TECHNISCHE HOGESCHOOL EINDHOVEN
Afdeling Algemene Wetenschappen
Onderafdeling der Wiskunde

INLEIDING LOGICA

door

Prof. Dr. N.G. de Bruijn

Tweede druk 1984

Technische Hogeschool Eindhoven

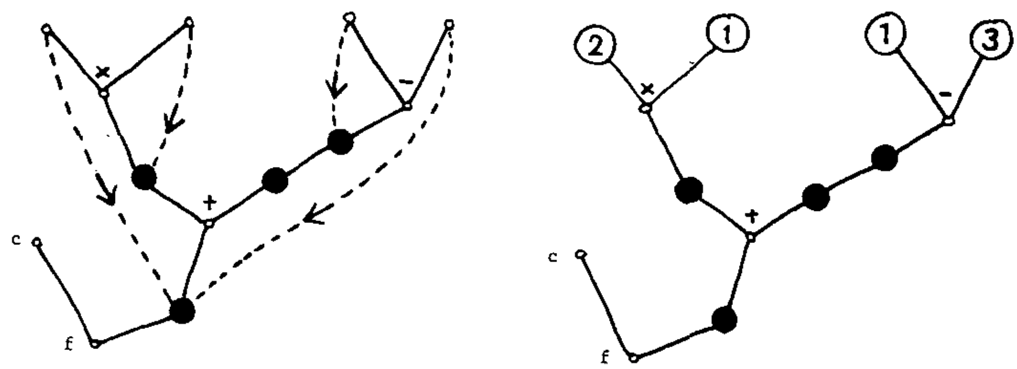
Dictaatnummer 2.307.1
Prijs f. 11,50

Onderafdeling der Wiskunde en Informatica

Syllabus en aanvullingen bij het college

Inleiding Logica

Tweede druk 1984



TECHNISCHE HOGESCHOOL EINDHOVEN

Onderafdeling der Wiskunde en Informatica

Syllabus behorende bij het college

INLEIDING LOGICA

door

Prof. dr. N.G. de Bruijn

Tweede druk 1984

Inhoudsopgave

HOOFDSTUK 1. SYNTACTISCHE AANGELEGENHEDEN

1.1. Wat is syntax?

In taalkunde maakt men onderscheid tussen syntax en semantiek. Syntax heeft betrekking op de vorm waarin woorden en zinnen gezegd worden, semantiek heeft betrekking op de betekenis. Wij zullen hier het woord syntax gebruiken wanneer het gaat over de manier waarop onze formules in elkaar zijn gezet. Met zegt bijv. dat 2 + 4 = 6 correct is, en 2 + 2 = 6 fout, maar dat 2++=++ = syntactisch niet deugt.

1.2. Symboolrijen

We zullen alle letters, cijfers en tekens symbolen noemen; een eindig rijtje van zulke symbolen heet een symboolrij. Een kleine complicatie treedt op als we te weinig symbolen tot onze beschikking hebben, en dan symbolen gaan maken die uit meer dan een letter of teken bestaan, zoals bijv. sin, log, lim. In dat geval zullen we speciale voorzieningen moeten treffen (bijv. door middel van spaties) om aan te geven waar het ene symbool ophoudt en waar het andere begint. Laten we daar voorlopig maar niet aan denken.

Vooorbeelden van symboolrijen zijn

b r 8 (#

& % + H f * a (

Als we de tweede rij achter de eerste plaatsen, vormen ze samen weer een symboolrij

b r 8 (# & % + H f * a (

en die symboolrij noemen we de concatenatie van de eerste symboolrij met de tweede.

We zullen bijzondere aandacht besteden aan de ronde haakjes uit een symboolrij. We nemen een rij, bijv.

```
     a  (  b * (  (  T  *)  +  (  (  p  )  ?  )
```

en we schrijven er gehele getallen onder op de volgende manier:

```
     a  (  b * (  (  T  *)  +  (  (  p  )  ?  )
  0     1      2  3      2     3  4     3     2
```

Het systeem is dat we links beginnen met een nul, het getal met 1 verhogen direct na een rond openingshaakje, en met 1 verlagen direct na een rond sluitingshaakje.

We zullen een symboolrij goedhaaks noemen wanneer bij dit nummeringssysteem alle geplaatste getallen positief zijn behalve de eerste en de laatste, die beide nul zijn.

De volgende symboolrijen zijn goedhaaks:

((* ( ) (+ a)) + (a # b))

((( ) (( )) ( ) ( )))

Wat nu volgt is geen goedhaakse symboolrij, maar wel is het de concatenatie van twee goedhaakse symboolrijen:

((a + B) * (g)) + (p - q)

Merk op dat het hier op twee manieren mogelijk is om de rij in twee goedhaakse te splitsen, nl. vóór resp. na het tweede plusteken.

1.3. Haakjesexpressies

Een haakjesexpressie is een symboolrij van een bepaalde soort. We zullen beschrijven hoe men de verzameling van alle haakjesexpressies stap voor stap produceert.

We gebruiken bij deze beschrijving het woord "letter". Daarmee wordt bedoeld ieder symbool dat geen rond haakje en geen komma is. In de praktijk zou zo'n symbool ook weer een rijtje letters (zoals sin of log) kunnen zijn.

(i) Een symboolrij die slechts uit een enkele letter bestaat is een haakjesexpressie.

(ii) Een letter gevolgd door een rond openingshaakje,gevolgd door een haakjesexpressie, gevolgd door een rond sluithaakje is weer een haakjesexpressie.

(iii) Als onder (ii), maar nu tussen de twee genoemde haakjes niet een enkele haakjesexpressie, maar een serie van twee of meer dergelijke expressies, gescheiden door komma's.

Voorbeelden van haakjesexpressies zijn

f

x

f(x)

f(y,x,p)

g(f(a,b,c),h(e))

f(g(p),h(u,k(u,H(i,j))),x)

Gemakkelijk ziet men dat alle haakjesexpressies goedhaaks zijn. De losse letters (onder (i) genoemd) zijn goedhaaks, en als men een stelletje goedhaakse symboolrijen concateneert, eventueel gescheiden door komma's, en in zijn geheel tussen haakjes plaatst, is het resultaat weer goedhaaks. Het symbool dat uiteindelijk helemaal vooraan geplaatst wordt zal de goedhaaksheid niet storen.

De voorste f in

f(g(p),h(u,k(u,H(i,j))),x)

heet de kop van de expressie, en de haakjesexpressies die er samen tussen haakjes achter staan, heten de subexpressies van deze f. Het zijn

g(p)

h(u,k(u,H(i,j)))

x

Ook kan men sub-subexpressies aanwijzen. En men kan bijv. zeggen dat H(i,j) de tweede subexpressie van de k is.

Zoals bij (i) werd uitgedrukt, is ook een losse letter een haakjes-expressie. Die is dan zijn eigen kop, en het aantal subexpressies is nul.

We zullen nu gaan veronderstellen dat er bij elke letter een niet-negatief geheel getal behoort dat aangeeft hoeveel subexpressies die letter in een haakjesexpressie behoort te hebben. Dat betekent dat dingen als

f(x,f(a,b),y)

voortaan verboden zijn, want hier heeft de f de ene keer twee en de andere keer drie subexpressies.

Als het aantal subexpressies van een letter 1,2 of 3 is, heet die letter resp. <u>unair</u>, <u>binair</u>, <u>ternair</u>. Uitgaande van deze terminologie zullen we het aantal subexpressies dat een letter dient te hebben de "<u>airiteit</u>" van die letter noemen.

Een letter waarvan de airiteit positief is zullen we een <u>operator</u> noemen. Letters met airiteit nul heten soms <u>constanten</u>, soms <u>variabelen</u>.

We kiezen nu een stelletje letters met daarbij airiteiten om ze in voorbeelden te kunnen gebruiken.

a	b	x	y	f	p	W	V
0	0	0	0	2	2	2	3

Een toegelaten haakjesexpressie is bijv.

V(x,f(y,W(a,b)),p(x,f(a,b))) (1)

Het grappige is nu dat men de haakjes en komma's rustig weg kan laten, dus kan schrijven

V x f y W a b p x f a b (2)

omdat men in staat is de weggelaten haakjes en komma's weer terug te vinden. We zullen dit even gaan bestuderen. Laat ons zo'n symboolrij die uit een toegelaten haakjesexpressie ontstaat door weglating van de haakjes en komma's even een "code" noemen. Als we een stuk van de code hebben ingelezen zijn we al in staat geweest een stuk van de haakjesexpressie te schrijven. Bovendien weten we wat ons nog te wachten staat. We noteren dat bijv. met "H)),H)" als we bedoelen dat we nog te schrijven hebben: een haakjesexpressie, twee sluithaakjes, een komma, een haakjesexpressie en een sluithaakje.

We passen het volgende schema toe, waarin de koppen boven de kolommen het volgende betekenen. "Verwacht" betekent wat we nog zullen moeten gaan schrijven, waarbij het symbool H staat voor "haakjesexpressie". "Lees" duidt op het volgende symbool van de in te lezen code, en "airit" slaat op de airiteit van dat symbool. "Schrijf" is wat we vervolgens als bijdrage aan de te bepalen haakjesexpressie gaan opschrijven. De kolommen "schrap" en "voeg toe" slaan op het aan de voorkant wijzigen van wat er in de kolom "verwacht" staat. Het schema geeft alle mogelijkheden aan, waarbij we ons wat airiteit betreft, echter hebben beperkt tot de gevallen 0, 1, 3.

verwacht	lees	airit.	schrijf	schrap	voeg toe
, ...			,	,	
) ...			)	)	
H ...	x	0	x	H	
H ...	f	1	f(	H	H)
H ...	W	3	W(	H	H,H,H)

Als we de in het bovenstaande schema uitgedrukte werkwijze toepassen op de code (2), komt het volgende voor de dag.

