelijk 'klein', 'min' en 'onder' en omgekeerd. Dit principe wordt *dualiteit* genoemd, en zullen we in het vervolg een aantal keren toepassen.

We gaan nu de begrippen uit Definitie 9.3 nader bestuderen.

Wegens de antisymmetrie van een partiële ordening R kan er hoogstens één grootste element van B zijn, want als $a \in B$ en $b \in B$ beide grootste element zijn, dan moet aRb en bRa gelden, zodat $a = b$.

Is $a \in B$ het grootste element van B, dan noteren we: $a = \max(B)$.

Vanwege dualiteit kan er evenzo hoogstens één kleinste element van B zijn.

Is $b \in B$ het kleinste element van B, dan noteren we: $b = \min(B)$.

De volgende stelling zegt dat iets soortgelijks geldt voor grootste ondergrens en kleinste bovengrens.

Stelling 9.4 Voor elke partiële ordening op een verzameling A heeft elke deelverzameling $B \subseteq A$ hoogstens één kleinste bovengrens en hoogstens één grootste ondergrens.

Bewijs:

Vanwege dualiteit is het voldoende om alleen te bewijzen dat $B \subseteq A$ hoogstens één kleinste bovengrens heeft.

Stel dat $a \in A$ en $a' \in A$ allebei een kleinste bovengrens van B zijn.

Dan zijn ze allebei een bovengrens van B.

Omdat a een kleinste bovengrens van B is, geldt aRa'.

Omdat a' een kleinste bovengrens van B is, geldt $a'Ra$.

Vanwege antisymmetrie geldt nu dat $a = a'$.

Einde Bewijs.

In de definitie hebben wel op deze stelling vooruitgelopen door te spreken over 'de' kleinste bovengrens en 'de' grootste ondergrens.

Is $a \in A$ de kleinste bovengrens van B, dan noteren we: $a = \sup(B)$, of in het Engels: $a = \text{lub}(B)$.

Is $b \in A$ de grootste ondergrens van B, dan noteren we: $b = \inf(B)$, of in het Engels: $b = \text{glb}(B)$.

Zowel voor kleinste bovengrens als grootste ondergrens van een deelverzameling $B \subseteq A$ zijn er drie mogelijkheden:

- hij bestaat en is een element van B;
- hij bestaat maar is geen element van B;
- hij bestaat niet.

We lichten dit toe aan de ordening $\leq$ op de reële getallen. Hierin heeft de deelverzameling $\mathbf{Z}$ geen bovengrens en geen ondergrens, dus zeker ook geen kleinste bovengrens en geen grootste ondergrens. De twee verzamelingen

$$\{x \in \mathbf{R} \mid 1 \leq x \leq 2\} \quad \text{en} \quad \{x \in \mathbf{R} \mid 1 < x < 2\}$$

hebben allebei het getal 2 als kleinste bovengrens en het getal 1 als grootste ondergrens. In het eerste geval zijn beide getallen wel bevat in de gegeven deelverzameling, in het tweede geval niet.

Stelling 9.5 Laat A een partieel geordende verzameling zijn en B een deelverzameling van A. Dan geldt

- als de kleinste bovengrens $\sup(B)$ van B bestaat en $\sup(B) \in B$ dan heeft B een grootste element $\max(B)$ en geldt $\max(B) = \sup(B)$;
- als het grootste element $\max(B)$ van B bestaat, dan bestaat ook de kleinste bovengrens $\sup(B)$ van B en geldt $\sup(B) = \max(B) \in B$;
- als de grootste ondergrens $\inf(B)$ van B bestaat en $\inf(B) \in B$ dan heeft B een kleinste element $\min(B)$ en geldt $\min(B) = \inf(B)$;
- als het kleinste element $\min(B)$ van B bestaat, dan bestaat ook de grootste ondergrens $\inf(B)$ van B en geldt $\inf(B) = \min(B) \in B$.

Bewijs:

De eerste bewering volgt direct uit de definitie van grootste element en kleinste bovengrens.

Voor de tweede bewering nemen we aan dat $\max(B)$ bestaat en moeten we laten zien dat $\sup(B)$ bestaat en dat $\sup(B) = \max(B) \in B$. De eis dat $\max(B) \in B$ geldt per definitie; we hoeven alleen te laten zien dat $\max(B)$ voldoet aan de definitie van kleinste bovengrens van B.

Volgens de definitie van grootste element is inderdaad $\max(B)$ een bovengrens van B. Stel dat ook c een bovengrens is van B, dan is $\max(B)Rc$ vanwege $\max(B) \in B$. Hiermee is bewezen dat $\max(B)$ een kleinste bovengrens is van B.

De derde en vierde bewering volgen met dualiteit uit de eerste en tweede bewering.

Einde Bewijs.

Als $A = \mathcal{P}(V)$ voor zekere verzameling V en R is de partiële ordening $\subseteq$ en $B \subseteq A$, dan is

$$\overline{B} = \bigcup_{X \in B} X$$

de kleinste bovengrens van B, want er geldt:

- $\forall X \in B \langle X \subseteq \overline{B} \rangle$, dus $\overline{B}$ is een bovengrens van B;
- als Y een bovengrens is van B dan geldt $\forall X \in B \langle X \subseteq Y \rangle$, en dus ook $\overline{B} = \bigcup_{X \in B} X \subseteq Y$.

Net zo is $\bigcap_{X \in B} X$ de grootste ondergrens van B. Zoals gebruikelijk is hierbij gedefinieerd $\bigcup_{X \in \emptyset} X = \emptyset$ en $\bigcap_{X \in \emptyset} X = V$ omdat de lege verameling $\emptyset$ en het universum V de neutrale elementen zijn van respectievelijk de vereniging en de doorsnede.

We beschouwen nu de partiële ordening $|$ op $A = \{x \in \mathbf{N} |\ 2 \leq x \leq 15\}$. Hiervan hebben we eerder het Hasse-diagram gegeven.

Minimale elementen van A zijn: 2, 3, 5, 7, 11, 13.
Maximale elementen van A zijn: 8, 9, 10, 11, 12, 13, 14, 15.
A heeft geen kleinste element en ook geen grootste element.
Als deelverzameling van zichzelf heeft A geen bovengrenzen en ook geen ondergrenzen.

Zij $B = \{2, 3\}$.
Maximale èn minimale elementen van B zijn 2 en 3.
B heeft geen kleinste en geen grootste element.
B heeft geen ondergrenzen (in A), dus ook geen grootste ondergrens.
Bovengrenzen van B (in A) zijn 6 en 12.
De kleinste bovengrens van B (in A) is 6: $\sup(B) = 6$.

We nemen nu $C = \{2, 4\}$.
Het grootste element van C is 4: $\max(C) = 4$.
Dit is tevens het enige maximale element van C.
Het kleinste element van C is 2: $\min(C) = 2$.
Dit is tevens het enige minimale element van C.
De enige ondergrens van C (in A) is 2.
Dit is ook de grootste ondergrens van C (in A): $\inf(C) = 2$.
Bovengrenzen van C (in A) zijn 4, 8, 12.
De kleinste bovengrens van C (in A) is 4: $\sup(C) = 4$.

Het kan voorkomen dat een deelverzameling wel bovengrenzen maar geen kleinste bovengrens heeft. Zo is bij de partiële ordening $|$ op $\{2, 3, 12, 18\}$ zowel 12 als 18 een bovengrens van $\{2, 3\}$, maar geen van beide bovengrenzen is de kleinste bovengrens omdat niet geldt $12|18$ en ook niet geldt $18|12$. Vanwege dualiteit kunnen analoge situaties optreden ten aanzien van ondergrenzen. Verzin zelf nog meer voorbeelden, vooral aan de hand van tekeningen van posets.

We hebben gezien dat boven- en ondergrenzen en grootste en kleinste elementen niet altijd bestaan. De volgende stelling geeft een criterium waarvoor ze wel bestaan.

Stelling 9.6 Gegeven is een totale ordening R op een verzameling A en een eindige niet-lege deelverzameling B van A. Dan heeft B een grootste element $\max(B)$, een kleinste element $\min(B)$, een kleinste bovengrens $\sup(B)$, een grootste ondergrens $\inf(B)$ en geldt $\max(B) = \sup(B)$ en $\min(B) = \inf(B)$.

Bewijs:

Als R een totale ordening is, is ook R^{-1} een totale ordening; vanwege dualiteit is het dus voldoende te bewijzen dat $\max(B)$ en $\sup(B)$ bestaan en gelijk aan elkaar zijn.

We bewijzen met inductie naar n:

$$\text{Als } \#B = n \geq 1 \text{ dan bestaat } \max(B).$$

Basisstap: als $\#B = 1$ dan is $B = \{b\}$ en voldoet b aan de definitie van grootste element van B.

Inductiestap: stel dat elke verzameling met $n \geq 1$ elementen een grootste element bevat, dan moeten we bewijzen dat B met $\#B = n+1$ ook een grootste element bevat.

Kies een willekeurig element $b \in B$. Dan geldt $\#(B - \{b\}) = n \geq 1$, en weten we volgens de inductiehypothese dat $B - \{b\}$ een grootste element b' bevat. Omdat de ordening totaal is, geldt bRb' of $b'Rb$.

- Stel bRb'. Kies een willekeurig element $a \in B$. Als $a = b$ dan geldt aRb'. Als $a \neq b$ dan geldt $a \in B - \{b\}$ end dus aRb' want b' is het grootste element van $B - \{b\}$. In beide gevallen geldt aRb', dus voldoet b' aan de definitie van grootste element van B.
- Stel $b'Rb$. Kies een willekeurig element $a \in B$. Als $a = b$ dan geldt aRb vanwege reflexiviteit. Als $a \neq b$ dan geldt $a \in B - \{b\}$ en dus aRb' want b' is het grootste element van B - {b}. Vanwege transitiviteit en $b'Rb$ geldt dan aRb. In beide gevallen geldt aRb, dus voldoet b aan de definitie van grootste element van B.

In beide gevallen hebben we bewezen dat B een grootste element $\max(B)$ bevat.

Hiermee is het bewijs met inductie voltooid.

We moeten nog laten zien dat ook $\sup(B)$ bestaat en dat $\sup(B) = \max(B)$, dit hebben we echter in Stelling 9.5 al bewezen.

Einde Bewijs.

Met betrekking tot de (niet-totale) partiële ordening $|$ op $\mathbf{N}$ merken we zonder bewijs op dat daar elke verzameling een kleinste bovengrens en een grootste ondergrens heeft. De grootste ondergrens heet dan *grootste gemeenschappelijke deler*, afgekort tot *ggd*, in het Engels *greatest common divisor*, afgekort tot *gcd*. De kleinste bovengrens heet dan *kleinste gemeenschappelijke veelvoud*, afgekort tot *kgv*, in het Engels *least common multiple*, afgekort tot *lcm*. Zo is van de verzameling $\{6, 9, 15\}$ de ggd gelijk aan 3, en de kgv gelijk aan 90.

In deze ordening is 1 het kleinste element en is 0 het grootste element. Dit is misschien wat tegen-intuitief, maar aan de hand van de definitie eenvoudig na te gaan, want 1 is

deler van elk getal, en 0 is deelbaar door elk getal. Zo is 0 de ggd van de lege verzameling, en is ook 0 de kgv van een oneindige verzameling getallen.

Definitie 9.7 Een partieel geordende verzameling (A, R) heet een *tralie* (Engels: *lattice*) als voor elk tweetal elementen x en y van A de deelverzameling $\{x, y\}$ een kleinste bovengrens en een grootste ondergrens heeft.
Een partieel geordende verzameling (A, R) heet een *volledig tralie* (Engels: *complete lattice*) als elke niet-lege deelverzameling van A een kleinste bovengrens en een grootste ondergrens heeft.

Voorbeelden van volledige tralies zijn $\subseteq$ op $\mathcal{P}(V)$, en de deelbaarheidsrelatie op $\mathbf{N}$. Uit Stelling 9.6 volgt direct dat elke totale ordening een tralie is. Er zijn echter totale ordeningen die geen volledig tralie zijn, bijvoorbeeld de ordening $\leq$ op $\mathbf{N}$ of $\mathbf{R}$: hier heeft de hele verzameling geen bovengrens, en dus zeker geen kleinste bovengrens.