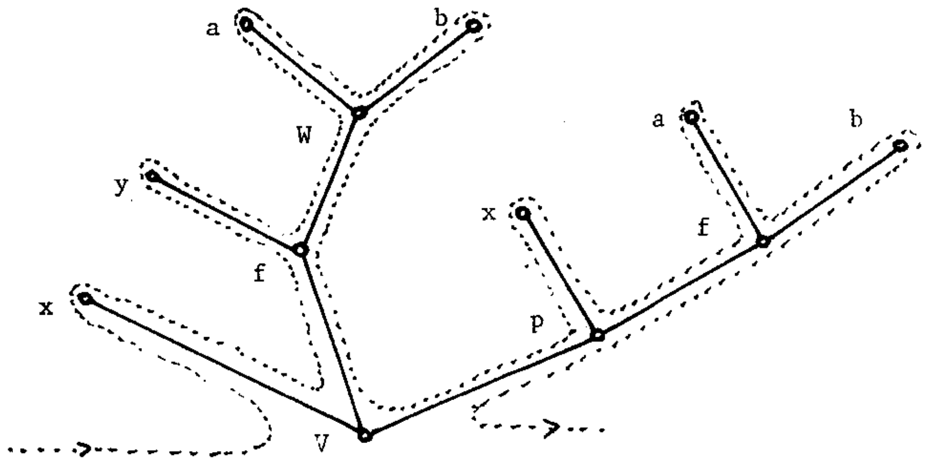
verwacht	lees	airit.	schrijf	schrap	voeg toe
H	V	3	V(	H	H,H,H)
H,H,H)	x	0	x	H	
,H,H)			,	,	
H,H)	f	2	f(	H	H,H)
H,H),H)	y	0	y	H	
,H),H)			,	,	
H),H)	W	2	W(	H	H,H)
H,H)),H)	a	0	a	H	
,H)),H)			,	,	
H)),H)	b	0	b	H	
)),H)			)),	)),	
H)	p	2	p(	H	H,H)
H,H))	x	0	x	H	
,H))			,	,	
H))	f	2	f(	H	H,H)
H,H)))	a	0	a	H	
,H)))			,	,	
H)))	b	0	b	H	
)))			)))	)))	

Het feit dat in elke stap van de gevolgde algoritme de desbetreffende opdracht uitvoerbaar is, en het feit dat aan het einde van het proces de kolom "verwacht" leeg is geraakt, garandeert dat de ingelezen symboolrij inderdaad een code is geweest.

Men kan een soortgelijk algoritme opzetten om na te gaan of een gegeven symboolrij met gegeven airiteiten inderdaad een haakjesexpressie is die voldoet aan de eis dat elke letter evenveel subexpressies heeft als zijn airiteit bedraagt.

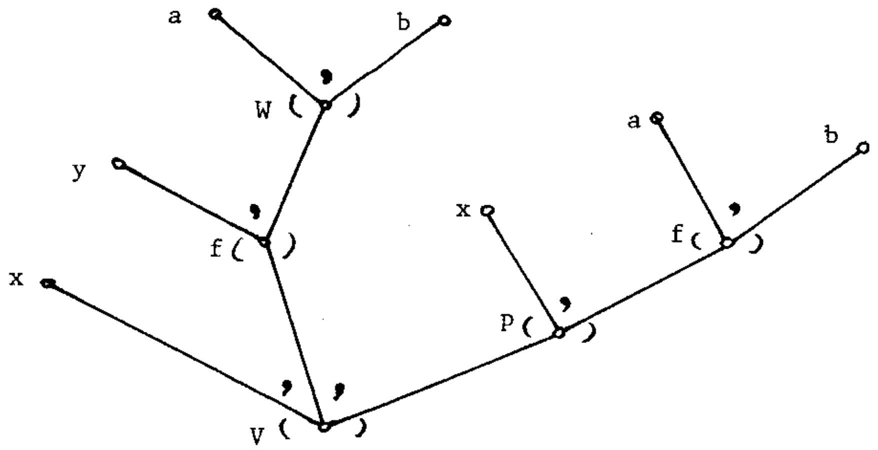
1.4. Haakjesexpressies voorstellen door bomen

We kunnen elke haakjesexpressie tekenen als een boom. De kop van de haakjesexpressie is het onderste punt van de boom, en van daaruit gaan evenveel takken omhoog als de airiteit van die kop bedraagt. Aan de uiteinden van die opgaande takken komen dan de bomen die met de subexpressies corresponderen. De bij de expressie (1) behorende boomfiguur spreekt min of meer voor zichzelf (zie figuur 1). De uiteinden (toppen) van de boom dragen de letters met airiteit 0.



Figuur 1. De boom van de haakjesexpressie (1).

We zetten bij elk punt van de boom de bijbehorende letter aan de linkerkant. Als we de boom aflopen zoals een van links komende slak dat zou doen, en zoals aangegeven door een stippellijn in figuur 1, en als we alle tegengekomen letters noteren, dan lezen we precies de code (2) af. Als we echter eerst haakjes plaatsen om alle knooppunten, en komma's in de oksels, zoals in figuur 2 is gebeurd, leest de slak precies de oorspronkelijke haakjesexpressie (1).

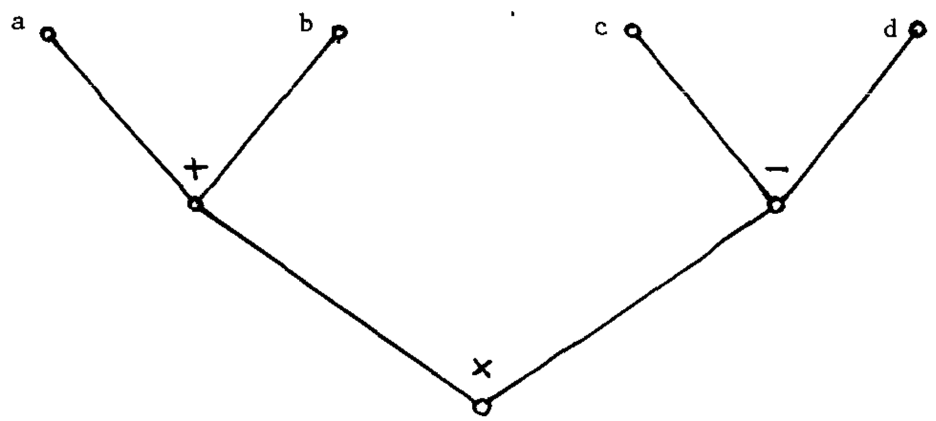


Figuur 2. De boom van figuur 1, voorzien van haakjes en komma's.

1.5. Expressies met infixsymbolen

In vele takken van de wiskunde worden boomvormige formules met z.g. infixnotaties aangegeven. Zo wordt bijv. de som van a en b niet met iets als "som(a,b)" maar met "a+b" aangeduid. De eerstgenoemde, waar de operatornaam voorop staat, en die tot de bouw van haakjesexpressies leidt, wordt prefixnotatie genoemd, de laatste infix. Voor de prefixnotatie zou het eigenlijk niet nodig zijn een ander symbool dan + te gebruiken: met zou ook "+(a,b)" kunnen schrijven.

Eigenlijk doet de keuze van notatie er niet veel toe, want wat we met een samengestelde formule bedoelen wordt keurig door een boom aangegeven, zoals bijv. figuur 3 voorstelt wat in gebruikelijke notatie met (a+b) × (c−d) wordt aangegeven.

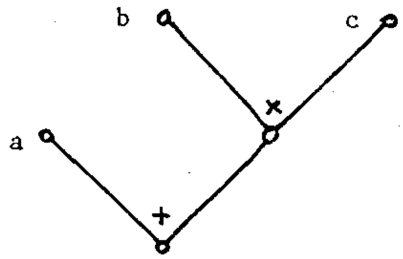


Figuur 3. De boom van $(a+b) \times (c-d)$.

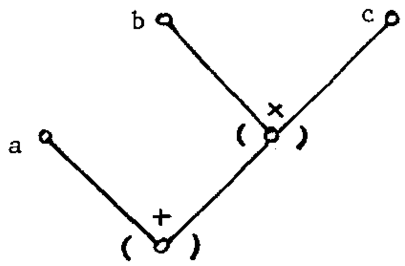
We vermelden nog enkele bekende infixnotaties: $a > b$, $a = b$, a / b uit de rekenkunde, $a \wedge b$, $a \vee b$, $a \rightarrow b$, uit de logica, en $a \cap b$, $a \cup b$, $a \in b$, $a \subset b$ uit de verzamelingenleer.

Infixnotaties missen het (overigens betrekkelijke) voordeel dat ze zonder haakjes geschreven kunnen worden (zoals we voor haakjesexpressies een haakjesloze code fabriceerden). Toch kan men ook bij infixnotatie flink op haakjes bezuinigen, en wel op grond van prioriteitsregels.

We willen afspreken dat $\times$ sterker bindt dan $+$, waarmee we bedoelen dat in een uitdrukking als $a + b \times c$ eerst het product van b en c moet worden genomen en dat dan pas de optelling aan de beurt komt. Het gaat bij deze kwestie niet over het eerst moeten uitrekenen van dat product, maar alleen over de manier van opvatting. Met $a + b \times c$ is bedoeld wat er in figuur 4 staat.



Figuur 4. De boom van $a + b \times c$.



Figuur 5. Idem met haakjes.

Als we om de knopen haakjes zetten krijgen we wat in figuur 5 staat, wat in slakkegang leidt tot $(a + (b \times c))$.

We gaan nu verordineren dat "$\times$ sterker bindt dan +". Daaraan ontlenen we het recht om in de situaties van figuur 6 de haakjes om het

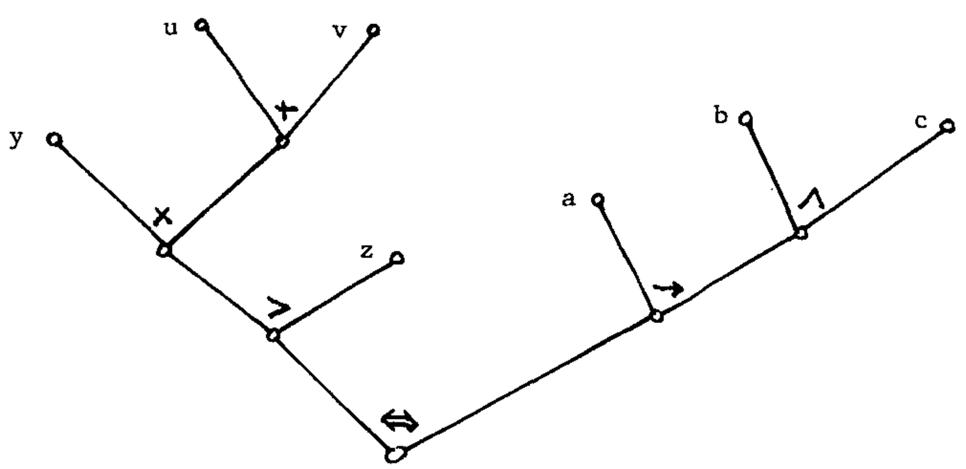
Figuur 6. Situaties waarbij de haakjes om het sterkst bindende teken weggelaten mogen worden.

maalteken weg te laten. Algemeen: we laten haakjes weg om een operatieknoop als er een operatie onder hangt die zwakker bindt.

Men staat vaak toe de haakjes bij unaire knopen weg te laten; misverstand kan dat niet geven.

Tenslotte merken we op dat het buitenste haakjespaar om een formule kan worden weggelaten: men schrijft $a - (b - c)$ in plaats van $(a - (b - c))$.

Een samengesteld voorbeeld: × bindt sterker dan +, × sterker dan >, ∧ sterker dan →, en al deze operatoren binden sterker dan ⇔. De boom uit figuur 7 heeft nog maar op één plaats haakjes nodig, nl. om het plusteken. Nadat die haakjes zijn geplaatst leest de slak wat er onder de figuur staat aangegeven.



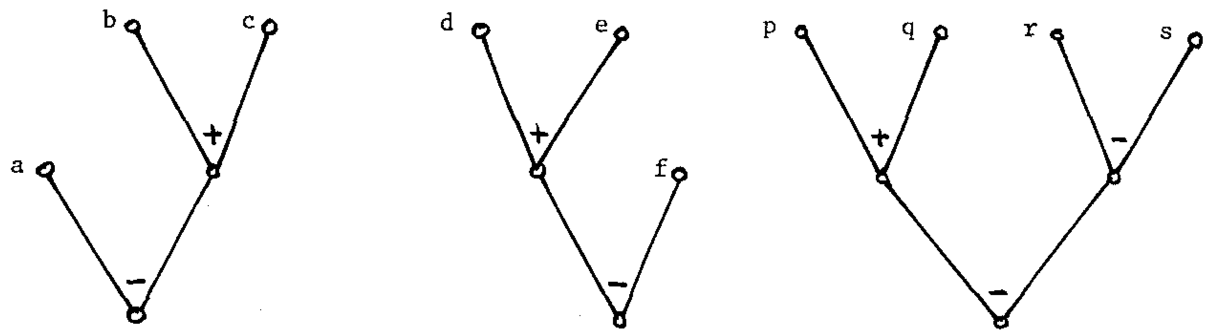
<u>Figuur 7. $y \times (u+v) > z \Leftrightarrow a \rightarrow b \wedge c$</u>

In het algemeen zullen we binnen een wiskundevak een z.g. <u>hiërarchie</u> maken. We werken met een aantal niveau's, en op elk niveau zetten we een stel operatoren, bijv.

×	/	
+	−	
>	<	=
∧	∨	
→		
⇔		

Hoe hoger het niveau, hoe sterker de binding. We spreken verder af dat als bijv. & en $ operatoren zijn van hetzelfde niveau, we in de linker boom van figuur 8 de haakjes om de & weg mogen laten, maar in de rechter boom niet. Zo kunnen de drie boompjes uit figuur 9 door de eronder geplaatste formules worden beschreven, tenminste wanneer + en - hetzelfde niveau in de hiërarchie wordt gegeven.

Figuur 8. Haakjes om & mogen links wel, rechts niet worden weggelaten



Figuur 9. Bomen voor a - (b + c), d + e - f, p + q - (r - s)

Onze afspraak over het weglaten van haakjes bij unaire operatoren komt er eigenlijk op neer dat we de unaire operatoren de hoogste prioriteit geven.

Als we omgekeerd uitgaan van een formule waarin een aantal haakjes zijn weggelaten, zoals

$$(x - (a + b)) - p\ q\ c \times d + s \times p\ e\ /\ (f - h),$$

(waarin p en q unaire operatoren zijn) dan gaan we als volgt te werk. We beschouwen de goedhaakse stukken elk als één geheel, en we korten ze af tot een enkele letter. Dan komt er

$$u - p\ q\ c \times d + s \times p\ e\ /\ v\ .$$

Van de tekens $-$, $\times$, $+$, $/$ stellen we het laagst voorkomende niveau vast, dat is hier het niveau van $+$ en $-$. Vervolgens kijken we wanneer er in de formule voor het laatst een teken van dat niveau optreedt. Dat teken gaat met de wortel van de boom corresponderen, want we splitsen

$$(u - p\ q\ c \times d) + (s \times p\ e\ /\ v).$$

Nadat dit gebeurd is gaan we met de afzonderlijke stukken verder. Tenslotte vervangen we p q c door p(q(c)) en p c door p(c).
Dit leidt tot

$$(u - (p(q(c)) \times d)) + ((s \times p(e))\ /\ v).$$

Los van deze notatieafspraken staat dat sommige operatoren associatief zijn. Zo zijn (a + b) + c en a + (b + c) aan elkaar gelijk, althans in de algebra. Dan kan worden uitgedrukt door

$$a + b + c = a + (b + c).$$

Onze afspraak komt erop neer dat met a + b + c is bedoeld (a + b) + c. Dit wordt de linksassociatieve opvatting genoemd.

In sommige algebraïsche systemen waarin zulke associatieve wetten gelden mogen dus wel meer haakjes worden weggelaten dan in het algemeen het geval is. Maar dat is een geheel andere kwestie dan het weglaten op grond van prioriteitsregels.

We vestigen er terloops even de aandacht op dat, wanneer met afgeronde getallen gewerkt wordt, die associatieve wetten voor optelling en vermenigvuldiging niet meer algemeen gelden.

1.6. Opmerkingen

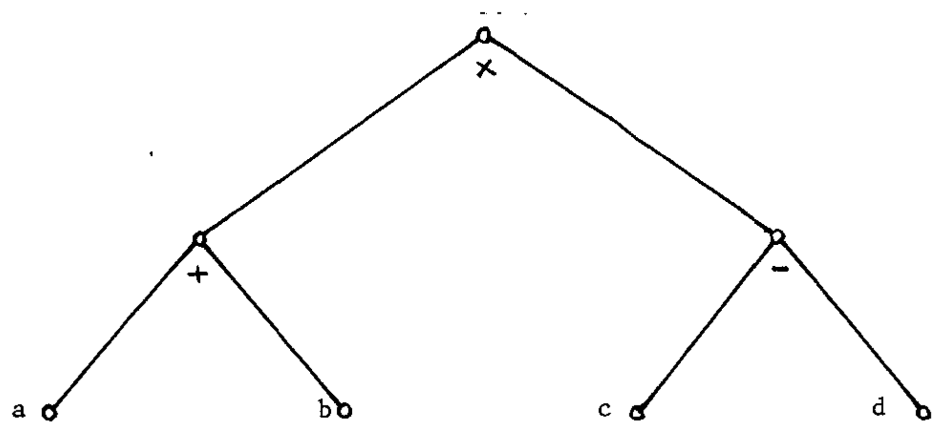
1. Formules als a < x < b vallen buiten onze beschouwing. Het is "doorschrift" voor (a < x) ∧ (x < b).
2. Pas op met het minteken. Het wordt niet alleen als binaire maar ook als unaire operator gebruikt. Bedenk dat -5 = 0 - 5.
3. Heel vervelend is voor ons dat de wiskundige praktijk sommige infixsymbolen gewoon weglaat. Het bekendst is de gewoonte om het gewone product van a en b door a b aan te geven. Wanneer we formules willen bespreken op de manier die we in het voorafgaande hebben gevolgd, zullen we deze wat al te korte notatie eerst door een andere moeten vervangen.
4. De notatie (2) voor formule (1) (vgl. ook figuur 1) wordt de Poolse notatie genoemd. (Łukasiewicz). Zeer bekend is ook de omgekeerd Poolse notatie("reverse Polish"). Die krijgt men als men de operatoren postfix noteert (dus (x,y)f i.p.v. f(x,y)),wat erop neerkomt dat men in figuur 2 de operatoren rechts van de knopen schrijft. Als dan weer de slak van links naar rechts loopt komt er

x y a b W f x a b f p V.

Deze omgekeerd Poolse notatie wordt veel gebruikt in gevallen waar de operaties moeten worden "uitgevoerd" (bijv. door een computer). Men vormt een "stapel" en leest de omgekeerd Poolse notatie van links naar rechts. Men begint met lege stapel. Komt men een letter met airiteit 0 tegen, dan wordt die boven op de stapel geplaatst. Leest men een operator met bijv. airiteit 3, dan wordt die operator op de bovenste drie elementen van de stapel toegepast, die drie worden weggenomen en het resultaat van de operatie wordt weer boven op de stapel geplaatst. Heeft men de gehele formule afgewerkt, dan blijkt de stapel nog maar één ding te bevatten, en dat is het eindresultaat.

1.7. Treurwilgen

Velen hebben de gewoonte bomen te tekenen met de wortel bovenaan en de takken afhangend naar beneden. De boom van figuur 3 wordt dan getekend als in figuur 10. Figuur 10 ontstaat uit figuur 3 door boven en onder te verwisselen. Wat links was blijft links, wat rechts was blijft rechts.



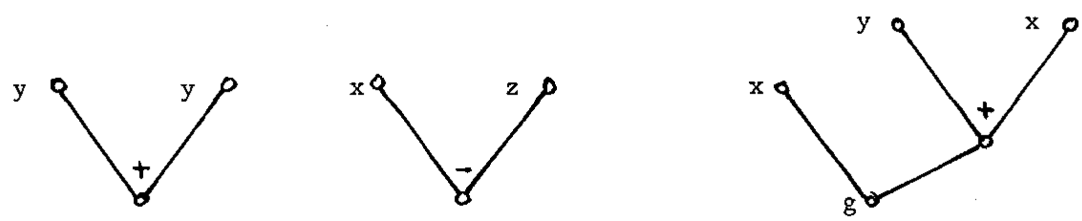
Figuur 10. De treurwilg van $(a+b) \times (c-d)$.

1.8. Substitutie

We verklaren het begrip substitutie aan boomvormige formules waarbij we ons dus om haakjes niet hoeven te bekommeren. Wanneer we substitutie bedrijven in haakjesformules met prefix- of infixnotatie kunnen we het best eerst in gedachten naar de boom teruggaan, daar de substitutie uitvoeren, en daarna kijken waar de haakjes moeten komen.

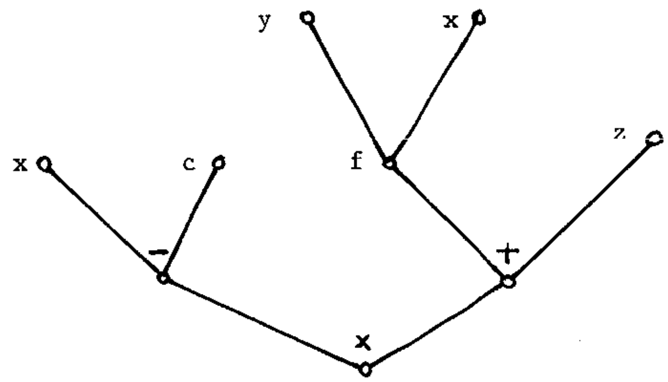
We wijzen een aantal letters met airiteit nul aan, die we met de naam variabelen zullen aanduiden. Laat ons nemen x,y,z. Deze variabelen mogen dus alleen bij toppen van de boom staan, en niet bij knopen.

We hebben te maken met wat er gesubstitueerd wordt en met waarin er gesubstitueerd wordt. Wat er gesubstitueerd wordt, beschrijven we door bij elk der letters x, y, z een boom aan te geven. Deze bomen, die we even kortaf aanduiden met $\varphi(x)$, $\varphi(y)$, $\varphi(z)$ (zie voorbeeld in figuur 11), mogen zelf de letters x, y en z weer bevatten, en het komt juist daardoor dat substitutie vaak verkeerd wordt gedaan.