Stelling 9.8 In een tralie (A, R) heeft elke eindige niet-lege deelverzameling van A een kleinste bovengrens en een grootste ondergrens.

Bewijs:

Vanwege dualiteit is het voldoende te bewijzen dat elke eindige niet-lege deelverzameling B van A een kleinste bovengrens heeft. Dit gaan we met inductie naar n bewijzen, waar $n = \#B \geq 1$.

Basisstap: als $\#B = 1$ dan is $B = \{b\}$ en voldoet b aan de definitie van kleinste bovengrens van B.

Inductiestap: stel dat elke verzameling met $n \geq 1$ elementen een kleinste bovengrens heeft, dan moeten we bewijzen dat B met $\#B = n + 1$ ook een kleinste bovengrens heeft.

Kies een element $b \in B$. Dan geldt $\#(B - \{b\}) = n \geq 1$, en weten we volgens de inductiehypothese dat $B - \{b\}$ een kleinste bovengrens b' heeft. Omdat (A, R) een tralie is, heeft $\{b, b'\}$ een kleinste bovengrens c.

Kies een willekeurig element $a \in B$.

- Stel $a = b$, dan geldt aRc omdat c een bovengrens is van $\{b, b'\}$.
- Stel $a \neq b$. Dan geldt $a \in B - \{b\}$, en dus aRb' want b' is een bovengrens van $B - \{b\}$. Maar er geldt ook $b'Rc$ omdat c een bovengrens is van $\{b, b'\}$. Uit transitiviteit volgt nu aRc.

Voor elk willekeurig element $a \in B$ geldt dus aRc, dus c is een bovengrens van B.

Stel nu dat ook d een bovengrens van B is.

Dan geldt bRd, en er geldt dat d een bovengrens van $B - \{b\}$ is.

Omdat b' de kleinste bovengrens van $B - \{b\}$ is, geldt $b'Rd$.

Samen met bRd volgt nu dat d een bovengrens is van $\{b, b'\}$.

Omdat c de kleinste bovengrens is van $\{b, b'\}$ volgt hieruit dat cRd.

Hiermee hebben we bewezen dat c een kleinste bovengrens is van B, hetgeen we moesten bewijzen.

Einde Bewijs.

Het verschil tussen een tralie en een volledig tralie zit hem dus alleen in de eis op oneindige verzamelingen. Een direct gevolg van Stelling 9.8 is dat elk eindig tralie een volledig tralie is.

De volgende stelling geeft een verrassend verband tussen volledige tralies en het bestaan van dekpunten. Een element $a \in A$ heet een *dekpunt* van een afbeelding $f : A \to A$ als $f(a) = a$. Als (A, R) een partieel geordende verzameling is, dan heet een afbeelding $f : A \to A$ *monotoon* als voor alle $x, y \in A$ geldt:

$$\text{als } xRy \text{ dan geldt ook } f(x)Rf(y).$$

Stelling 9.9 Laat (A, R) een volledig tralie zijn, $A \neq \emptyset$, en $f : A \to A$ een monotone afbeelding. Dan heeft f een dekpunt.

Bewijs:

Definieer $B \subseteq A$ door $B = \{z \in A |\ zRf(z)\}$.

Omdat (A, R) een volledig tralie is bestaat $\inf(A)$.

Vanwege $\inf(A) \in B$ geldt $B \neq \emptyset$, omdat (A, R) een volledig tralie is bestaat $\sup(B)$.

Definieer nu $a = \sup(B)$.

Kies $x \in B$ willekeurig. Dan geldt xRa want a is een bovengrens van B. Omdat f monotoon is, geldt $f(x)Rf(a)$. Vanwege de definitie van B geldt $xRf(x)$, met transitiviteit volgt $xRf(a)$.

We hebben dus bewezen dat $f(a)$ een bovengrens is van B.

Omdat a de kleinste bovengrens is van B geldt $aRf(a)$.

Wegens de monotonie van f geldt nu $f(a)Rf(f(a))$.

Dus $f(a) \in B$, wegens de definitie van B.

Maar dan hebben we $f(a)Ra$, want a is een bovengrens van B.

Samen met $aRf(a)$ en anti-symmetrie volgt dus $a = f(a)$.

Hiermee is bewezen dat a een dekpunt van f is.

Einde Bewijs.

Op $\mathbf{N}$ is de deelbaarheidsrelatie $|$ een volledig tralie. Een voorbeeld van een monotone afbeelding $f : \mathbf{N} \to \mathbf{N}$ is de afbeelding f gedefinieerd door $f(x) = 2x$ voor alle $x \in \mathbf{N}$, want

als $x|y$ dan geldt ook $2x|2y$. Volgens Stelling 9.9 heeft f een dekpunt. Dat is inderdaad het geval, want $f(0) = 0$, dus 0 is een dekpunt van f.

Een voorbeeld van een monotone afbeelding $f : \mathbf{R} \to \mathbf{R}$ met betrekking tot het tralie $(\mathbf{R}, \leq)$ is de afbeelding f gedefinieerd door $f(x) = x + 1$ voor alle $x \in \mathbf{R}$. Deze monotone afbeelding heeft geen dekpunt, want er bestaat geen $x \in \mathbf{R}$ waarvoor $x = x + 1$. Dit is niet in tegenspraak met Stelling 9.9, want het tralie $(\mathbf{R}, \leq)$ is geen volledig tralie.

Een voorbeeld van een monotone afbeelding $f : \mathcal{P}(\mathbf{N}) \to \mathcal{P}(\mathbf{N})$ met betrekking tot het volledige tralie $(\mathcal{P}(\mathbf{N}), \subseteq)$ is de afbeelding f gedefinieerd door

$$f(V) = (\{17\} \cup \{2x + 3 \mid x \in V\}) - \{13\}$$

voor elke $V \subseteq \mathbf{N}$. Volgens Stelling 9.9 heeft f een dekpunt; dit is inderdaad het geval, want voor

$$U \;=\; \{5 * 2^{k+2} - 3 \mid k \in \mathbf{N}\} \;=\; \{17, 37, 77, 157, 317, 637, 1277, \ldots\}$$

geldt $f(U) = U$, dus U is een dekpunt.

Laten we nog even bij het bewijs van Stelling 9.9 stilstaan. Om te controleren dat het klopt is niet zo moeilijk: gewoon alle stappen nagaan, en dat zijn er niet zo heel veel. Dus als je dit bewijs hebt, is het niet zo moeilijk om je ervan te overtuigen dat de stelling geldt. Maar als je dit bewijs nou niet hebt, en je zou zelf moeten proberen de stelling te bewijzen? Dat is behoorlijk lastig. We hebben wel bewijzen gegeven die je zelf ook zou kunnen verzinnen. Bijvoorbeeld het bewijs dat $|$ een partiële ordening is. Dan moet je per definitie drie eigenschappen nagaan, en dat nagaan is een kwestie van invullen en zien dat het klopt. Het bewijs van Stelling 9.9 is duidelijk van een andere soort. Hoe kom je bijvoorbeeld op het idee om voor B die specifieke verzameling te nemen, en daar dan weer de kleinste bovengrens van te nemen? Hoewel niet iedereen daar even gevoelig voor is, kunnen we zeggen dat een dergelijk kort bewijs van een niet-voor-de-hand-liggende bewering bepaalde charmes heeft. Een kort en verrassend bewijs wordt wel een *elegant bewijs* genoemd, al is het natuurlijk zeer persoonlijk wat wel en wat niet elegant is . . . .

9.2 Sorteren en lexicografische ordening

Als R een totale ordening op een verzameling A is, en B is een eindige deelverzameling van A met n elementen, dan is er precies één rij $b_1, b_2, b_3, \ldots, b_n$ zodanig dat

- $\{b_1, b_2, b_3, \ldots, b_n\} = B$, en
- voor elke $i \in \{1, 2, 3, \ldots, n-1\}$ geldt $b_i R b_{i+1}$.

Dit is niet zo moeilijk in te zien: wegens transitiviteit volgt uit de tweede eis dat b_1 het kleinste element van B moet zijn, en volgens Stelling 9.6 bestaat dat element. Net zo is

$$b_2 = \min(B - \{b_1\}),$$

$$b_3 = \min(B - \{b_1, b_2\}),$$

$$b_4 = \min(B - \{b_1, b_2, b_3\}),$$

net zo lang tot de hele rij vastligt.

Het vinden van deze rij $b_1, b_2, b_3, \ldots, b_n$ bij een gegeven eindige verzameling B heet *sorteren*. Als een verzameling elementen als gesorteerde rij wordt opgeslagen, is efficiënt zoeken mogelijk. Als de woorden in een woordenboek niet gesorteerd zouden zijn, zou het opzoeken van een woord daarin heel inefficiënt zijn: je kunt dan niets beters verzinnen dan vanaf de eerste bladzijde alle woorden nalopen totdat je het tegenkomt. Gelukkig zijn de woorden in een woordenboek en in de index van dit dictaat wel gesorteerd, en daarmee kun je gelijk aan een willekeurig woord op een willekeurig opgeslagen bladzijde zien of het woord wat je zoekt ervoor of erna te vinden zal moeten zijn. Dit maakt heel efficiënt zoeken mogelijk.

Voor dit sorteren en zoeken is de onderliggende totale ordening essentieel. Voor getallen ligt het voor de hand de gebruikelijke totale ordening $\leq$ te nemen, zo levert sorteren van de verzameling $\{9, 12, 7, 3, 18, 1, 6, 4\}$ de gesorteerde rij

$$1, 3, 4, 6, 7, 9, 12, 18$$

op.

Om woorden in een woordenboek te kunnen sorteren is een totale ordening op woorden nodig, waarbij een woord een eindige rij letters is. We gaan nu bespreken hoe je zo'n ordening in zijn algemeenheid kunt definiëren zodanig dat die overeenkomt met de gebruikelijke alfabetische ordening.

Op de letters hebben we al een totale ordening, namelijk de totale ordening gegeven door de volgorde

$$a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z.$$

Een letter noemen we kleiner dan een andere letter als hij eerder in deze rij voorkomt. We definiëren nu een *woord* over een verzameling A als een eindige rij elementen van A; de verzameling woorden over een verzameling A wordt aangegeven als A^*. De verzameling A waarover de woorden worden beschouwd heet zelf het *alfabet*. Op deze manier is een 'gewoon' woord een woord over het gebruikelijke alfabet, namelijk de verzameling van 26 letters. Op die 26 letters hebben we al een ordening, we gaan nu een manier beschrijven waarmee een ordening op een verzameling A een nieuwe ordening definieert op de verzameling A^* van alle woorden over A.

Ter bevordering van de leesbaarheid schrijven we de ordening op A als $\preceq$ en gebruiken we de notatie $\prec$ voor de relatie op A gedefinieerd door

$$a \prec b \iff a \preceq b \wedge \neg(a = b).$$

Het idee van de *lexicografische ordening* $\preceq^*$ op A^* is dat je eerst naar de meest linkse letter kijkt, en op grond daarvan probeert te beslissen welk van de twee woorden de kleinste is. In geval van gelijkheid lukt dat niet, dan kijk je naar de tweede letter. Als die ook weer gelijk zijn, kijk je naar de derde, enzovoorts. Verder wil je dat een beginstuk van een woord kleiner is dan het woord zelf. De algemene definitie luidt als volgt: er geldt $a_1, \ldots, a_n \preceq^* b_1, \ldots, b_m$ precies dan als een van de twee volgende voorwaarden geldt:

- er is een $i \in \{1, \ldots, \min(m,n)\}$ waarvoor $a_i \prec b_i$ en voor elke j met $j < i$ geldt $a_j = b_j$, of
- $n \leq m$ en voor elke $i \in \{1, \ldots, n\}$ geldt $a_i = b_i$.

Voor het geval dat A bestaat uit de 26 letters is dit inderdaad precies de ordening die gehanteerd worden bij woordenboeken en andere alfabetische rangschikkingen. In dit geval wordt de lexicografische ordening ook wel *alfabetische ordening* genoemd.