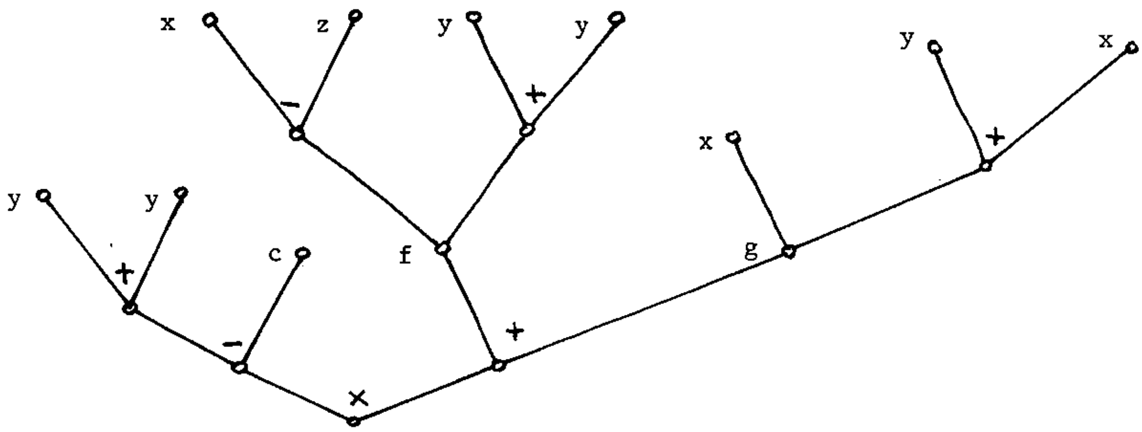
Figuur 11. De bomen $\varphi(x)$, $\varphi(y)$, $\varphi(z)$.

We passen de substitutie uit figuur 11 toe op de boom van figuur 12 (we zeggen ook wel: we voeren de substitutie uit in de boom van figuur 12). Elke x in figuur 12 wordt vervangen door de eerste boom uit figuur 11,



Figuur 12. De boom waarin de substitutie wordt uitgevoerd.

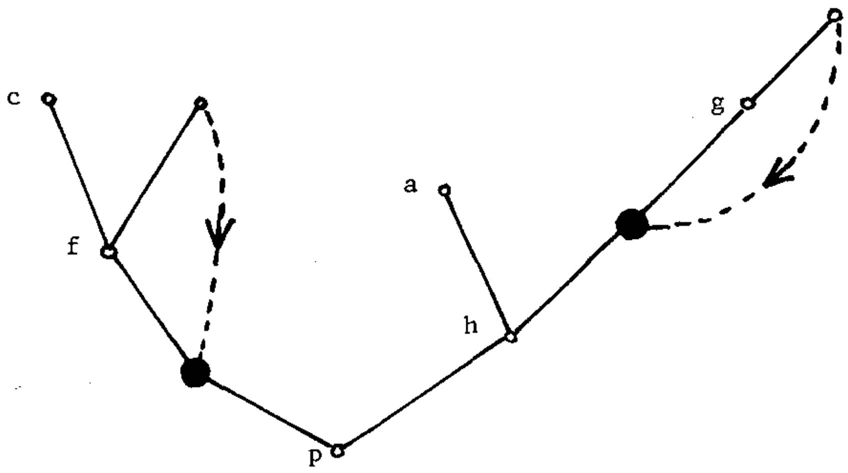
elke y uit figuur 12 door de tweede, elke z door de derde. We zeggen nadrukkelijk dat elke y uit figuur 12 wordt vervangen, en niet elke y uit de boom die ontstaan is nadat de x'en door de bijbehorende boompjes zijn vervangen. Dat maakt nogal wat verschil, want die boompjes kunnen ook y's bevatten. Het resultaat van de substitutie staat in figuur 13 aangegeven.



Figuur 13. Het resultaat van de substitutie.

1.9. Gebonden variabelen

We gaan nu kijken naar boomvormige formules waarin een soort punten voorkomt dat we tot nu toe niet hebben gezien. Het zijn punten die lijken op wat men ziet bij operaties met airiteit 1, maar die een geheel ander doel dienen. We geven ze voorlopig met een dikke punt aan, en we noemen ze binders. Bovendien zijn er in deze nieuwe bomen stippellijnen getrokken van sommige eindpunten naar binders, en er staan geen namen meer bij de betreffende eindpunten. In figuur 14 zijn wat van die stippellijnen getekend, van pijlen voorzien.

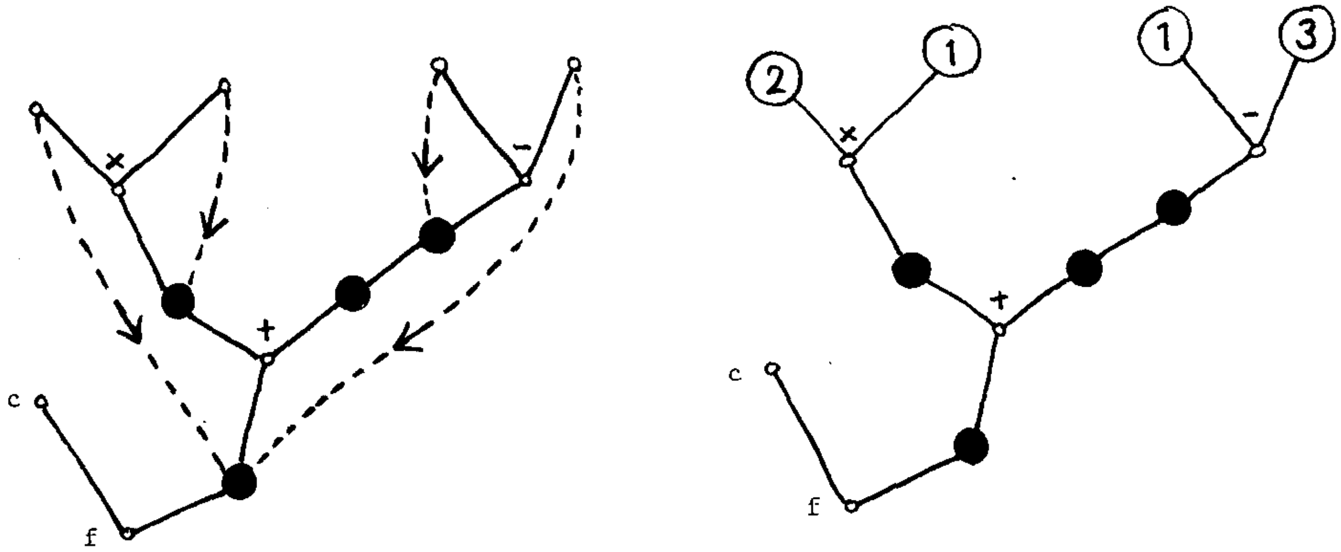


Figuur 14. Een boom met referentiepijlen van toppen naar binders.

Er is een belangrijke beperking: de pijlen mogen alleen lopen van een top naar een binder die men tegenkomt langs de kortste weg van die top naar de wortel. Desnoods is die wortel zelf een binder.

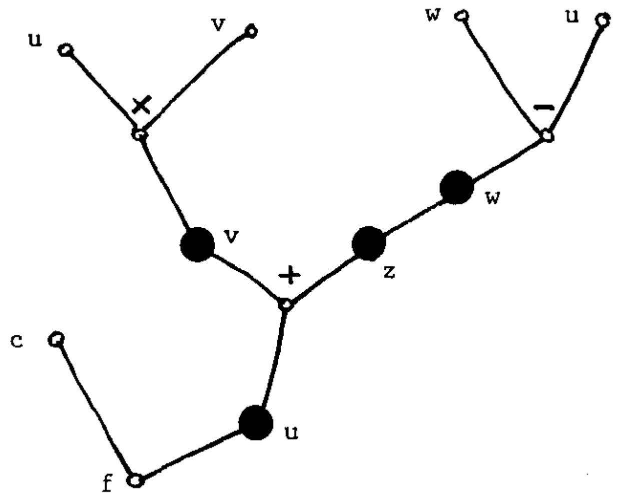
Alle andere punten van de boom worden behandeld als vroeger: als een punt geen top met stippelpijl en ook geen binder is, staat er een symbool bij, hetzij infix, hetzij prefix.

Een middel om het tekenen van stippellijnen te vermijden is het aangeven van referentiediepte. Als bij een eindpunt bijv. 2 in een cirkeltje staat, dan geeft dat aan dat de pijl naar de tweede binder moet lopen die men tegenkomt op de kortste weg naar de wortel. In figuur 15 is twee keer eenzelfde boom met binders getekend, de eerste keer met referentiepijlen, de tweede keer met referentiediepten.



Figuur 15. Bindingen aangegeven door pijlen resp. referentiediepten.

De wiskundige praktijk werkt niet met bomen maar met formules die volgens het een of andere systeem tot symboolrij zijn gemaakt. Stippelpijlen en referentiediepten zouden daarbij erg onhandig zijn. Men gebruikt in plaats daarvan z.g. gebonden variabelen. Bij iedere binder kiest men een letter die niet voorkomt in de figuur en niet in de tekst waarbinnen de figuur optreedt. De letters bij verschillende binders verschillen onderling. Deze letters heten gebonden variabelen. In figuur 16 geven we met gebonden variabelen aan wat in figuur 15 op twee manieren werd gedaan. Het is duidelijk dat men de pijlen of referentiediepten onmiddellijk kan terugvinden.

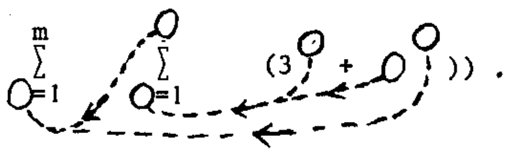


Figuur 16. De boom van figuur 15, nu met gebonden variabelen.