We willen graag bewijzen dat als $\preceq$ een willekeurige partiële ordening is op een willekeurige verzameling A, dan is $\preceq^*$ een partiële ordening op A^*. Nu kunnen we dit rechtstreeks met de definitie doen, maar dit vergt nogal wat gevalsonderscheid. Als we bijvoorbeeld transitiviteit willen bewijzen nemen we aan dat $r \preceq^* s$ en $s \preceq^* t$ voor rijen r, s, t en moeten we bewijzen dat $r \preceq^* t$. Daartoe moeten we zowel voor $r \preceq^* s$ als voor $s \preceq^* t$ alle mogelijke gevallen van de definitie onderscheiden. Om dit te voorkomen geven we eerst een equivalente karakterisering van $\preceq^*$.

Daartoe definiëren we een nieuwe verzameling $\overline{A} = A \cup \{q\}$, waar q een element is dat niet in A bevat is. We definiëren een partiële ordening $\sqsubseteq$ op $\overline{A}$ door

$$a \sqsubseteq b \iff a = q \vee (a \in A \wedge b \in A \wedge a \preceq b).$$

Het is eenvoudig na te gaan dat $\sqsubseteq$ een partiële ordening op $\overline{A}$ is; dit is een constructie die vaak bij het manipuleren met ordeningen gebruikt wordt. We hebben gewoon een nieuw element aan A toegevoegd, en de ordening op A uitgebreid door dit nieuwe element kleiner te verklaren dan alle andere elementen. Voor deze nieuwe ordening definiëren we

$$a \sqsubset b \iff a \sqsubseteq b \wedge \neg(a = b).$$

We definiëren nu de afbeelding $f : A^* \times \{k \in \mathbf{N} | k > 0\} \to \overline{A}$ door

$$f((a_1, \ldots, a_n), k) = \begin{cases} a_k & \text{als } k \leq n \\ q & \text{als } k > n. \end{cases}$$

Het volgende lemma volgt direct uit de definitie van $\preceq^*$:

Lemma
Voor $r, s \in A^*$ geldt

$$r \preceq^* s \iff r = s \vee \exists i \langle f(r,i) \sqsubset f(s,i) \wedge \forall j \langle j < i \to f(r,j) = f(s,j) \rangle \rangle.$$

Op het eerste gezicht ziet dit er misschien wat ingewikkeld uit. Het is echter niet meer dan het precies opschrijven van de volgende observatie:

> voeg een nieuw element q aan A toe dat kleiner is dan alle andere elementen, en denk alle rijtjes elementen van A aangevuld met een voldoende aantal q's. Dan kunnen we de tweede voorwaarde in de definitie van $\preceq^*$ terugbrengen tot gelijkheid van beide rijen.

Met dit lemma kunnen we met veel minder gevalsonderscheid de gewenste stelling bewijzen.

Stelling 9.10 Als $\preceq$ een partiële ordening is op A dan is $\preceq^*$ een partiële ordening op A^*.
Als $\preceq$ een totale ordening is op A dan is $\preceq^*$ een totale ordening op A^*.

Bewijs:

Neem aan dat $\preceq$ een partiële ordening is op A; we gaan bewijzen dat $\preceq^*$ een partiële ordening is op A^*.

Uit het lemma volgt direct dat $\preceq^*$ reflexief is.

Om antisymmetrie te bewijzen stellen we dat $r \preceq^* s$ en $s \preceq^* r$. Als $r \neq s$ zijn er volgens het lemma i en k met $f(r,i) \sqsubset f(s,i) \wedge \forall j\langle j < i \rightarrow f(r,j) = f(s,j)$ en $f(s,k) \sqsubset f(r,k) \wedge \forall j\langle j < k \rightarrow f(r,j) = f(s,j)$. Dit is in tegenspraak met de definitie van $\sqsubset$. Dus geldt $r = s$ en is antisymmetrie bewezen.

Om transitiviteit te bewijzen stellen we dat $r \preceq^* s$ en $s \preceq^* t$. Als $r = s$ of $s = t$ volgt direct dat $r \preceq^* t$. In het resterende geval zijn er volgens het lemma i en k met $f(r,i) \sqsubset f(s,i) \wedge \forall j\langle j < i \rightarrow f(r,j) = f(s,j)$ en $f(s,k) \sqsubset f(t,k) \wedge \forall j\langle j < k \rightarrow f(s,j) = f(t,j)$. Kies $m = \min(i,k)$, dan geldt $f(r,m) \sqsubset f(t,m) \wedge \forall j\langle j < m \rightarrow f(r,j) = f(t,j)$, volgens het lemma volgt hieruit dat $r \preceq^* t$. Hiermee is transitiviteit bewezen.

Hiermee hebben we bewezen dat $\preceq^*$ een partiële ordening is op A^*.

Voor het tweede deel van de stelling nemen we aan dat $\preceq$ een totale ordening is op A en kiezen we $r, s \in A^*$. Als $f(r,i) = f(s,i)$ voor elke $i > 0$ dan is $r = s$ en dus ook $r \preceq^* s$.

In het resterende geval is er een $i > 0$ met $f(r,i) \neq f(s,i)$. Kies voor i de kleinste waarde waarvoor $f(r,i) \neq f(s,i)$, dan is $f(r,j) = f(s,j)$ voor alle j met $j < i$.

Omdat $\preceq$ een totale ordening is op A is $\sqsubseteq$ een totale ordening is op $\overline{A}$, en geldt dus $f(r,i) \sqsubset f(s,i)$ of $f(s,i) \sqsubset f(r,i)$.

Volgens het lemma geldt in het eerste geval dat $r \preceq^* s$, en in het tweede geval dat $s \preceq^* r$.

Hiermee is bewezen dat $\preceq^*$ een totale ordening is op A^*.

Einde Bewijs.

Als R een partiële ordening op een verzameling A is en S een partiële ordening op een verzameling B, dan is er ook een *lexicografische ordening* RS op het Cartesisch product $A \times B$ te definiëren:

$$(a,b)RS(a'b') \iff (aRa' \wedge a \neq a') \vee (a = a' \wedge bSb').$$

Hiervoor geldt een soortgelijke stelling:

Stelling 9.11 Als R een partiële ordening is op A en S een partiële ordening is op B dan is RS een partiële ordening op $A \times B$.
Als R een totale ordening is op A en S een totale ordening is op B dan is RS een totale ordening op $A \times B$.

Het bewijs van deze stelling is een stuk eenvoudiger dan dat van Stelling 9.10 en laten we aan de lezer over.

9.3 Opgaven

Opgave 9.1

Op $\mathbf{R}$ definiëren we de relaties R, S en T door

$$xRy \Leftrightarrow \sin(x) \leq \sin(y),$$

$$xSy \Leftrightarrow (x = y \vee \sin(x) < \sin(y)),$$

$$xTy \Leftrightarrow |x| \leq y.$$

Ga voor elk van deze drie relaties na of het een partiële ordening is of niet; bewijs uw antwoord.

Opgave 9.2

Welke van de volgende relaties R op $\mathbf{Z} \times \mathbf{Z}$ definiëren een partiële ordening op $\mathbf{Z} \times \mathbf{Z}$ (motiveer uw beweringen):

a. $(m, n)R(r, s)$ betekent $m < r$ of $(m = r$ en $n \geq s)$;

b. $(m, n)R(r, s)$ betekent $n - s \geq (m - r)^2$;

c. $(m, n)R(r, s)$ betekent $m \geq r$ en $n \leq s$;

d. $(m, n)R(r, s)$ betekent $m + n \leq r$ en $n \leq s$;

e. $(m, n)R(r, s)$ betekent $m + n \leq r + s$ en $r \leq s$.

Opgave 9.3

Bewijs dat als het maximum $\max(B)$ van B bestaat, dan bestaat ook $\sup(B)$ en geldt $\sup(B) = \max(B)$.

Opgave 9.4

Bewijs dat de kleinste bovengrens van de lege verzameling gelijk is aan het kleinste element van de hele verzameling.

Opgave 9.5

Gegeven zijn twee verzamelingen A en B, een afbeelding $f : A \to B$ en een partiële ordening R op B. Bewijs dat

$$S = \{(x, y) \in A \times A \mid f(x)Rf(y)\}$$

een partiële ordening op A is dan en slechts dan als f injectief is.

Opgave 9.6

Laat de relatie R op de natuurlijke getallen gedefinieerd zijn door

$$R = \{(x, y) \mid x + y \text{ is even en } x \leq y\}.$$

a. Bewijs dat R een partiële ordening is.

b. Bepaal alle minimale elementen en alle bovengrenzen met betrekking tot deze partiële ordening R van de verzameling $B = \{2, 4, 5, 6, 7, 8\}$.

Opgave 9.7

Geef een voorbeeld van een poset die geen tralie is maar wel een grootste element en een kleinste element heeft.

Opgave 9.8

Voor ieder natuurlijk getal $n \neq 0$ duiden we met $d(n)$ het aantal delers van n in $\mathbf{N}$ aan. Dus $d(1) = 1$, $d(6) = 4$. We definiëren apart $d(0) = 0$.
Op $X = \{0, 1, 2, \ldots, 20\}$ definiëren we de volgende relatie K:

$$mKn \Leftrightarrow (n = m \text{ of } d(m) < d(n)).$$

a. Ga na dat (X, K) een poset is.

b. Teken het Hasse-diagram van (X, K).

c. Laat zien dat (X, K) geen tralie is.

d. Heeft X een grootste en/of een kleinste element?

e. Welke elementen van X zijn maximaal, resp. minimaal?

f. $A = \{3, 4, \ldots, 15\}$. Geef de verzameling van alle bovengrenzen van A in X. Is er een kleinste bovengrens, zo ja welke?

Geef de verzameling van alle ondergrenzen van A in X. Is er een grootste ondergrens, zo ja welke?

g. Welke elementen x van X voldoen aan ($3Kx$ en $xK15$)?

Opgave 9.9

Bewijs dat elke totale ordening een tralie is zonder gebruik te maken van Stelling 9.6.

Opgave 9.10

Op $\mathbf{R}$ definiëren we een relatie R door

$$xRy \;\Leftrightarrow\; (x = y \text{ of } \cos(x) < \cos(y))$$

Laat zien dat $(\mathbf{R}, R)$ wel een poset maar geen tralie is.

Opgave 9.11

Op $\mathbf{R} \times \mathbf{R}$ definiëren we de relatie K door

$$(m, n)K(r, s) \;\Leftrightarrow\; (m \leq r \wedge n \leq s).$$

Bewijs dat $(\mathbf{R} \times \mathbf{R}, K)$ een tralie is.

Opgave 9.12

Als R een relatie is op A, en B is een deelverzameling van A, dan *induceert* R een relatie R' op B door voor alle $x \in B$ en alle $y \in B$ te definiëren: $xR'y \Leftrightarrow xRy$.

Geef een bewijs of een tegenvoorbeeld voor elk van de volgende uitspraken:

a. Als R een equivalentierelatie op A is, dan is R' een equivalentierelatie op B.

b. Als (A, R) een poset is, dan is (B, R') een poset.

c. Als (A, R) een tralie is, dan is (B, R') een tralie.

d. Als R een totale ordening is op A, dan is R' een totale ordening op B.

Opgave 9.13

Zij (A, R) een tralie en $x, x', y, y' \in A$ met xRx' en yRy'. Bewijs dat

$$\inf(\{x, y\})\ R\ \inf(\{x', y'\}) \quad \text{en} \quad \sup(\{x, y\})\ R\ \sup(\{x', y'\}).$$

Opgave 9.14

Zij (A, R) een tralie. Bewijs dat

$$\sup\{x, \inf\{y, z\}\}\ R\ \inf\{\sup\{x, y\}, \sup\{x, z\}\}$$

voor alle elementen x, y, z van A.

Opgave 9.15

We bekijken de poset $(A, \leq)$, waarbij $A = \{x \in \mathbf{R} |\ 0 \leq x \leq 3\}$, en $\leq$ de gewone ordening van reële getallen is. De afbeelding $f : A \to A$ is gegeven door

$$\begin{array}{lcll} f(x) & = & (1 + x)/2 & \text{als } 0 \leq x < 2 \\ f(x) & = & (2 + x)/2 & \text{als } 2 \leq x \leq 3 \end{array}$$

a. Bewijs dat $\inf(B) = 1$ en $\sup(B) = 2$ voor de verzameling B gedefinieerd door $B = \{x \in A |\ 1 < x < 2\}$.

b. Bewijs dat f een monotone afbeelding is.

c. Bepaal de dekpunten van f.

d. De poset $(A, \leq)$ is een volledig tralie. Welk van de dekpunten van f wordt geconstrueerd in het bewijs van Stelling 9.9?