Voorlopig kunnen we nog geen goede voorbeelden uit de wiskundige praktijk geven, doordat die praktijk daar niet goed genoeg voor is! Maar we kunnen denken aan formules als

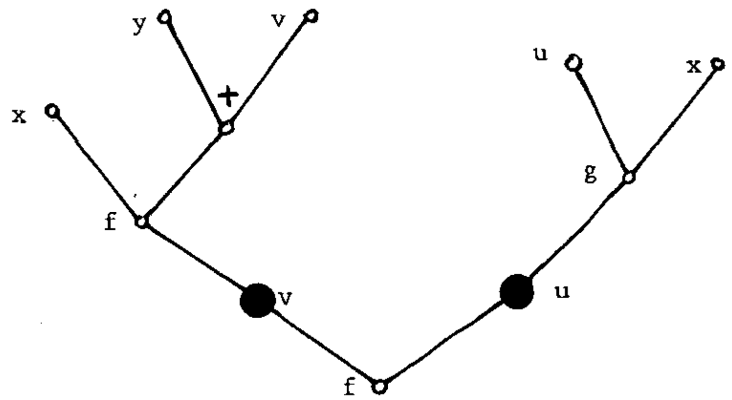
$$\sum_{n=1}^{m} \left(\sum_{k=1}^{n} (3^k + k^n) \right)$$

waarin n en k gebonden variabelen zijn. Met pijlen kan men nu iets maken als



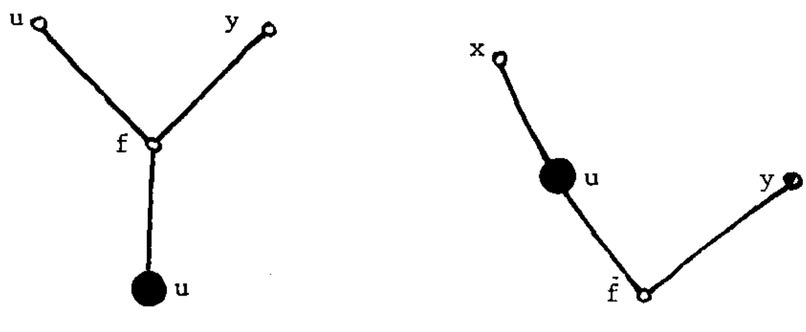
1.10. Substitutie bij formules met bindingen

Formules met bindingen kunnen naast een aantal gebonden variabelen (die op de beginpunten van de stippellijnen staan, of daar geschreven kunnen worden) ook nog andere variabelen bevatten, die we vrije variabelen zullen noemen. Ze zijn in de beschouwde formule niet gebonden (hoewel we de mogelijkheid openlaten dat de hele formule later deel wordt van een grotere formule waarin die variabelen wel worden gebonden).



Figuur 17. Formule met bindingen en vrije variabelen.

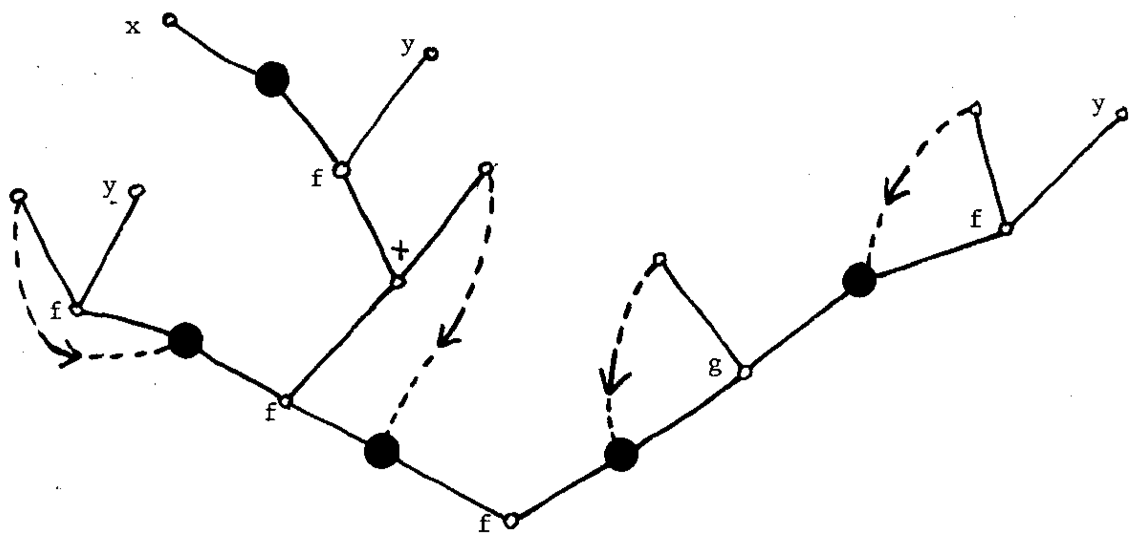
In figuur 17 is zo'n formule getekend, met als vrije variabelen x en y. We gaan nu in deze formule een substitutie φ uitvoeren, die in figuur 18 is beschreven, evenals in figuur 11 een substitutie beschreven was.



Figuur 18. De bomen φ(x) en φ(y).

De substitutie van figuur 18 is lastiger, doordat er ook weer bindingen in staan, en zelfs de x en y weer voorkomen. Bij uitvoering van dergelijke substituties kunnen we nogal eens in moeilijkheden komen doordat eenzelfde naam als naam van verschillende gebonden variabelen zou kunnen gaan optreden. Het zou zelfs kunnen gebeuren dat gebonden variabelen in de te substitueren formules dezelfde naam dragen als vrije of gebonden variabelen in de formule waarin gesubstitueerd wordt. Dan is Leiden in last.

We maken daarom de volgende veilige afspraak voor de uitvoering van de substitutie. We tekenen alle betrokken formules eerst in de vorm met referentiestippellijnen, zoals in de linkertekening van figuur 15. Daarna vervangen we elke x in de boom van figuur 17 door de zo aangepaste $\varphi(x)$ en elke y door de zo aangepaste $\varphi(y)$. Daardoor ontstaat de boom van figuur 19.



Figuur 19. Het resultaat van de substitutie.

Wanneer we zulks willen, kunnen we figuur 19 natuurlijk weer vervangen door een boom waarin de gebonden variabelen namen hebben en de pijlen zijn weggelaten. We doen dat door bij elk in de figuur voorkomend bindingspunt een eigen variabele te kiezen. Deze moeten onderling verschillen, maar ook verschillen van alle in de figuur reeds voorkomende vrije variabelen en constanten.

HOOFDSTUK 2. PROPOSITIELOGICA

2.1. Inleiding

Logica is het vak waarin men zich wijdt aan de studie van het redeneren. Zo'n studie kan op vele manieren worden begonnen, en juist de eerste opzet is een groot probleem. En als het erom gaat aan beginnelingen iets duidelijk te maken is er de moeilijkheid dat die een periode van gewenning nodig hebben om zich te schikken in zaken die de kenner heel gewoon vindt. Onderwijskundig is er veel voor een tweerondensysteem te zeggen: een eerste informele ronde ter gewenning, en een tweede waarin de dingen eens echt goed uit de doeken gedaan worden.

Meestal begint een inleiding over logica met een poging om uit te leggen wat "uitspraken", of met een ander woord, "proposities" zijn. Dit doet men door wat voorbeelden te geven uit het dagelijks leven, of door iets vaags te zeggen als "een propositie is een mededeling die hetzij waar, hetzij onwaar is". Terwijl men juist zou verwachten dat de logica gaat verklaren wat de woorden "waar" en "onwaar" betekenen.

Voorbeelden uit het dagelijks leven zijn doorgaans niet erg gelukkig. Ze hebben bijv. het nadeel dat ze zinswendingen bevatten die lijken op zinswendingen die men ten bate van de wiskunde wil bestuderen, maar daarmee niet goed vergelijkbaar zijn. Een mededeling als "als het morgen regent neem ik mijn paraplu mee" lijkt taalkundig wel op "als de hoeken aan de basis gelijk zijn, zijn de opstaande zijden gelijk", maar de betekenis van het "als . . . . dan" ligt in de eerste zin heel anders dan in de tweede.

Maar ook als we voorbeelden uit de wiskunde kiezen, is er iets niet eerlijk. We gaan dan uit van zinnen die ons in de wiskunde vertrouwd zijn. Dat heeft het voordeel dat we allerlei lastige zaken, zoals het voorkomen van variabelen in zinnen, betrekkelijk gemakkelijk voor ons zien. Maar dan vergeten we te lichtvaardig dat het de taak van de logica is om te verklaren hoe zulke zinnen moeten worden gebouwd.

Toch zou het ons heel moeilijk vallen om als een soort droogzwemles de logica te bedrijven: alles van de grond opbouwen voordat er een idee ontstaat waar het toe leidt, of "waar het eigenlijk over gaat", is noch voor de docent, noch voor de student een werkbare methode. We zullen dus op grote schaal moeten zondigen tegen de principes die we als heilig beschouwen, om iets van die principes te kunnen begrijpen. Het enige wat we voorlopig er tegen zouden kunnen doen is om het er steeds bij te zeggen als we eigenlijk aan het knoeien zijn.

Misschien is het wel een illusie te menen dat alles echt van de grond af tot ieders tevredenheid zou kunnen worden opgebouwd. Het is niet duidelijk, en niet voor iedereen hetzelfde, wat "de grond" is, en wat voor soort opbouwmethodiek van dat punt af mag worden gevolgd.

2.2. Operationele beschrijving

In hoofdzaak zullen we de voorkeur geven aan een "operationele" beschrijving. Dat komt erop neer dat we vertellen hoe we met een logisch systeem omgaan, en niet wat de "betekenis" ervan is. We sluiten ons hierdoor aan bij de bekende woorden van Wittgenstein: "Don't ask for the meaning, ask for the use".

2.3. Natuurlijke deductie

We zullen voor de opbouw van de logica een systeem volgen dat heel nauw aansluit bij de structuur van redeneringen, zodat onderwijs in logica enig inzicht kan verschaffen in wat bewijzen zijn. Dat systeem heet "natuurlijke deductie". Het systeem heeft onder andere het voordeel dat de behandeling van de predicatenlogica zo goed aansluit bij die van de propositielogica.

Een geheel andere opzet is die van de waarheidstafels, die zich althans voor de propositielogica nog altijd in een zekere populariteit verheugen. We zullen ons er wel mee bezig houden, maar pas nadat de natuurlijke deductie afgehandeld is (Hoofdstuk 4).

2.4. Proposities

We willen niet beginnen met een serieuze opbouw van het begrip propositie. Een echte opbouw zou voor de beginner moeilijk verteerbaar zijn, doordat het zo lang zou duren voordat duidelijk wordt waar het allemaal om draait. We zullen ons gedragen alsof we het begrip propositie al hebben, en beginnen met wat voorbeelden. In deze voorbeelden stellen de letters x, p en b reële getallen voor.

(1)	$x > p$
(2)	$x + 1 > x$
(3)	$2 > 1$
(4)	$2 < 1$
(5)	$3x + 2 = 8$
(6)	als $b > 0$ dan is $2b > b$
(7)	als $b > 0$ dan is
(8)	$x + 2$
(9)	$- x + + -$

Hier zijn (1), (2), (3), (4), (5), (6) proposities, (7), (8), (9) zijn het niet. Daarvan stelt (8) althans nog iets voor, nl. een reëel getal. Aan (7) en (9) wordt helemaal geen betekenis toegekend.

De proposities (2), (3) en (6) zijn "waar", (4) is "onwaar". Van (1) en (5) kunnen we zoiets niet zeggen zonder meer van x en p resp. van x af te weten.

2.5. Nieuwe proposities opbouwen uit oude

We hebben niet gezegd hoe proposities gevormd kunnen worden, maar we zullen hier een paar dingen van algemene aard vaststellen, nl. verschillende eenvoudige manieren waarop nieuwe proposities uit oude kunnen worden gevormd.

a. Ontkenning. Van elke propositie kunnen we de "ontkenning" vormen. Uit "x is groter dan p" vormen we "x is niet groter dan p". We noteren de ontkenning in het algemeen ~~door~~ voorplaatsen van het teken $\neg$, eventueel met nog wat haakjes erbij om ongelukken te voorkomen. Dus

$$\neg(x+1 > x), \qquad \neg(2 > 1), \qquad \neg(3x + 2 = 8).$$

Men zou kunnen opmerken dat de ontkenning van een ware propositie een onware is, en omgekeerd. Maar voorlopig zullen we ons met waarheid niet bezig houden.

b. Conjunctie. Uit twee proposities kunnen we door z.g. conjunctie een nieuwe vormen: Uit "x is groter dan p" en "2 > 1" vormen we

(x is groter dan p) en (2 > 1).

In plaats van "en" gebruiken we het teken $\wedge$. Zo schrijven we

$$(x > p) \wedge (2 > 1).$$

Het gaat alleen over het feit dat deze conjuncties proposities zijn, niet over de vraag of ze waar, dan wel onwaar zijn.

c. Disjunctie. Uit twee proposities kunnen we door z.g. disjunctie een nieuwe vormen: Uit "x is groter dan p" en "2 > 1" vormen we

(x is groter dan p) of (2 > 1).

In plaats van "of" gebruiken we ook het teken $\vee$. Zo schrijven we

$$(x > p) \vee (2 > 1).$$

Het gaat weer alleen over het feit dat deze disjuncties proposities zijn, niet over de vraag of ze waar, dan wel onwaar zijn.

d. Implicatie. Uit twee proposities kunnen we ook door z.g. implicatie een nieuwe vormen: Uit "x is groter dan p" en "2 > 1" vormen we

als (x is groter dan p) dan is (2 > 1).

In plaats van "als ... dan" gebruiken we ook het teken $\rightarrow$. Zo schrijven we

$$(x > p) \rightarrow (2 > 1).$$

Het gaat weer alleen over het feit dat deze implicaties proposities zijn, niet over de vraag of ze waar dan wel onwaar zijn. De kwestie van de waarheid ligt hier trouwens wat lastiger dan bij de vorige rubrieken.

Opmerking. De symbolen $\neg$, $\wedge$, $\vee$, $\rightarrow$ heten connectieven.
Syntactisch gezien is $\neg$ een unaire prefixoperator, en de drie andere zijn binair en infix.

Ten aanzien van die infixsymbolen spreken we als prioriteitsregel af dat $\wedge$ en $\vee$ even sterk binden, en dat beide sterker binden dan $\rightarrow$. Zo is bijv. $a \wedge b \rightarrow c \wedge d \vee e$ te interpreteren als $(a \wedge b) \rightarrow ((c \wedge d) \vee e)$.

Zoals in 1.5 werd gezegd mogen we de haakjes om de subexpressie van een unaire operator weglaten. We schrijven dus $\neg a$ i.p.v. $\neg(a)$, en $\neg\neg a$ i.p.v. $\neg(\neg(a))$. Men zou ook kunnen zeggen dat $\neg$ een hogere prioriteit heeft dan de infixsymbolen.

Als voorbeeld noemen we $\neg a \wedge \neg b$, wat de conjunctie van $\neg a$ en $\neg b$ voorstelt.

In onze tekst zullen we meestal niet veel moeite doen om op haakjes te bezuinigen. We zullen zelfs wel extra haakjes aanbrengen om misverstanden te voorkomen. Zo schrijven we vaak $(\neg a) \rightarrow b$ in plaats van $\neg a \rightarrow b$.

2.6. Propositievariabelen

Om ingewikkelde samenstellingen van proposities gemakkelijk te kunnen bespreken, gaan we proposities door letters voorstellen. Voor deze letters zullen we bij voorkeur a,b,c,d ... kiezen. We noemen deze letters propositievariabelen (maar soms noemen we ze, als hun betekenis is vastgelegd, liever propositieconstanten).

Als we $x > p$ door a, en $2 > 1$ door b voorstellen, dan is $(x > p) \wedge (2 > 1)$ door $a \wedge b$ voor te stellen.

2.7. Logische formules

Uitdrukkingen, die we op syntactisch correcte wijze samenstellen uit propositievariabelen en propositieconstanten met behulp van connectieven, worden logische formules genoemd. Zo zijn bijv. $(a \wedge b) \rightarrow (\neg c)$ en $\neg((a \rightarrow F) \wedge (b \rightarrow F))$ logische formules.

2.8. Afleidingen

We zullen ons gaan verdiepen in het mechanisme van afleidingen. Dat komt neer op het bekijken van het spel van het maken van onderstellingen en het daaruit trekken van conclusies.

Om met een voorbeeld uit de wiskunde te beginnen, onderstellen we dat we zitten in een situatie waar we weten dat de letters x, y en z reële getallen voorstellen. We zeggen ook wel dat we in een context zitten waarin x, y en z reële getallen zijn. We hebben nog niet gezegd wat proposities in het algemeen zijn, maar hierop vooruitlopende zeggen we dat "x > y", "y > z", enz., proposities zijn.

Het spel van onderstellingen en conclusies houdt nu bijv. in dat uit de onderstellingen "x > y" en "y > z" de conclusie "x > z" kan worden getrokken. We zeggen ook wel dat uit die onderstellingen die conclusie kan worden afgeleid.

Een andere manier om ditzelfde te zeggen is dat onder de onderstellingen "x > y" en y > z" de propositie "x > z" geldig is. We kunnen ook hier weer het woord "context" gebruiken, en zeggen dat in een context die "x > y" en "y > z" bevat ook de propositie "x > z" geldig is. We gebruiken dus het woord context op twee manieren: (1) om aan te duiden dat zekere letters daar betekenis hebben als bijv. reële getallen, en (2) om aan te geven dat zekere proposities tot de onderstellingen behoren.

Een prettige methode om die contexten te administreren, althans in geschreven tekst (bij drukwerk is het wat minder plezierig, doordat het buiten de genormaliseerde zetwijzen valt), is de methode van de <u>vlaggen</u> en <u>vlaggestokken</u>.

We zetten elke onderstelling als tekst op een vlag, en de vlaggestok loopt aan de linkerkant van de tekst door over het tekstgedeelte waar die onderstelling gehandhaafd wordt. Als voorbeeld van een wiskundige afleiding geven we

$\boxed{x > y}$

  $\boxed{y > z}$

      $x > z$

      $x + y > z + y$

      $(x > y) \wedge (y > z)$

We geven hierop wat commentaar. Het voorbeeld is in de eerste plaats bedoeld om aan te geven hoe die vlaggestokken gebruikt worden. De regels volgens welke de conclusies worden getrokken, waren nog niet goed door afspraken voorbereid.

Een eerste opmerking is dat eigenlijk ook het feit dat in onze context de letters x, y en z reële getallen voorstellen, met behulp van vlaggen moet worden uitgedrukt. We zullen dat even vergeten, maar komen er later wel op terug.

De eerste twee conclusies zijn niet gemotiveerd op grond van logische regels, maar op grond van wiskundige stellingen. De eerste conclusie ("$x > z$") is gemaakt op grond van de zogenaamde transitiviteit van de ongelijkheid; voor de tweede ("$x + y > z + y$") is nog wat meer nodig: men zou eigenlijk daarvoor nog een afzonderlijk afleidinkje moeten schrijven.

Maar bij de derde conclusie ("$(x > y) \wedge (y > z)$") ligt het veel eenvoudiger. We hoeven daarvoor niets te weten over de betekenis van de proposities "$x > y$" en "$y > z$". We hoeven alleen een beroep te doen op de fundamentele (nog te formuleren) logische regel dat wanneer twee proposities tot de onderstellingen behoren, hun conjunctie een conclusie mag zijn.

We zullen ons met wiskundige regels in het geheel niet ophouden en ons tot logische beperken.

Om die logische regels te bespreken maken we gebruik van propositievariabelen, zoals a, b, c. Als we een regel formuleren in termen van propositievariabelen, dan is die regel bedoeld voor alle gevallen waarin die propositievariabelen door misschien meer gecompliceerde proposities zijn vervangen. Zo kan de conclusie "$(x > y) \wedge (y > z)$" in het bovenstaande voorbeeld worden getrokken op grond van een (nog te formuleren) regel die zegt dat onder de onderstellingen a en b de conclusie $a \wedge b$ mag worden getrokken.

Afleidingsregel 1 (de regel "HERHAAL").

Een eerste, zeer eenvoudige regel is dat als a in de lijst van onderstellingen voorkomt, diezelfde a ook als conclusie mag worden getrokken. Dus in de context van een stel onderstellingen zijn al die onderstellingen geldige proposities.

Afleidingsregel 2.

Een tweede regel die door de keus van de termen "onderstelling", "conclusie" bijna vanzelfsprekend klinkt, is deze: Als een propositie onder zekere onderstellingen geldig is, dan is die propositie ook geldig wanneer de verzameling der onderstellingen met één of meer onderstellingen wordt uitgebreid. We zullen deze regel doorgaans in combinatie met andere regels toepassen. Het gebruik van afleidingsregel 2 wordt dan niet afzonderlijk vermeld. Vandaar dat we deze regel dan ook geen afkortende naam geven.

De regels die we vervolgens gaan formuleren gelden allemaal in iedere context. Ze zijn van de vorm: als enkele met name genoemde proposities in zekere context geldig zijn, dan zijn ook eën of meer andere proposities geldig in diezelfde context. Alleen bij regel 6 ligt het iets ingewikkelder.

Al deze regels zijn bedoeld met mogelijkheid tot substitutie: als f en g logische formules zijn, en een regel is uitgedrukt met propositievariabelen a en b, dan mogen in die regel de a en b door f en g vervangen worden. Afleidingsregel 3 is dus als volgt te lezen: als f en g logische formules zijn, en als in zekere context f ∧ g geldig is, dan zijn in die context ook f en g afzonderlijk geldig.

2.9. Regels voor de conjunctie

Afleidingsregel 3 (de regel EL ∧).

Als a ∧ b in de een of andere context geldig is, dan zijn a en b in die context beide geldig.

We drukken deze regel in verkorte vorm uit door het schema

$$\frac{a \wedge b}{a \qquad b}$$

Boven de streep staan de proposities waarvan we willen zeggen dat ze tot de onderstellingen behoren (in dit geval is er maar één), onder de streep de proposities waarvan we willen zeggen dat ze als conclusies mogen worden getrokken.

Afleidingsregel 4 (de regel IN ∧).

$$\frac{a \qquad b}{a \wedge b}$$

2.10. Regels voor de implicatie

Als a en b proposities zijn, dan is ook de "implicatie van a naar b", genoteerd met "a → b", een propositie. Het werken met implicaties is wezenlijk moeilijker dan het werken met conjuncties, zoals wel zal blijken bij afleidingsregel 6, die een geheel andere vorm heeft dan de afleidingsregels 3, 4 en 5.

Afleidingsregel 5 (de regel EL $\to$; deze regel wordt gewoonlijk "modus ponens" genoemd).

$$\frac{a \qquad a \to b}{b}$$

Afleidingsregel 6 (de regel IN $\to$).