Opgave 9.16

Sorteer de volgende woorden over het alfabet $\{a, b, c, d\}$ volgens de ordening $\preceq^*$ waarbij $\preceq$ de totale ordening op $\{a, b, c, d\}$ is die voldoet aan $d \preceq b$, $b \preceq a$ en $a \preceq c$:

$$abcd, aa, cbddd, d, abc, dd, abcb, c.$$

Opgave 9.17

Bewijs Stelling 9.11.

Hoofdstuk 10

Oneindige verzamelingen

Voor twee eindige verzamelingen A en B kunnen er alleen bijectieve afbeeldingen van A naar B bestaan als $\#A = \#B$. Ook is het duidelijk dat er geen bijectieve afbeeldingen van A naar B kunnen zijn als de ene verzameling eindig veel elementen heeft en de andere oneindig veel. Maar hoe zit het als A en B beide oneindig veel elementen hebben? We zullen zien dat er dan heel vaak wel, maar vaak ook niet bijectieve afbeeldingen van A naar B bestaan. Gevoelsmatig kun je zeggen dat twee verzamelingen even groot zijn als er een bijectie tussen bestaat; voor eindige verzamelingen komt dit volgens voorgaande observaties precies overeen met de betekenis dat ze precies evenveel elementen bevatten. Om verwarring met minder precies dagelijks spraakgebruik te voorkomen zullen we in plaats van 'even groot' spreken over 'gelijkmachtig', maar het is wel aan te bevelen om het idee van 'even groot' daarbij in gedachten te houden.

Definitie 10.1 Twee verzameling A en B heten *gelijkmachtig* als er een bijectieve afbeelding van A naar B bestaat.
Een verzameling A heet *aftelbaar oneindig* als er een bijectieve afbeelding van $\mathbf{N}$ naar A bestaat.
Een verzameling A heet *aftelbaar* als A eindig is of aftelbaar oneindig.
Een verzameling A heet *overaftelbaar* als A niet aftelbaar is.

Omdat

- de identieke afbeelding een bijectie is,
- de inverse van een bijectie een bijectie is, en
- de samenstelling van twee bijecties een bijectie is,

zien we dat gelijkmachtigheid een *equivalentierelatie* op verzamelingen is.

We geven een paar voorbeelden van aftelbaar oneindige verzamelingen.

Neem voor A de verzameling van alle even natuurlijke getallen. Dan kunnen we een afbeelding $t : \mathbf{N} \to A$ definiëren door $t(x) = 2 * x$ te stellen voor alle $x \in \mathbf{N}$. Deze

afbeelding is bijectief want elk even getal is op precies één manier als 2-voud te schrijven. De verzameling A is dus een aftelbaar oneindige verzameling.

Aan dit voorbeeld zien we iets vreemds wat bij eindige verzamelingen niet kan optreden: we hebben twee gelijkmachtige verzamelingen waarvan er een een *echte deelverzameling* is van de ander: elk even natuurlijke getal is wel een natuurlijk getal, maar niet elk natuurlijk getal is even.

Beschouw $\mathbf{Z}$, de verzameling van alle gehele getallen. We gaan een bijectie van $\mathbf{N}$ naar $\mathbf{Z}$ maken door de natuurlijke om en om naar positieve en negatieve getallen te sturen:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 & \dots \end{pmatrix}$$

Dit kunnen we als volgt in een preciese definitie weergeven:

$$f(2n) = n \quad \text{voor alle } n \in \mathbf{N},$$

$$f(2n+1) = -n-1 \quad \text{voor alle } n \in \mathbf{N}.$$

Voor elke $y \in \mathbf{Z}$ is er precies één $x \in \mathbf{N}$ met $f(x) = y$, de afbeelding $f : \mathbf{N} \to \mathbf{Z}$ is dus bijectief. Hiermee is bewezen dat $\mathbf{Z}$ een aftelbaar oneindige verzameling is.

Iets ingewikkelder is het bewijs dat $\mathbf{N} \times \mathbf{N}$ een aftelbaar oneindige verzameling is. Dit kunnen we rechtstreeks doen door een manier aan te geven waarmee alle elementen van $\mathbf{N} \times \mathbf{N}$ worden afgeteld, en daarvan te bewijzen dat elk element van $\mathbf{N} \times \mathbf{N}$ precies één keer aan de beurt komt. Een mogelijke manier wordt aangegeven in het volgende plaatje

n								
	3	9	13	18	24			
	2	5	8	12	17	23		
	1	2	4	7	11	16	22	
	0	0	1	3	6	10	15	21
		0	1	2	3	4	5	6
								m

Deze afbeelding f voldoet aan $f((m,n)) = n + (m+n) * (m+n+1)/2$, waarbij m de horizontale en n de vertikale coördinaat is. Het is vrij lastig om met deze formule te bewijzen dat dit inderdaad een bijectie is; het is veel inzichtelijker om het algemene proces in een stelling te formuleren, en dat is wat we nu gaan doen. Het algemene proces is dat je de gewenste verzameling opsplitst in een oneindig aantal groepjes die zelf allemaal eindig zijn, in dit geval diagonale strookjes in het plaatje die van linksboven naar rechtsonder lopen. De gewenste nummering wordt gevonden door in het eerste strookje te beginnen met nummeren totdat alle elementen van dat eerste strookje genummerd zijn, dan verder te nummeren in het tweede strookje, tot ze daar allemaal aan de beurt zijn gekomen, dan het derde strookje, enzovoorts. Dit idee wordt in de volgende stelling verder uitgewerkt.

Stelling 10.2 Gegeven is een eindige verzameling A_i voor elke $i \in \mathbf{N}$. Dan is $A = \bigcup_{i=0}^{\infty} A_i$ een aftelbare verzameling.

Bewijs:

Als A eindig is zijn we klaar.

In het resterende geval is A oneindig; we gaan het gewenste resultaat bewijzen door een bijectieve afbeelding van $\mathbf{N}$ naar A te construeren.i

Om niet te verzanden in een brij van notatie geven we alleen het idee van deze constructie aan.

De eerste $\#A_0$ elementen van $\mathbf{N}$ worden bijectief op A_0 afgebeeld.

Vervolgens worden de volgende $\#(A_1 - A_0)$ elementen van $\mathbf{N}$ bijectief op $A_1 - A_0$ afgebeeld.

Dan worden de volgende $\#(A_2 - (A_0 \cup A_1))$ elementen van $\mathbf{N}$ bijectief op $A_2 - (A_0 \cup A_1)$ afgebeeld.

Dit proces zet zich voort: steeds worden de volgende k elementen van $\mathbf{N}$ bijectief op $A_j - (\bigcup_{i=0}^{j-1} A_i)$ afgebeeld, waarbij k het aantal elementen van $A_j - (\bigcup_{i=0}^{j-1} A_i)$ is, oftewel de elementen van A_j die nog niet eerder aan de beurt zijn geweest.

Omdat A oneindig is zet dit proces zich onbeperkt voort en wordt voor elke element van $\mathbf{N}$ uiteindelijk het beeld in A bepaald, zodanig dat elk element van A precies één keer aan de beurt komt.

Einde Bewijs.

Nu is het eenvoudig om te bewijzen dat $\mathbf{N} \times \mathbf{N}$ een aftelbaar oneindige verzameling is. Deze verzameling is namelijk te schrijven als $\bigcup_{i=0}^{\infty} A_i$ waarbij voor elke $i \in \mathbf{N}$ de eindige verzameling A_i gedefinieerd is door

$$A_i = \{(m, n) \in \mathbf{N} \times \mathbf{N} \mid m \leq i \wedge n \leq i\}.$$

Volgens Stelling 10.2 is nu $\mathbf{N} \times \mathbf{N}$ aftelbaar, en omdat hij oneindig is is hij aftelbaar oneindig.

We gaan nu laten zien dat $\mathbf{Q}$, de verzameling van rationale getallen, gedefinieerd door

$$\mathbf{Q} = \{\frac{p}{q} \mid p, q \in \mathbf{Z} \wedge q > 0\}$$

een aftelbaar oneindige verzameling is. Deze verzameling is namelijk te schrijven als $\bigcup_{i=0}^{\infty} A_i$ waarbij voor elke $i \in \mathbf{N}$ de eindige verzameling A_i gedefinieerd is door

$$A_i = \{\frac{p}{q} \mid p, q \in \mathbf{Z} \wedge -i \leq p \leq i \wedge 0 < q \leq i\}.$$

Volgens Stelling 10.2 is nu $\mathbf{Q}$ aftelbaar, en omdat hij oneindig is is hij aftelbaar oneindig.

De volgende stellingen geven een aantal algemene criteria voor aftelbaarheid.

Stelling 10.3 Als A aftelbaar is en $B \subseteq A$, dan is ook B aftelbaar.
Als A en B aftelbaar zijn, dan is ook $A \cup B$ aftelbaar.
Als A en B aftelbaar zijn, dan is ook $A \times B$ aftelbaar.

Bewijs:

Neem aan dat A aftelbaar is en $B \subseteq A$.

Omdat A aftelbaar is is er een bijectie $f : \mathbf{N} \to A$.

Definieer $B_i = \{b \in B \mid \exists k \langle k \leq i \wedge b = f(k) \rangle\}$.

Voor elk element b van B geldt $b \in A$; omdat f bijectief is er dan een $i \in \mathbf{N}$ met $b = f(i)$, dus ook $b \in B_i$.

Hieruit volgt dat $B = \bigcup_{i=0}^{\infty} B_i$; omdat B_i eindig is voor elke i concluderen we met Stelling 10.2 dat B aftelbaar is.

Hiermee is de eerste bewering van de stelling bewezen.

Neem nu aan dat A en B aftelbaar zijn.

Dan zijn er bijecties $f : \mathbf{N} \to A$ en $g : \mathbf{N} \to B$.

Definieer voor elke $i \in \mathbf{N}$ de eindige verzamelingen

$$C_i = \{f(i)\} \cup \{g(i)\}$$

en

$$D_i = \{(a, b) \in A \times B \mid \exists k, m \langle k \leq i \wedge a = f(k) \wedge m \leq i \wedge b = g(m) \rangle\}.$$

Dan is eenvoudig in te zien dat $A \cup B = \bigcup_{i=0}^{\infty} C_i$ en $A \times B = \bigcup_{i=0}^{\infty} D_i$.

Uit Stelling 10.2 volgt nu dat $A \cup B$ en $A \times B$ aftelbaar zijn.

Einde Bewijs.

In het vervolg noteren we weer de verzameling van eindige rijtjes elementen van een verzameling A als A^* en noemen we een element van A^* een *woord* over A. Het aantal (niet noodzakelijk verschillende) elementen in een woord w noemen we de *lengte* van w en noteren we met $\#w$.

Stelling 10.4 Gegeven is een niet-lege aftelbare verzameling A. Dan is de verzameling A^* van woorden over A aftelbaar oneindig.

Bewijs:

Als $a \in A$ dan zijn $a, aa, aaa, aaaa, \ldots$ oneindig veel elementen van A^*.

We moeten nog bewijzen dat A^* aftelbaar is. We maken daartoe onderscheid tussen A eindig of oneindig.

Stel A is eindig. Definieer voor elke $i \in \mathbf{N}$:

$$W_i = \{w \in A^* \mid \#w = i\}.$$

Omdat A eindig is is W_i dat ook voor elke i; vanwege $A^* = \bigcup_{i=0}^{\infty} W_i$ geldt volgens Stelling 10.2 dat A^* aftelbaar is.

In het resterende geval is A oneindig. Omdat A aftelbaar is is er een bijectie $f : \mathbf{N} \to A$.

Definieer $A_i = \{a \in A \mid f(a) \leq i\}$ voor elke $i \in \mathbf{N}$.

Dan is A_i eindig voor elke $i \in \mathbf{N}$.

Definieer voor elke $i \in \mathbf{N}$:

$$W_i = \{w \in A_i^* \mid \#w \leq i\}.$$

Dan is ook W_i eindig voor elke $i \in \mathbf{N}$.

Het is eenvoudig na te gaan dat $A^* = \bigcup_{i=0}^{\infty} W_i$.

Volgens Stelling 10.2 geldt ook in dit geval dat A^* aftelbaar is.

Einde Bewijs.

Met het combineren van deze stelling met Stelling 10.3 is van heel ingewikkelde verzamelingen zoals

$$(\mathbf{Q} \times \mathbf{Z}^* \cup \mathbf{N}^*)^*$$

direct in te zien dat ze aftelbaar zijn. Zo is ook de verzameling van alle mogelijke programma's in je favoriete programmeertaal een aftelbare verzameling, want elk programma is een (soms wel vrij lang) woord over een eindige verzameling symbolen. Het lijkt wel of alles aftelbaar is, maar dat is toch niet het geval. In de rest van dit hoofdstuk zullen we zien dat zowel de verzameling $\mathbf{R}$ van reële getallen en de verzameling $\mathcal{P}(\mathbf{N})$ van deelverzamelingen van de natuurlijke getallen overaftelbaar zijn, oftewel niet aftelbaar.

10.1 Het diagonaalargument

Stelling 10.5 Zij X een willekeurige verzameling. Dan is er geen surjectieve afbeelding van X naar $\mathcal{P}(X)$.

Bewijs:

Stel dat $f : X \to \mathcal{P}(X)$ een surjectieve afbeelding is.

Definieer $W = \{x \in X \mid x \notin f(x)\}$.

Dit is een element van $\mathcal{P}(X)$, omdat f surjectief is, is er een $y \in X$ zo dat $f(y) = W$.

We maken nu een gevalsonderscheid tussen $y \in W$ en $y \notin W$.

Stel $y \in W$, dan $y \notin f(y)$. Vanwege $f(y) = W$ geldt dan $y \notin W$, tegenspraak met de aanname.

Stel $y \notin W$, dan $\neg(y \notin f(y))$ oftewel $y \in f(y)$. Vanwege $f(y) = W$ geldt dan $y \in W$, tegenspraak met de aanname.

In beide gevallen hebben we een tegenspraak afgeleid, waarmee bewezen is dat er geen surjectieve afbeelding $f : X \to \mathcal{P}(X)$ is.

Einde Bewijs.

In het bijzonder hebben we nu bewezen dat er geen surjectieve afbeelding, dus zeker geen bijectieve afbeelding van $\mathbf{N}$ naar de oneindige verzameling $\mathcal{P}(\mathbf{N})$ bestaat, oftewel dat $\mathcal{P}(\mathbf{N})$ overaftelbaar is.

Het argument in Stelling 10.5 heet wel het *diagonaalargument*.

Stelling 10.6 De verzameling $\mathbf{R}$ van reële getallen is overaftelbaar.
Voor elke $x, y \in \mathbf{R}$ met $x < y$ is de verzameling

$$(x, y) = \{x \in \mathbf{R} \mid x < z < y\}$$

overaftelbaar

Bewijs:

Definieer

$$A = \{x \in \mathbf{R} \mid 0 \leq x < 1, \text{ en in de decimale ontwikkeling van } x \text{ komen alleen 0 en 1 voor}\}.$$

Voor $X \subseteq \mathbf{N}$ definiëren we het getal $f(X)$ beginnende met $0, \ldots$, en verder voor elke $i \in \mathbf{N}$ op de $i+1$-e positie na de komma een 1 als $i \in X$ en anders een 0.

Op deze wijze is elk element van A op precies één manier als $f(X)$ weer te geven, dit definieert een bijectie $f : \mathcal{P}(\mathbf{N}) \to A$.

Dan is de inverse $f^{-1} : A \to \mathcal{P}(\mathbf{N})$ ook een bijectie.

Stel dat $\mathbf{R}$ aftelbaar is, we gaan nu een tegenspraak afleiden.

Omdat $A \subseteq \mathbf{R}$ volgt uit Stelling 10.3 dat ook A aftelbaar is.

Dan is er een bijectie $g : \mathbf{N} \to A$.

Dan is de samenstelling $f^{-1} \circ g : \mathbf{N} \to \mathcal{P}(\mathbf{N})$ ook een bijectie.

Dit is in tegenspraak met Stelling 10.5, dus $\mathbf{R}$ is overaftelbaar.

Voor het tweede deel van de stelling merken we op dat voor x, y met $x < y$ de afbeelding $g : (x, y) \to \mathbf{R}$ gedefinieerd door

$$g(z) = \frac{1}{z - x} + \frac{1}{z - y}$$

een bijectieve afbeelding is; dit kan met standaardtechnieken uit de analyse worden bewezen.

Stel dat (x, y) aftelbaar is, dan is er een bijectie $h : \mathbf{N} \to (x, y)$.

Dan is ook $g \circ h : \mathbf{N} \to \mathbf{R}$ een bijectie.

Dan is $\mathbf{R}$ aftelbaar, in tegenspraak met wat we net hebben bewezen.

Einde Bewijs.

Om te bewijzen dat een bepaalde verzameling overaftelbaar is, is het meestal het handigst om te stellen dat hij aftelbaar is, en vervolgens met het toepassen van bekende bijecties en het toepassen van Stelling 10.3 af te leiden dat een bekende overaftelbare verzameling als $\mathbf{R}$ of (x, y) of $\mathcal{P}(\mathbf{N})$ ook aftelbaar is. Dit is dan een tegenspraak, waarmee bewezen is dat de oorspronkelijke verzameling overaftelbaar is.

Als voorbeeld hiervan bewijzen we dat de verzameling

$$A = \{x \in \mathbf{R} \mid 13 < 5x < 14 \wedge x \notin \mathbf{Q}\}$$

een overaftelbare verzameling is.

Stel A is aftelbaar. Omdat $\mathbf{Q}$ aftelbaar is, is dan volgens Stelling 10.3 ook $A \cup \mathbf{Q}$ aftelbaar. Een deelverzameling hiervan is

$$A' = \{x \in \mathbf{R} \mid 13 < 5x < 14\} = (\frac{13}{5}, \frac{14}{5}),$$

die dan volgens Stelling 10.3 ook aftelbaar is. Dit is in tegenspraak met Stelling 10.6. Dus is A overaftelbaar.

We hebben al eerder opgemerkt dat gelijkmachtigheid een equivalentierelatie op verzamelingen is. Een equivalentieklasse hiervan wordt een *kardinaalgetal* genoemd. Zo is de klasse van alle verzamelingen met precies drie elementen een kardinaalgetal, en is ook de klasse van alle aftelbare verzamelingen een kardinaalgetal. De kardinaalgetallen die horen bij de eindige verzamelingen corresponderen precies met de natuurlijke getallen, je zou dit bijna als definitie van de natuurlijke getallen op kunnen vatten. Als je er goed over nadenkt staat dit heel dicht bij de manier waarop kleine kinderen leren tellen: het getal drie slaat op iets waarvan je er drie exemplaren hebt, maar dan volledig geabstraheerd van alle eigenschappen van die exemplaren. In onze terminologie nemen we de verzameling van die drie exemplaren, en het nemen van de equivalentieklasse komt precies overeen met de abstractie van de eigenschappen van de elementen: als we drie andere exemplaren hadden genomen waren we toch op dezelfde equivalentieklasse uitgekomen omdat er een bijectie bestaat tussen de ene verzameling met drie elemtenten en de andere verzameling met drie elemtenten.

Het aardige van kardinaalgetallen is dat je je niet beperkt tot eindige verzamelingen, en op deze wijze ook op een nette manier oneindige getallen kunnen beschouwen. Het kleinste oneindige kardinaalgetal is $\aleph_0$: de klasse van alle aftelbare verzamelingen. Dit rare kriebeltje $\aleph$ heet *aleph* en is de eerste letter van het Hebreeuwse alfabet. Uit het feit dat er overaftelbare verzamelingen bestaan concluderen we dat er meer oneindige kardinaalgetallen bestaan dan alleen $\aleph_0$. Er zijn er zelfs oneindig veel: uit Stelling 10.5 concluderen we dat er

- geen bijectie bestaat van $\mathbf{N}$ naar $\mathcal{P}(\mathbf{N})$,
- geen bijectie bestaat van $\mathcal{P}(\mathbf{N})$ naar $\mathcal{P}(\mathcal{P}(\mathbf{N}))$,
- geen bijectie bestaat van $\mathcal{P}(\mathcal{P}(\mathbf{N}))$ naar $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbf{N})))$,
- $\cdots\cdots\cdots$,

dus zitten $\mathbf{N}$, $\mathcal{P}(\mathbf{N})$, $\mathcal{P}(\mathcal{P}(\mathbf{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbf{N})))$,... allemaal in verschillende kardinaalgetallen. Dit proces zet zich onbeperkt voort, en geeft aanleiding tot oneindig veel verschillende oneindige kardinaalgetallen.

10.2 Opgaven

Opgave 10.1

Maak een expliciete bijectie $f : \mathbf{N} \to \mathbf{N} - \{5\}$, d.w.z. definieer $f(n)$ voor elke $n \in \mathbf{N}$.

Opgave 10.2

Gegeven is een bijectie $f : \mathbf{N} \to X$, en een verzameling $Y = \{y_1, y_2, y_3\}$ zo dat $Y \cap X = \emptyset$. Maak een bijectie $g : \mathbf{N} \to X \cup Y$, gebruik makend van f.

Opgave 10.3

Laat X en Y disjuncte aftelbaar oneindige verzamelingen zijn. Veronderstel dat $f : \mathbf{N} \to X$ en $g : \mathbf{N} \to Y$ bijecties zijn. Construeer een bijectie $h : \mathbf{N} \to X \cup Y$ in termen van f en g.

Opgave 10.4

Bewijs dat de verzameling van alle afbeeldingen van $\mathbf{N}$ naar $\{0, 1\}$ overaftelbaar is.

Opgave 10.5

Bewijs dat de verzameling $\mathbf{R} - \mathbf{Q}$ overaftelbaar is.

Opgave 10.6

Bewijs dat de verzameling van eindige deelverzamelingen van $\mathbf{N}$ aftelbaar is. (Aanwijzing: pas Stelling 10.2 toe op

$$A_i = \{X \subseteq \mathbf{N} \mid \#X \leq i \wedge \forall x \in X \ \langle x \leq i \rangle\}.)$$

Hoofdstuk 11

Extra opgaven

Als extra oefening en ter oriëntatie op de toetsing geven we de midsemestertesten en de tentamens van vorige jaren. Deze bestonden elk uit vijf opgaven die alle even zwaar telden.

Midsemestertest 22 oktober 1997 met uitwerkingen

Opgave 11.1

Bewijs dat $(p \to q) \to ((p \wedge r) \to (q \wedge r))$ een tautologie is met behulp van een waarheidstafel.

Uitwerking:

p	q	r	$(p \to q)$	$\to$	$((p \wedge r)$	$\to$	$(q \wedge r))$
0	0	0	1	1	0	1	0
0	0	1	1	1	0	1	0
0	1	0	1	1	0	1	0
0	1	1	1	1	0	1	1
1	0	0	0	1	0	1	0
1	0	1	0	1	1	0	0
1	1	0	1	1	0	1	0
1	1	1	1	1	1	1	1

Aangezien in de kolom van het hoofdconnectief uitsluitend enen staan, is hiermee bewezen dat de gegeven propositie een tautologie is.

Opgave 11.2

Bewijs dat $(p \to q) \to ((p \wedge r) \to (q \wedge r))$ een tautologie is met behulp van deductie, modus ponens en de introductie- en eliminatie regel voor conjunctie.

Uitwerking:

te bew. $(p \to q) \to ((p \wedge r) \to (q \wedge r))$
Bewijs:

1 Stel $p \to q$
2 te bew. $(p \wedge r) \to (q \wedge r)$
Bewijs:
2.1 Stel $p \wedge r$
2.2 p (eliminatie $\wedge$, 2.1)
2.3 q (modus ponens, 2.2, 1)
2.4 r (eliminatie $\wedge$, 2.1)
2.5 $q \wedge r$ (introductie $\wedge$, 2.3, 2.4)
Einde bewijs 2 (deductie, 2.1, 2.5)
Einde bewijs (deductie, 1, 2)

Opgave 11.3

Bepaal een disjunctieve normaalvorm van $(p \wedge r) \to (q \wedge r)$.