Als in de één of andere context na toevoeging van de onderstelling a de propositie b geldig is, dan is in de oorspronkelijke context de implicatie $a \to b$ geldig.

We geven even een voorbeeldje van een afleiding die deze regels toepast.

$\boxed{a}$	
$\boxed{b \wedge c}$	
b	(op grond van EL $\wedge$)
$(b \wedge c) \to b$	(op grond van IN $\to$)
$((b \wedge c) \to b) \wedge a$	(op grond van IN $\wedge$)
$a \to ((b \wedge c) \to b) \wedge a)$	(op grond van IN $\to$)

Opmerkingen. 1. In de regels 4 en 6 wordt in de conclusies een conjunctie resp. een implicatie bereikt. Men noemt die regels dan ook wel de regels voor "introductie van conjunctie" en "introductie van implicatie". Vandaar de afkortingen IN $\wedge$ en IN $\to$.

In de regels 3 en 5 komen de conjunctie resp. implicatie bij de onderstellingen voor, maar niet bij de conclusies. In deze regels worden conjunctie en implicatie gebruikt, en niet afgeleid. Daar ze in de conclusies niet meer voorkomen, noemt men deze regels wel "eliminatie van conjunctie" resp. "eliminatie van implicatie". Vandaar de afkortingen EL $\wedge$ en EL $\rightarrow$.

2. Soms bereiken we proposities die geldig blijken zonder dat er onderstellingen gemaakt zijn, of, anders gezegd, geldig zijn in een lege context. Dat is bijv. het geval geweest in bovenstaande afleiding van $a \rightarrow ((b \wedge c) \rightarrow b) \wedge a)$. We zeggen in zo'n geval zonder meer dat de propositie is afgeleid.

2.11. Voorbeelden van afleidingen

Om de toelichting zo duidelijk mogelijk te maken geven we een nummer aan elke tekstregel van de afleiding, met inbegrip van de onderstellingsvlaggen. In de aanwijzingen gebruiken we die nummers voor verwijzing. De nummers die we opgeven, hebben betrekking op wat er in de afleidingsregels boven de streep staat. Bij regel IN $\rightarrow$ werkt het een beetje anders. In de voorbeelden is wel duidelijk hoe dit gebeurt.

1. Afleiding van $(a \wedge b) \rightarrow (b \wedge a)$

1	$\boxed{a \wedge b}$	
2	$\quad a$	EL $\wedge$ (1)
3	$\quad b$	EL $\wedge$ (1)
4	$\quad b \wedge a$	IN $\wedge$ (3,2)
5	$(a \wedge b) \rightarrow (b \wedge a)$	IN $\rightarrow$ (4) .

2. Afleiding van ((a → (b → c)) → (b → (a → c)).

1	a → (b → c)	
2	b	
3	a	
4	b → c	EL → (1,3)
5	c	EL → (4,2)
6	a → c	IN → (5)
7	b → (a → c)	IN → (6)
8	(a → (b → c)) → (b → (a → c))	IN → (7)

3. Afleiding van a ∧ (b ∧ c) uit de onderstelling (a ∧ b) ∧ c.

1	(a ∧ b) ∧ c	
2	a ∧ b	EL ∧ (1)
3	c	EL ∧ (1)
4	a	EL ∧ (2)
5	b	EL ∧ (2)
6	b ∧ c	IN ∧ (5,3)
7	a ∧ (b ∧ c)	IN ∧ (4,6)

2.12. De kunst van het afleiden

Vaak stellen we ons als taak een gegeven logische formule af te leiden, bijv. in een lege context. Die formule is ons doel.

Zo'n afleiding schrijven we zelden direct van boven naar beneden op. Hier en daar werken we een beetje van achteraf door ons een of meer subdoelen te stellen. Er blijft dan een gat in de afleiding, en we gaan dat gat dichten, soms van boven af, soms van onder af. Laat bijv. ons doel zijn

$$((a \rightarrow b) \wedge (b \rightarrow a)) \rightarrow (((a \rightarrow c) \rightarrow (b \rightarrow c)) \wedge ((b \rightarrow c) \rightarrow (a \rightarrow c)).$$

We beginnen een afleiding als volgt te ontwerpen:

$\boxed{(a \rightarrow b) \wedge (b \rightarrow a)}$

<1>

subdoel $(a \rightarrow c) \rightarrow (b \rightarrow c)$

<2>

subdoel $(b \rightarrow c) \rightarrow (a \rightarrow c)$

$((a \rightarrow c) \rightarrow (b \rightarrow c)) \wedge ((b \rightarrow c) \rightarrow (a \rightarrow c))$.

Er zijn gaten, aangeduid met <1> en <2>. Doordat de situatie zo symmetrisch is, behoeven we alleen maar over gat <1> na te denken. Dit gat vullen we door als doel te stellen om in

$\boxed{a \rightarrow c}$

<3>

$b \rightarrow c$

het gat <3> te vullen. Dit proberen we te vullen met

$\boxed{b}$

<4>

c

Het subdoel c heeft niet meer de vorm van een implicatie of conjunctie. Het wordt dus tijd om eens hogerop naar de gegevens te kijken. Gat <4> zou te vullen zijn met EL $\rightarrow$ als a maar afgeleid kon worden, want $a \rightarrow c$ is beschikbaar. Maar we hebben b $\rightarrow$ a door toepassing van EL $\wedge$ op het bovenste gegeven, en b is beschikbaar omdat het een onderstelling is. We krijgen dus inderdaad a met EL $\rightarrow$, en het gat <4> is gedicht.

2.13. Contradictie

In wiskundige redeneringen hoort men vaak: "nu is een contradictie (d.i. tegenspraak) bereikt", en dan worden daaruit verdere conclusies getrokken. Dat een contradictie is bereikt wordt gewoonlijk gezien als een soort situatie, en men heeft dan niet het gevoel dat "contradictie" een propositie is, die op dat ogenblik is afgeleid. Wij zullen dat wel gaan doen. We nemen een fundamentele propositieconstante aan die we F zullen noemen. Deze F wordt ook "falsum" of "contradictie" genoemd. Soms wordt in één of andere context F afgeleid, wat overeenkomt met de zegswijze "en nu is een tegenspraak bereikt".

Wat we eigenlijk willen concluderen uit het bereiken van een contradictie in een zekere context is, dat de onderstelling van die context "niet waar" is (gemakshalve denken we even alleen aan het geval dat die context uit slechts één onderstelling bestaat; in het algemene geval moet men zeggen dat de onderstellingen niet met elkaar verenigbaar zijn, of dat de laatste onderstelling niet klopt in de context gevormd door alle andere).

Laat ons in overeenstemming hiermee bij elke propositie a een propositie $\neg$a invoeren (uitspreken als "niet a"), als afkorting voor "a $\rightarrow$ F". Syntactisch is $\neg$ een unaire operator.

Dit maakt redeneringen van de volgende soort mogelijk.

1	$\boxed{f}$	
2	...	
3	...	
4	F	
5	¬ f	IN → (3)

In dit schema kan f de een of andere logische formule zijn, zoals bijv. (a → b) → a. We laten ons er niet over uit wat er op de stippeltjes in tekstregels 2 en 3 gestaan heeft. De hele zaak speelt zich af in de één of andere context waarin het mogelijk is op die puntjes geldige proposities neer te schrijven en waarin vervolgens in tekstregel 4 tot F kan worden geconcludeerd.

Als voorbeeld geven we een afleiding van ¬ ¬ a uit a.

1	$\boxed{a}$	
2	$\boxed{\neg a}$	
3	F	EL → (2,1)
4	¬¬ a	IN → (3)

Bedenk dat in tekstregel 2 de onderstelling ook als a → F gelezen kan worden, en dat in tekstregel 4 eigenlijk (a → F) → F staat.

In deze redenering speelt F eigenlijk geen bijzondere rol. Met een propositievariabele b kunnen we op precies dezelfde manier afleiden dat onder de onderstelling a geldt dat (a → b) → b.

2.14. De regel van de dubbele ontkenning

Wat we eigenlijk ook willen is dit: als we uit $\neg$ a een contradictie hebben afgeleid, willen we tot a concluderen. Dat zou een afleiding zijn van het volgende type:

$$\begin{array}{|l} \boxed{\neg a} \\ \quad \ldots \\ \quad \ldots \\ \quad F \end{array}$$

a (op grond waarvan??)

Om dit te realiseren voeren we een nieuwe afleidingsregel in, die zegt: als in de een of andere context $\neg\neg$ a geldig is dan is daar a zelf ook geldig. Dus

Afleidingsregel 7 (de regel DBNG).

$$\frac{\neg\neg a}{a}$$

De afkorting DBNG staat voor "dubbele negatie". Deze regel staat in nauw verband met wat men de regel van de uitgesloten derde noemt (steeds is a geldig of $\neg$ a, een derde mogelijkheid is er niet). Het is deze afleidingsregel 7 die ons logische systeem in feite tot het systeem van de z.g. klassieke propositielogica maakt.

We geven wat voorbeelden. Eerst leiden we uit de implicatie a $\rightarrow$ b de z.g. contrapositie ($\neg$b) $\rightarrow$ ($\neg$a) af; hierbij wordt DBNG nog niet gebruikt.

1	$\boxed{a \to b}$	
2	$\boxed{\neg b}$	
3	$\boxed{a}$	
4	b	EL $\to$ (1,3)
5	F	EL $\to$ (2,4)
6	$\neg a$	IN $\to$ (5)
7	$(\neg b) \to (\neg a)$	IN $\to$ (6)

Het tweede voorbeeld leidt de z.g. <u>falsumregel</u> af, die zegt dat uit de contradictie eenvoudig alles volgt. We merken terzijde op, dat de z.g. intuïtionistische logica deze regel wel heeft, maar die van de dubbele ontkenning niet.

1	$\boxed{F}$	
2	$\boxed{\neg a}$	
3	F	HERHAAL (1)
4	$\neg\neg a$	IN $\to$ (3)
5	a	DBNG (4)

Er zijn ook proposities die in het geheel geen F bevatten en die we toch niet zonder DBNG kunnen afleiden. Een mooi voorbeeld is dat van Peirce: $((a \to b) \to a) \to a$. Merk op dat we op grond van de afspraken over het weglaten van haakjes ook $a \to b \to a \to a$ mogen schrijven, maar dit vindt bijna iedereen onplezierig, misschien omdat het associativiteit zou suggereren.