Uitwerking:

$$\begin{array}{rcl}(p \wedge r) \to (q \wedge r) & \equiv & \neg(p \wedge r) \vee (q \wedge r) \\ & \equiv & ((\neg p) \vee (\neg r)) \vee (q \wedge r) \\ & \equiv & (\neg p) \vee (\neg r) \vee (q \wedge r).\end{array}$$

De uitdrukking $(\neg p) \vee (\neg r) \vee (q \wedge r)$ is een disjunctieve normaalvorm van $(p \wedge r) \to (q \wedge r)$.
Andere goede antwoorden zijn $(\neg p) \vee q \vee (\neg r)$, en

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r).$$

Opgave 11.4

Gebruik de notatie $K(x, y)$ voor: x is een kind van y. Schrijf in predicaat-logische notatie: x heeft precies één kind.

Uitwerking:

$$\exists y \langle K(y, x) \ \wedge \ \forall z \langle K(z, x) \to y = z \rangle \rangle.$$

Opgave 11.5

Laat A en B willekeurige verzamelingen zijn. Bewijs dat $A = A - (B - A)$.

Uitwerking:

$$\begin{array}{rcll}x \in A - (B - A) & \Leftrightarrow & x \in A \wedge \neg(x \in B - A) & \text{(definitie van } -) \\ & \Leftrightarrow & x \in A \wedge \neg(x \in B \wedge \neg(x \in A)) & \text{(definitie van } -) \\ & \Leftrightarrow & x \in A \wedge (\neg(x \in B) \vee \neg\neg(x \in A)) & \text{(wet van DeMorgan)} \\ & \Leftrightarrow & x \in A \wedge (\neg(x \in B) \vee x \in A) & \text{(dubbele ontkenning)} \\ & \Leftrightarrow & x \in A & (p \wedge (q \vee p) \leftrightarrow p \\ & & & \text{is een tautologie)}\end{array}$$

Uit $x \in A - (B - A) \Leftrightarrow x \in A$ volgt dat $A = A - (B - A)$.

Midsemestertest 23 oktober 1998 met uitwerkingen

Opgave 11.6

Bepaal een uitdrukking die opgebouwd is uit de atomen p, q, r, s en haakjes, en verder alleen maar de symbolen $\neg$ en $\vee$, en die equivalent is aan

$$(p \wedge q) \rightarrow (r \wedge s).$$

Uitwerking:

$$\begin{array}{lcll} (p \wedge q) \rightarrow (r \wedge s) & \equiv & \neg(p \wedge q) \vee (r \wedge s) & \text{(definitie } \rightarrow) \\ & \equiv & (\neg p \vee \neg q) \vee (r \wedge s) & \text{(DeMorgan)} \\ & \equiv & (\neg p \vee \neg q) \vee \neg\neg(r \wedge s) & \\ & \equiv & (\neg p \vee \neg q) \vee \neg(\neg r \vee \neg s) & \text{(DeMorgan)} \end{array}$$

Een mogelijk antwoord is dus $(\neg p \vee \neg q) \vee \neg(\neg r \vee \neg s)$.

Sommige mensen stelden een waarheidstafel op, bestaande uit 16 regels. Het is echter niet direct duidelijk hoe je van zo'n waarheidstafel een uitdrukking maakt die uitsluitend opgebouwd is uit $\neg$ en $\vee$. Toch waren er mensen die met deze omslachtige methode een goed antwoord vonden.

Opgave 11.7

Bewijs dat $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ een tautologie is met behulp van deductie en de overige afleidingsregels.

Uitwerking:

	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$		
	Bewijs:		
B1	Stel $(\neg q \wedge (p \rightarrow q))$		
B2	$\neg q$	(B1, eliminatie $\wedge$)	
B3	$p \rightarrow q$	(B1, eliminatie $\wedge$)	
B4	te bewijzen: $p \rightarrow$ FALSE		
	Bewijs van B4:		
B4.1	stel p		
B4.2	q	(B3, B4.1, modus ponens)	
B4.3	FALSE	(B2, B4.2, introductie false)	
	Einde bewijs B4 (deductie)		
B5	$\neg p$ (B4, contradictie)		
	Einde bewijs (deductie)		

Opgave 11.8

Gebruik de notatie

$K(x, y)$ voor: x is een kind van y,

$M(x)$ voor: x is mannelijk.

Schrijf in predicaat-logische notatie: de vader van z heeft een kleindochter.

Uitwerking:

$$\exists x, y, w \langle K(z,x) \wedge M(x) \wedge K(y,x) \wedge K(w,y) \wedge \neg M(w) \rangle$$

Hierin is x de vader van z, is y een kind van x (mogelijk z), en is w een dochter van y.

Een veel gemaakte fout was dat geëist werd dat w een dochter van z is. Dit hoeft niet het geval te zijn: als z geen dochter heeft, maar een broer of zus van z wel, dan heeft de vader x van z toch een kleindochter.

Verder waren er veel fouten in de quantificaties. De persoon z was in de opgave gegeven, en moet dus niet door een quantor worden gebonden.

Opgave 11.9

Bewijs dat $\neg(\forall x \langle P(x) \wedge Q(x) \rangle)$ equivalent is aan $\exists x \langle \neg Q(x) \rangle \vee \exists y \langle \neg P(y) \rangle$.

Uitwerking:

Toepassing van standaardregels geeft:

$$\begin{aligned} \neg(\forall x \langle P(x) \wedge Q(x) \rangle) &\equiv \exists \langle \neg(P(x) \wedge Q(x)) \rangle \\ &\equiv \exists \langle \neg P(x) \vee \neg Q(x) \rangle \\ &\equiv \exists \langle \neg Q(x) \vee \neg P(x) \rangle \\ &\equiv \exists x \langle \neg Q(x) \rangle \vee \exists x \langle \neg P(x) \rangle \\ &\equiv \exists x \langle \neg Q(x) \rangle \vee \exists y \langle \neg P(y) \rangle. \end{aligned}$$

Opgave 11.10

Laat A en B willekeurige verzamelingen zijn. Bewijs dat $\mathcal{P}(A - B) \subseteq \mathcal{P}(A)$.

Uitwerking:

Kies $X \in \mathcal{P}(A - B)$ willekeurig.
Dan $X \subseteq A - B$.
Vanwege $A - B \subseteq A$ en transitiviteit van inclusie geldt dan ook $X \subseteq A$.
Dan geldt $X \in \mathcal{P}(A)$.
Hiermee is bewezen dat $\mathcal{P}(A - B) \subseteq \mathcal{P}(A)$.

Oefententamen najaar 1997 met uitwerkingen

Opgave 11.11

Bewijs dat $((p \to q) \wedge (q \to r)) \to (p \to r))$ een tautologie is met behulp van deductie, modus ponens en de introductie- en eliminatie regel voor conjunctie.

Uitwerking:

te bew. $((p \to q) \wedge (q \to r)) \to (p \to r))$
Bewijs:
1 Stel $(p \to q) \wedge (q \to r)$
2 $p \to q$ (eliminatie $\wedge$, 1)

3 $q \to r$ (eliminatie $\wedge$, 1)
4 te bew. $p \to r$
Bewijs:
4.1 Stel p
4.2 q (modus ponens, 4.1, 2)
4.3 r (modus ponens, 4.2, 3)
Einde bewijs 4 (deductie, 4.1, 4.3)
Einde bewijs (deductie, 1, 4)

Opgave 11.12

Gebruik de notatie $K(x, y)$ voor: x is een kind van y. Schrijf in predicaat-logische notatie: een van de kinderen van x heeft een grootouder.

Uitwerking:

$$\exists y, z, w \langle K(y, x) \ \wedge \ K(y, z) \ \wedge \ K(z, w) \rangle.$$

Opgave 11.13

Laat A, B en C willekeurige verzamelingen zijn. Bewijs dat $(A - B) \cup C = (A \cup C) - ((A \cap B) - C)$.

Uitwerking:

Schrijf $p \equiv x \in A$, $q \equiv x \in B$ en $r \equiv x \in C$. Er geldt:

$$\begin{array}{lll}
x \in (A \cup C) - ((A \cap B) - C) & & \\
\quad \Leftrightarrow & x \in A \cup C \wedge \neg(x \in (A \cap B) - C) & \text{(definitie van } -) \\
\quad \Leftrightarrow & (x \in A \vee x \in C) \wedge \neg(x \in (A \cap B) - C) & \text{(definitie van } \cup) \\
\quad \Leftrightarrow & (p \vee r) \wedge \neg(x \in (A \cap B) - C) & \text{(definitie van } p, r) \\
\quad \Leftrightarrow & (p \vee r) \wedge \neg(x \in (A \cap B) \wedge \neg(x \in C)) & \text{(definitie van } -) \\
\quad \Leftrightarrow & (p \vee r) \wedge \neg(x \in (A \cap B) \wedge \neg r) & \text{(definitie van } r) \\
\quad \Leftrightarrow & (p \vee r) \wedge \neg((x \in A \wedge x \in B) \wedge \neg r) & \text{(definitie van } \cap) \\
\quad \Leftrightarrow & (p \vee r) \wedge \neg((p \wedge q) \wedge \neg r) & \text{(definitie van } p, q) \\
\quad \Leftrightarrow & (p \vee r) \wedge (\neg(p \wedge q) \vee \neg\neg r) & \text{(DeMorgan)} \\
\quad \Leftrightarrow & (p \vee r) \wedge ((\neg p \vee \neg q) \vee \neg\neg r) & \text{(DeMorgan)} \\
\quad \Leftrightarrow & (p \vee r) \wedge ((\neg p \vee \neg q) \vee r) & (\neg\neg r \equiv r) \\
\quad \Leftrightarrow & (p \wedge (\neg p \vee \neg q)) \vee r & \text{(distributiviteit)} \\
\quad \Leftrightarrow & ((p \wedge \neg p) \vee (p \wedge \neg q)) \vee r & \text{(distributiviteit)} \\
\quad \Leftrightarrow & (\text{FALSE} \vee (p \wedge \neg q)) \vee r & \\
\quad \Leftrightarrow & (p \wedge \neg q) \vee r & \\
\quad \Leftrightarrow & (x \in A \wedge \neg(x \in B)) \vee x \in C & \text{(definitie van } p, q, r) \\
\quad \Leftrightarrow & (x \in A - B) \vee x \in C & \text{(definitie van } -) \\
\quad \Leftrightarrow & x \in (A - B) \cup C & \text{(definitie van } \cup)
\end{array}$$

Hieruit volgt het gevraagde.

Bij het zoeken naar zo'n lange keten van equivalenties is het vaak handig om bij de ingewikkeldste kant te beginnen en vandaaruit naar de eenvoudigste kant toe proberen te werken.

Opgave 11.14

Gegeven zijn twee verzamelingen A en B, een afbeelding $f : A \to B$ en een partiële ordening R op B. Bewijs dat

$$S = \{(x, y) \in A \times A \mid f(x)Rf(y)\}$$

een partiële ordening op A is dan en slechts dan als f injectief is.

Uitwerking:

Stel eerst dat f injectief is.

Kies $x \in A$ willekeurig. Vanwege reflexiviteit van R geldt $f(x)Rf(x)$, en dus geldt $(x, x) \in S$, en dus xSx. Hiermee is bewezen dat S reflexief is.

Kies $x, y \in A$ willekeurig. Stel dat xSy en ySx. Dan geldt $f(x)Rf(y)$ en $f(y)Rf(x)$. Vanwege antisymmetrie van R geldt dan $f(x) = f(y)$. Vanwege de injectiviteit van f geldt dan $x = y$. Hiermee is bewezen dat S antisymmetrisch is.

Kies $x, y, z \in A$ willekeurig. Stel dat xSy en ySz. Dan geldt $f(x)Rf(y)$ en $f(y)Rf(z)$. Vanwege transitiviteit van R geldt dan $f(x)Rf(z)$. Hieruit volgt dat xSz. Hiermee is bewezen dat S transitief is.

Hiermee is bewezen dat S een partiële ordening is in het geval dat f injectief is.

Stel nu omgekeerd dat S een partiële ordening is. Kies $x, y \in A$ willekeurig. Stel dat $f(x) = f(y)$. Dan geldt vanwege de reflexiviteit van R dat $f(x)Rf(y)$ en $f(y)Rf(x)$. Hieruit volgt dat xSy en ySx. Vanwege antisymmetrie van S volgt hieruit dat $x = y$. Hiermee is bewezen dat f injectief is.

Hoe verzin je nou zo'n bewijs? Het bewijs dat iets een partiële ordening is bestaat per definitie uit het nagaan van reflexiviteit, antisymmetrie en transitiviteit. Het blijkt dat je de injectiviteit van f alleen gebruikt bij de antisymmetrie, daar hangt het dus blijkbaar op. Voor de omkering moet je injectiviteit van f bewijzen, dat betekent dat je een bewijs moet geven dat begint met "Stel dat $f(x) = f(y)$ën dat eindigt met "dan is $x = y$". Je weet ook dat je hierbij moet gebruiken dat S een partiële ordening is, in het bijzonder dat S antisymmetrisch is. Met deze beschouwingen ligt het gegeven bewijs voor de hand.

Opgave 11.15

Bewijs dat voor ieder natuurlijk getal n geldt $\displaystyle\sum_{k=0}^{n} 4k^3 = n^4 + 2n^3 + n^2$.

Uitwerking: We doen dit met volledige inductie naar n. Schrijf

$$P(n) \equiv \sum_{k=0}^{n} 4k^3 = n^4 + 2n^3 + n^2.$$

Vanwege $4 * 0^3 = 0 = 0^4 + 2 * 0^3 + 0^2$ geldt $P(0)$. Stel nu dat $P(n)$ geldt; met behulp daarvan gaan we $P(n + 1)$ bewijzen:

$$\begin{array}{lcll} \sum_{k=0}^{n+1} 4k^3 & = & (\sum_{k=0}^{n} 4k^3) + 4(n+1)^3 & \text{(definitie } \textstyle\sum\text{)} \\ & = & (n^4 + 2n^3 + n^2) + 4(n+1)^3 & \text{(de inductiehypothese } P(n)\text{)} \\ & = & n^4 + 6n^3 + 13n^2 + 12n + 4 & \text{(rekenen)} \\ & = & (n+1)^4 + 2(n+1)^3 + (n+1)^2 & \text{(rekenen)} \end{array}$$

Hiermee is $P(n+1)$ bewezen. Volgens het principe van volledige inductie is hiermee bewezen dat $P(n)$ voor ieder natuurlijk getal n geldt.

Tentamen 8 januari 1998

Opgave 11.16

Gebruik de notatie $K(x, y)$ voor 'x is een kind van y', en $M(x)$ voor 'x is mannelijk'. Schrijf in predicaat-logische notatie: 'x heeft een zus'.

Opgave 11.17

Laat A, B en C willekeurige verzamelingen zijn. Bewijs dat

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

(Alleen een Venn-diagram is niet voldoende.)

Opgave 11.18

Laat $f : X \to Y$ een afbeelding zijn. Laat B een deelverzameling van Y zijn en $y \in B$.

a. Geef een voorbeeld van dergelijke f, X, Y, y, B waarvoor $f^{-1}(B) = \emptyset$.

b. Bewijs dat $f^{-1}(B)$ niet de lege verzameling is als f surjectief is.

Opgave 11.19

Laat de relatie R op de natuurlijke getallen gedefinieerd zijn door

$$R = \{(x, y) \mid x + y \text{ is even en } x \leq y\}.$$

a. Bewijs dat R een partiële ordening is.

b. Bepaal alle minimale elementen en alle bovengrenzen met betrekking tot deze partiële ordening R van de verzameling $B = \{2, 4, 5, 6, 7, 8\}$.

Opgave 11.20

Bewijs dat voor ieder natuurlijk getal $n \geq 1$ geldt $\sum_{k=1}^{n}(4k - 3) = 2n^2 - n$.

Tentamen 8 april 1998

Opgave 11.21

Bepaal een disjunctieve normaalvorm van $(p \to q) \to (r \to p)$.

Opgave 11.22

Bewijs dat $((p \to q) \wedge (r \to s) \wedge p \wedge r) \to (q \wedge s))$ een tautologie is met behulp van deductie, modus ponens en de introductie- en eliminatie regel voor conjunctie.

Opgave 11.23

Laat de relatie R op de gehele getallen gedefinieerd zijn door

$$R = \{(x, y) \mid x^2 + x = y^2 + y\}.$$

a. Bewijs dat R een equivalentierelatie is.

b. Bepaal alle elementen van de equivalentieklasse van 1.

Opgave 11.24

Gegeven zijn drie verzamelingen A, B en C en twee injectieve afbeeldingen $f : A \to B$ en $g : B \to C$. Bewijs dat $g \circ f$ injectief is.

Opgave 11.25

Bewijs dat voor ieder natuurlijk getal $n \geq 1$ geldt $\sum_{k=1}^{n}(2k - 1) = n^2$.

Tentamen 5 januari 1999 met uitwerkingen

Aan dit tentamen hebben 130 personen deelgenomen, van wie er 98 een eindresultaat van een 6 of hoger hebben gehaald.

Opgave 11.26

Gebruik de notatie

- $K(x, y)$ voor 'x is een kind van y',
- $E(x, y)$ voor 'x en y zijn ex-klasgenoten', en
- $M(x)$ voor 'x is mannelijk'.

Schrijf in predicaat-logische notatie:

'de vader van a heeft vroeger samen met de moeder van b in de klas gezeten'.

Uitwerking:

$$\exists x, y \langle K(a, x) \wedge M(x) \wedge K(b, y) \wedge \neg M(y) \wedge E(x, y) \rangle.$$

Opmerking: de personen a en b zijn gegeven; de variabelen a en b moeten dus niet door een quantor worden gebonden.

Opgave 11.27

Laat A en B willekeurige verzamelingen zijn. Bewijs dat

$$B - (B \cap A) = B - A.$$

(Alleen een Venn-diagram is niet voldoende.)

Uitwerking:

Schrijf p voor $x \in A$, en q voor $x \in B$.

Voor een willekeurig element x geldt:

$$\begin{array}{lcll}
x \in B - (B \cap A) & \iff & x \in B \wedge \neg(x \in B \cap A) & \text{(definitie van } -) \\
& \iff & x \in B \wedge \neg(x \in B \wedge x \in A) & \text{(definitie van } \cap) \\
& \iff & q \wedge \neg(q \wedge p) & \text{(definitie van } p \text{ en } q) \\
& \iff & q \wedge (\neg q \vee \neg p) & \text{(DeMorgan)} \\
& \iff & (q \wedge \neg q) \vee (q \wedge \neg p) & \text{(distibutiviteit)} \\
& \iff & \text{FALSE} \vee (q \wedge \neg p) & \\
& \iff & q \wedge \neg p & \\
& \iff & x \in B \wedge \neg(x \in A) & \text{(definitie van } p \text{ en } q) \\
& \iff & x \in B - A & \text{(definitie van } -).
\end{array}$$

Vanwege $x \in B-(B\cap A) \iff x \in B-A$ kunnen we nu concluderen dat $B-(B\cap A) = B-A$.

Opgave 11.28

Gegeven zijn de getallen $b_0, b_1, b_2, \ldots$ die voldoen aan

$$b_0 = 1,$$

$$b_{n+1} = 3b_n + 2 \text{ voor elke } n \geq 0.$$

Bewijs dat voor ieder natuurlijk getal n geldt dat

$$b_n = 2 * 3^n - 1.$$

Uitwerking:

Schrijf $P(n)$ voor de bewering $b_n = 2 * 3^n - 1$. We gaan met volledige inductie naar n bewijzen dat $P(n)$ geldt voor elk natuurlijk getal n.

Basisstap:

Er geldt $b_0 = 1 = 2 * 3^0 - 1$, dus geldt $P(0)$.

Inductiestap:

We nemen aan dat $P(n)$ geldt voor zekere n (de inductiehypothese) en gaan nu bewijzen dat $P(n+1)$ geldt:

$$\begin{array}{lcll}
b_{n+1} & = & 3b_n + 2 & \text{(definitie van } b_{n+1}) \\
& = & 3(2 * 3^n - 1) + 2 & \text{(volgens de inductiehypothese } P(n)) \\
& = & 2 * 3 * 3^n - 3 + 2 & \text{(rekenen)} \\
& = & 2 * 3^{n+1} - 1 & \text{(rekenen)}.
\end{array}$$

Hiermee is $P(n+1)$ bewezen.

Volgens het principe van volledige inductie is nu bewezen dat $P(n)$ geldt voor elk natuurlijk getal n.

Opgave 11.29

Beschouw de relatie R op **N** gedefinieerd door

$$xRy \iff x + y < 10.$$

a. Is R reflexief?

b. Is R symmetrisch?

c. Is R anti-symmetrisch?

d. Is R transitief?

Bewijs voor elk van de vragen uw antwoord.

Uitwerking:

(a).

Kies $x = 6$, dan geldt niet $x + x < 10$, en dus ook niet xRx. Hieruit volgt dat R niet reflexief is.

(b).

Als xRy geldt, dan geldt $x + y < 10$. Vanwege $x + y = y + x$ (commutativiteit van de optelling) geldt dan ook $y + x < 10$, oftewel yRx. Hiermee is bewezen dat R symmetrisch is.

(c).

Kies $x = 2$ en $y = 3$, dan geldt $x + y < 10$ en $y + x < 10$, en dus xRy en yRx. Er geldt echter niet $x = y$; hieruit volgt dat R niet anti-symmetrisch is.

Opmerking: er zijn relaties die zowel symmetrisch als anti-symmetrisch zijn; uit het feit dat R symmetrisch is kan dus niet worden geconcludeerd dat R niet anti-symmetrisch is.

(d).

Kies $x = 6$ en $y = 2$ en $z = 7$, dan geldt $x + y < 10$ en $y + z < 10$, en dus xRy en yRx. Er geldt echter niet xRz omdat $x + z = 13 \geq 10$; hieruit volgt dat R niet transitief is.

Opgave 11.30

Beantwoord elk van de volgende vragen met 'ja' of 'nee' of een getal, zonder verder toelichting. De beoordeling voor deze opgave is het aantal goede min het aantal foute antwoorden. *Niet invullen is dus beter dan fout gokken.*

a. Geef de grootste ondergrens met betrekking tot de gewone ordening van de deelverzameling B van **Z**, gedefinieerd door

$$B \;=\; \{x \in \mathbf{Z} \mid x > 4 \wedge x \text{ is even}\}.$$

Antwoord: 6.

b. Hoeveel is $\sum_{i=1}^{200} i$?

Antwoord: 20100.

c. Laat $f : \mathbf{Z} \to \mathbf{Z}$ gedefinieerd zijn door $f(x) = x^2$ voor elke $x \in \mathbf{Z}$. Hoeveel elementen heeft $f^{-1}(\{-1, 0, 1, 2, 3, 4\})$?

Antwoord: 5.

d. Is de gerichte graaf op $\{1, 2, 3\}$ bestaande uit de kanten $(1, 2)$, $(2, 3)$ en $(3, 2)$ samenhangend?

Antwoord: nee.

e. Is de gerichte graaf op $\{1, 2, 3\}$ bestaande uit de kanten $(1, 2)$, $(2, 3)$ en $(3, 1)$ samenhangend?

Antwoord: ja.

f. Is $\mathbf{Z}$ met de gewone ordening een tralie?

Antwoord: ja.

g. Is $\mathbf{Z}$ met de gewone ordening een volledig tralie?

Antwoord: nee.

h. Is $\mathcal{P}(\{1, 2, 3, 4, 5\})$ aftelbaar?

Antwoord: ja.

i. Is $\mathbf{Z}$ aftelbaar?

Antwoord: ja.

j. Is $\mathcal{P}(\mathbf{Z})$ aftelbaar?

Antwoord: nee.

Tentamen 29 maart 1999 met uitwerkingen

Opgave 11.31

Bewijs dat

$$(p \to q) \to ((p \wedge r) \to (q \wedge r))$$

een tautologie is met behulp van deductie, modus ponens en de introductie- en eliminatie regel voor conjunctie.

Uitwerking:

te bew.	$(p \to q) \to ((p \wedge r) \to (q \wedge r))$	
	Bewijs:	
1	Stel $p \to q$	
2	te bew. $(p \wedge r) \to (q \wedge r)$	
	Bewijs:	
2.1	Stel $p \wedge r$	
2.2	p	(eliminatie $\wedge$, 2.1)
2.3	q	(modus ponens, 1, 2.2)
2.4	r	(eliminatie $\wedge$, 2.1)

2.5 $q \wedge r$ (introductie $\wedge$, 2.3, 2.4)
Einde bewijs 2 (deductie, 2.1, 2.5)
Einde bewijs (deductie, 1, 2)

Opgave 11.32

Bepaal een disjunctieve normaalvorm van $(r \wedge p) \rightarrow (q \wedge p)$.

Uitwerking:

$$(r \wedge p) \rightarrow (q \wedge p) \quad \equiv \quad \neg(r \wedge p) \vee (q \wedge p) \quad \equiv \quad (\neg r) \vee (\neg p) \vee (q \wedge p).$$

De laatste uitdrukking is een disjunctieve normaalvorm.

Opgave 11.33

Bewijs dat

$$\sum_{k=1}^{n} k * (k!) = (n+1)! - 1$$

voor elk positief natuurlijk getal n.

Uitwerking:

Schrijf $P(n)$ voor de bewering $\sum_{k=1}^{n} k * (k!) = (n+1)! - 1$. We gaan met volledige inductie naar n bewijzen dat $P(n)$ geldt voor elk positief natuurlijk getal n.

Basisstap:

Er geldt $\sum_{k=1}^{1} k * (k!) = 1 * (1!) = 1 = (1+1)! - 1$, dus geldt $P(1)$.

Inductiestap:

We nemen aan dat $P(n)$ geldt voor zekere n (de inductiehypothese)en gaan nu bewijzen dat $P(n+1)$ geldt:

$$\begin{array}{lcll} \sum_{k=1}^{n+1} k * (k!) & = & \sum_{k=1}^{n} k * (k!) + (n+1) * ((n+1)!) & (\text{definitie van } \textstyle\sum) \\ & = & (n+1)! - 1 + (n+1) * ((n+1)!) & (\text{volgens } P(n)) \\ & = & (n+2) * ((n+1)!) - 1 & (\text{rekenen}) \\ & = & ((n+1)+1)! - 1 & (\text{rekenen}). \end{array}$$

Hiermee is $P(n+1)$ bewezen.

Volgens het principe van volledige inductie is nu bewezen dat $P(n)$ geldt voor elk natuurlijk getal n.

Opgave 11.34

Gegeven is een verzameling A met een partiële ordening. Van $x, y, z \in A$ is gegeven dat x en y minimaal zijn in A en dat z een minimum is van A.

Bewijs dat $x = y$.

Uitwerking:

Omdat $x \in A$ en z een minimum is van A geldt $z \leq x$.
Omdat $z \leq x$ en x minimaal is in A geldt $z = x$.
Omdat $y \in A$ en z een minimum is van A geldt $z \leq y$.
Omdat $z \leq y$ en y minimaal is in A geldt $z = y$.
Omdat $z = x$ en $z = y$ geldt $x = y$.

Opgave 11.35

Beantwoord elk van de volgende vragen met 'ja' of 'nee' of een getal. De beoordeling voor deze opgave is het aantal goede min het aantal foute antwoorden.

Niet invullen is dus beter dan fout gokken.

Laat $f : \mathbf{Z} \to \mathbf{Z}$ gedefinieerd zijn door $f(x) = 3x$ voor elke $x \in \mathbf{Z}$.

a. Hoeveel elementen heeft

$f^{-1}(\{-4, -3, -2, -1, 0, 1, 2, 3, 4\})$?

Antwoord: 3

b. Is f surjectief?

Antwoord: nee

c. Is f injectief?

Antwoord: ja

d. Is de relatie $\neq$ op $\mathbf{N}$ transitief?

Antwoord: nee

e. Is de relatie $\neq$ op $\mathbf{N}$ symmetrisch?

Antwoord: ja

f. Is de relatie $\neq$ op $\mathbf{N}$ anti-symmetrisch?

Antwoord: nee

g. Is de relatie $\neq$ op $\mathbf{N}$ reflexief?

Antwoord: nee

h. Hoeveel niet-lege paden bestaan er in de gerichte graaf op $\{1, 2, 3, 4\}$ bestaande uit de kanten $(1, 4)$, $(2, 3)$ en $(4, 2)$?

Antwoord: 6

i. Hoeveel elementen heeft $\mathcal{P}(\{1, 2, 3, 4\})$?

Antwoord: 16

j. Is $\mathbf{Z} \times \mathbf{Z}$ aftelbaar?

Antwoord: ja

Index

n boven m, 104
n over m, 104

afbeelding, 75
afleidingsregels, 39
afleidingsregels voor predikaten, 53
aftelbaar, 145
aftelbaar oneindig, 145
aleph, 151
alfabet, 137
alfabetische ordening, 138
antisymmetrie, 125
antisymmetrisch, 125
arc, 111
argument, 76
associatief, 31, 63, 85, 110
atomaire propositie, 29
atomen, 29
axioma, 21, 25, 93

basisstap, 94
beeld, 76, 77
beperkt tot, 83
bereik, 39, 48, 76, 109
bestemmingstype, 76
bewijs, 21, 38
bewijs uit het ongerijmde, 11, 41
bijectie, 79
bijectief, 79
binaire notatie, 31
binomiaalcoëfficiënten, 104
binomium van Newton, 106
Boolse operatoren, 26
bovengrens, 129
brontype, 76

cartesisch product, 68
case analysis, 13
coördinaten, 68
codomain, 76
codomein, 76
commutatief, 31, 63, 85
complement, 62, 65
complete lattice, 134
complexe getallen, 60
component, 122
conclusie, 38
conjecture, 21
conjunctie, 26
conjunctieve normaalvorm, 36
connected, 113
connectieven, 26
contrapositie, 12, 31, 66
corollarium, 21
corollary, 21
counterexample, 12
cykel, 128

dag, 128
datacompressie, 79, 86
decompressie, 79, 86
decryptie, 86
deductie, 37, 40
deelbaar, 126
deelbaarheidsrelatie, 126
deelverzameling, 61
definitie, 21
dekpunt, 87, 135
delen met rest, 118
deler, 123, 126
DeMorgan, 31, 66
Descartes, 68
diagonaal, 73, 110
diagonaalargument, 150
directed acyclic graph, 128

disjunct, 62
disjunctie, 26
disjunctieve normaalvorm, 33
distribueert over, 31, 63
distributief, 31
domain, 75
domein, 75, 109
doorsnede, 61
driehoek van Pascal, 105
dualiteit, 130
duiventilprincipe, 11, 83
dummy, 48

echte deelverzameling, 61, 146
edge, 111
einde bewijs, 21
eindig, 46, 81
eindige rij, 101
eindige verzameling, 81
elegant bewijs, 136
eliminatie $\exists$, 54
eliminatie $\forall$, 53
eliminatie $\leftrightarrow$, 40
eliminatie $\rightarrow$, 40
eliminatie $\vee$, 40, 65
eliminatie $\wedge$, 40
eliminatie false, 40
eliminatie true, 40
encryptie, 79, 86
equationeel bewijs, 32
equivalent, 29
equivalentie, 26, 115
equivalentieklasse, 118
equivalentierelatie, 116, 145
esti-teken, 59
exhaustive, 14
existentiële quantor, 45
expressie, 52

factorial, 101
faculteit, 101
fibonaccigetallen, 102
fixed point, 87
functie, 75, 85
function, 75
functioneel programmeren, 85
functionele programmeertaal, 85

gcd, 133
gebonden, 46, 53
gebonden variabelen, 46
gehele getallen, 60
gelijk, 61, 76
gelijkmachtig, 145
gelijkwaardig, 29
geordende paren, 68
gerichte graaf, 111
gesloten uitdrukking, 48, 102
gevalsonderscheid, 13, 40, 41
gevolgd door, 110
ggd, 133
glb, 130
graaf, 111
grafiek, 110
greatest common divisor, 133
greatest lower bound, 129
grootste element, 129
grootste gemeenschappelijke deler, 133
grootste ondergrens, 129
gulden snede, 104

Hasse-diagram, 127
herbenoemen, 48, 52, 53
hulpstelling, 42

identieke afbeelding, 81
identiteit, 81, 110
image, 76, 77
implicatie, 26
inclusie, 61
inclusie-afbeelding, 81
indexverzameling, 70
induceert, 142
inductie, 93
inductiehypothese, 94
inductiestap, 94
inductieve definitie, 88, 101
inf, 130
infimum, 129
injectie, 78
injectief, 78
introductie $\exists$, 54
introductie $\forall$, 53

introductie $\leftrightarrow$, 40
introductie $\neg$, 40
introductie $\rightarrow$, 40
introductie $\vee$, 40
introductie $\wedge$, 40
introductie false, 40
introductie true, 40
invariant, 17, 95
inverse, 86, 87, 110
inverse image, 77

kant, 111
karakteristieke functie, 81
kardinaalgetal, 151
kgv, 133
kleinste bovengrens, 129
kleinste element, 129
kleinste gemeenschappelijke veelvoud, 133
knoop, 111

laatste stelling van Fermat, 21
lattice, 134
lcm, 133
least common multiple, 133
least upper bound, 129
leeg pad, 113
lege afbeelding, 81, 82
lege verzameling, 60
lemma, 21, 42
lengte, 148
lexicografische ordening, 137, 139
lineaire ordening, 126
literal, 33
lower bound, 129
lub, 130
lus, 121, 127

machtsverheffen, 68
machtsverzameling, 67, 68
majorant, 129
map, 75
matrixvoorstelling, 111
maximaal element, 129
maximum, 129
met terugleggen, 82
methode, 43
minimaal element, 129
minimum, 129
minorant, 129
modulo n, 117
modus ponens, 40
monotoon, 135

natuurlijke getallen, 60
negatie, 26
neutraal element, 32, 63, 84, 110
node, 111

ondergrens, 129
ongerichte graaf, 112, 121
onwaar, 24
opsommen, 59
ordening, 125
overaftelbaar, 145

pad, 113, 128
parameter, 86
partiële ordening, 125
partially ordered set, 125
partieel geordende verzameling, 125
partitie, 120
path, 113
permutatie, 82
pigeon hole principle, 11, 83
pijl, 111
pijlendiagram, 75, 110
poset, 125
power set, 67
predicaat, 46
prefix, 38
prefixnotatie, 49
prenex normaalvorm, 51
priemgetal, 96
principe van volledige inductie, 14, 93
procedure, 43
product, 68
proof, 21
proof by contradiction, 11
propositie, 21, 23
propositierekening, 32
proposition, 21

quantoren, 45
Quine dagger, 36

quod erat demonstrandum, 21

range, 76
rationale getallen, 60
reële getallen, 60
recursief, 101
recursieve definitie, 101
reflexief, 116, 125
relatie, 109
relatie op, 109
renaming, 48
rij, 101
rij van Fibonacci, 101

samenhangend, 113
samenhangscomponent, 122
samenstelling, 83, 110
scope, 39, 47, 48
scope-regels, 46
scope-regels voor referentie, 38
semantiek, 23, 28, 88
sequence, 101
Sheffer stroke, 34
sleutel, 79
sorteren, 137
source type, 76
stelling, 21, 55
sterke volledige inductie, 97
subbewijs, 38, 42
substitutie, 52
successor, 79
sup, 130
supremum, 129
surjectie, 79
surjectief, 78
symmetrisch, 112, 116
symmetrische verschil, 62, 66
syntax, 23, 28

target type, 76
tautologie, 29, 55
tegenvoorbeeld, 12
theorem, 21
torens van Hanoi, 98
totale ordening, 126
tralie, 134
transitief, 30, 64, 116, 125
type, 46, 53, 76, 85

uitputtend, 14
universele quantor, 45
universum, 46, 61, 62
upper bound, 129

variabelen, 46
Venn-diagram, 62
vereniging, 62
vermoeden, 21
veronderstelling, 38
verschil, 62
vertex, 111
verzameling, 59
verzameling van afbeeldingen, 82
volledig origineel, 77, 87
volledig tralie, 134
volledige inductie, 93
volledige inductie vanaf m, 97
vrij voorkomende, 48
vrije variabele, 46, 53

waar, 24
waarheidstafel, 26, 67
waarheidswaarde, 26
walk, 113
woord, 137, 148

zonder terugleggen, 82