1	$(a \to b) \to a$	
2	$\neg a$	
3	a	
4	$\neg b$	
5	F	EL $\to$ (2,3)
6	$\neg\neg b$	IN $\to$ (5)
7	b	DBNG (6)
8	$a \to b$	IN $\to$ (7)
9	a	EL $\to$ (1,8)
10	F	EL $\to$ (2,9)
11	$\neg\neg a$	IN $\to$ (10)
12	a	DBNG (11)
13	$(((a \to b) \to a) \to a)$	IN $\to$ (12)

2.15. Tautologieën

Een logische formule die in een lege context afleidbaar is heet een tautologie. Voorbeelden hebben we al gezien:

$a \to (\neg\neg a)$

$((a \to b) \to a) \to a$

$F \to a$

en we geven er nog wat meer:

$$\neg\neg a \rightarrow a$$

$$a \rightarrow a$$

$$a \rightarrow (b \rightarrow a)$$

$$\neg a \rightarrow (a \rightarrow b)$$

$$(a \rightarrow b) \wedge (b \rightarrow c) \rightarrow (a \rightarrow c)$$

$$((a \wedge b) \rightarrow c) \rightarrow (a \rightarrow (b \rightarrow c))$$

Uit tautologieën zijn weer nieuwe tautologieën te maken door middel van substitutie. Als een reeds gevonden tautologie de propositievariabelen a, b, c bevat, en als f, g, h logische formules zijn, en als we in de genoemde tautologie voor a, b, c resp. f, g, h substitueren, dan ontstaat weer een tautologie.

2.16. Equivalentie

We voeren de binaire infixoperator $\Leftrightarrow$ in door $a \Leftrightarrow b$ te definiëren als

$$(a \rightarrow b) \wedge (b \rightarrow a) \ .$$

Er zijn veel voorbeelden te geven van equivalenties die tautologieën zijn, bijv.

$$a \wedge b \Leftrightarrow b \wedge a$$

$$(a \wedge b) \wedge c \Leftrightarrow a \wedge (b \wedge c)$$

$$(a \wedge b) \rightarrow c \Leftrightarrow a \rightarrow (b \rightarrow c)$$

$$a \Leftrightarrow \neg\neg a$$

$$a \rightarrow (b \wedge c) \Leftrightarrow (a \rightarrow b) \wedge (a \rightarrow c)$$

$$a \rightarrow b \Leftrightarrow \neg(a \wedge \neg b) \ .$$

2.17. Het maken van nieuwe afleidingsregels

Als f en g logische formules zijn en als $f \rightarrow g$ een tautologie is, dan kunnen we

$$\frac{f}{g}$$

als nieuwe afleidingsregel gebruiken. De f en g bevatten weer propositievariabelen, en hier geldt weer de mogelijkheid tot substitutie. We laten dat aan een voorbeeld zien. Voor f nemen we $(a \wedge b) \wedge c$, voor g nemen we $((b \wedge c) \wedge a$. In lege context is afleidbaar

$$(a \wedge b) \wedge c \rightarrow (b \wedge c) \wedge a.$$

Nu hebben we de afleidingsregel gemaakt

$$\frac{(a \wedge b) \wedge c}{(b \wedge c) \wedge a} \quad ,$$

die als volgt kan worden gebruikt: Als f, g, h logische formules zijn, en als in de één of andere context $(f \wedge g) \wedge h$ geldig is, dan is in die context ook $(g \wedge h) \wedge f$ geldig.

Een ander voorbeeld: de falsumregel, d.i. de tautologie $F \rightarrow a$, kan als afleidingsregel gebruikt worden, nl.

$$\frac{F}{a} \; .$$

Hierboven ging het over afleidingsregels die voortkomen uit een tautologie van de vorm $f \rightarrow g$. Het kan ook ingewikkelder. Een tautologie van de vorm

$$(f \wedge g \wedge h) \rightarrow (p \wedge q)$$

geeft de volgende afleidingsregel:

$$\frac{f \quad g \quad h}{p \quad q} \quad .$$

2.18. Disjunctie

We zullen nu de disjunctie van a en b, d.i. de propositie a $\vee$ b, uitdrukken met behulp van de operatoren die we al hebben. We doen dat op niet-symmetrische manier; de symmetrie moet alsnog worden afgeleid.

We gaan uit van de gedachte dat "a of b" de inhoud heeft "als a niet dan b wel", met de bijgedachte "als a wel dan b misschien ook". We laten eerst zien dat deze ogenschijnlijk asymmetrische uitdrukking toch symmetrisch is wat betekenis betreft.

1	$\boxed{(\neg a) \rightarrow b}$	
2	$\boxed{\neg b}$	
3	$\boxed{\neg a}$	
4	b	EL $\rightarrow$ (1,3)
5	F	EL $\rightarrow$ (2,4)
6	$\neg\neg$ a	IN $\rightarrow$ (5)
7	a	DBNG (6)
8	$(\neg b) \rightarrow a$	IN $\rightarrow$ (7)

We maken nu de infixoperator $\vee$ doordat we $(\neg a) \rightarrow b$ afkorten tot a $\vee$ b. De bovenstaande afleiding levert dus de symmetrie: uit a $\vee$ b volgt b $\vee$ a. We hebben dus als tautologie

$$(a \vee b) \rightarrow (b \vee a) \ .$$

Ook een zeer bekende tautologie is $a \vee (\neg a)$; dit wordt de regel van de uitgesloten derde genoemd.

Op grond van de definitie van $a \vee b$ door $(\neg a) \rightarrow b$ hebben we als afleidingsregels natuurlijk

$$\frac{(\neg a) \rightarrow b}{a \vee b} \qquad \frac{(\neg b) \rightarrow a}{a \vee b} \ .$$

Verdere belangrijke afleidingsregels voor de disjunctie zijn:

$$\frac{a}{a \vee b} \qquad (\text{IN1 } \vee)$$

$$\frac{b}{a \vee b} \qquad (\text{IN2 } \vee)$$

$$\frac{a \vee b \quad a \rightarrow c \quad b \rightarrow c}{c} \qquad (\text{EL } \vee)$$

Deze regels volgen uit de volgende afleidingen:

1	$\boxed{a}$	
2	$\quad \boxed{\neg a}$	
3	$\quad F$	EL $\rightarrow$ (2,1)
4	$\quad b$	(falsumregel toegepast op 3)
5	$a \vee b$	IN $\rightarrow$ (4)

1	b	
2	$\neg a$	
3	b	HERHAAL (1)
4	$a \vee b$	IN $\rightarrow$ (3)

1	$\neg a \rightarrow b$	
2	$a \rightarrow c$	
3	$b \rightarrow c$	
4	$\neg c$	
5	a	
6	c	EL $\rightarrow$ (1,5)
7	F	EL $\rightarrow$ (4,6)
8	$\neg a$	IN $\rightarrow$ (7)
9	b	EL $\rightarrow$ (3,8)
10	c	EL $\rightarrow$ (2,9)
11	F	EL $\rightarrow$ (4,10)
12	$\neg\neg c$	IN $\rightarrow$ (11)
13	c	DBNG (12)

De regel EL $\vee$ wordt gebruikt om bij een afleiding in gevallen te splitsen. We willen van een logische formule h laten zien dat het een tautologie is, en we hebben logische formules f en g waarvan we de disjunctie f $\vee$ g tot onze beschikking hebben (bijv. als g de ontkenning van f is). We leiden dan eerst h af onder de onderstelling f, daarna onder de onderstelling g, en concluderen dan tot h:

1	$f \vee g$	
2	f	
3	...	
4	h	
5	g	
6	...	
7	h	
8	h	wegens 1,4,7

Als voorbeeld bewijzen we de tautologie

$$((a \to b) \vee (a \to c)) \to (a \to (b \vee c))$$

1	$(a \to b) \vee (a \to c)$	
2	a	
3	$a \to b$	
4	b	EL $\to$ (3,2)
5	$b \vee c$	IN1 $\vee$ (4)
6	$a \to c$	
7	c	EL $\to$ (6,2)
8	$b \vee c$	IN2 $\vee$ (7)
9	$b \vee c$	wegens 1,5,8
10	$a \to (b \vee c)$	IN $\to$ (9)

2.19. Alternatieve invoering van de disjunctie

We hebben $a \vee b$ ingevoerd door te zeggen dat het een afkorting is voor $(\neg a) \to b$. Een gemakkelijk af te leiden conclusie is dat $a \vee b$

equivalent is met $\neg((\neg a) \wedge (\neg b))$.

We hadden even goed $a \vee b$ kunnen invoeren door middel van $\neg((\neg a) \wedge (\neg b))$, en als conclusie kunnen trekken dat $a \vee b$ equivalent is met $(\neg a) \rightarrow b$ en met $(\neg b) \rightarrow a$. Het is een kwestie van smaak.

2.20. Verdere tautologieën die disjunctie bevatten.

Hierboven noemden we

$$a \vee b \leftrightarrow \neg((\neg a) \wedge (\neg b)) .$$

We noemen ook de z.g. distributieve wetten

$$(a \vee b) \wedge c \leftrightarrow (a \wedge c) \vee (b \wedge c)$$

$$(a \wedge b) \vee c \leftrightarrow (a \vee c) \wedge (b \vee c)$$

en ook nog

$$(a \vee b) \rightarrow c \leftrightarrow (a \rightarrow c) \wedge (b \rightarrow c)$$

2.21. Vervanging

Vaak heeft men bij afleidingen gemak van het volgende principe: men heeft in een zekere context een formule h afgeleid, die een formule f als subexpressie heeft, en in die context is $f \leftrightarrow g$. Dan kan de fomule die uit h ontstaat als we f door g vervangen, ook als afgeleid beschouwd worden.

We zullen dit principe niet uitvoerig toelichten. We zeggen slechts dat het te halen is uit tautologieën als

$$(a \leftrightarrow b) \rightarrow ((a \wedge c) \leftrightarrow (b \wedge c))$$

$$(a \leftrightarrow b) \rightarrow ((a \rightarrow c) \leftrightarrow (b \rightarrow c))$$

$$(a \leftrightarrow b) \rightarrow ((c \rightarrow a) \leftrightarrow (c \rightarrow b))$$

enz.

Als voorbeeld geven we een afleiding met behulp van het vervangingsprincipe. We willen de tautologie

$$(((a \rightarrow b) \rightarrow (\neg a)) \wedge (a \vee c) \wedge (b \vee c)) \rightarrow c$$

afleiden. De combinatie $(a \rightarrow b) \rightarrow (\neg a)$ doet wat onbekend aan, maar men kan laten zien dat het equivalent is met $(\neg a) \vee (\neg b)$. Ook is $a \vee c$ equivalent met $\neg a \rightarrow c$ en $b \vee c$ met $\neg b \rightarrow c$. Als we op grond van deze equivalenties vervangen, wordt onze formule een directe toepassing van EL $\vee$ met $\neg a$, $\neg b$ en c.

2.22. Gegeneraliseerde implicatie en gegeneraliseerde conjunctie

Bij de regel IN $\rightarrow$ is een waarschuwing op zijn plaats. In de wiskunde komt het nogal eens voor dat onder een onderstelling f een conclusie g wordt getrokken die niet alleen pas onder de onderstelling f kan worden afgeleid, maar die zelfs pas onder de onderstelling f gevormd kan worden. In onze eenvoudige wereld van logische formules kwam zoiets niet voor.

Een heel gewoon voorbeeld wordt gegeven door het feit dat $\ln x$ alleen gedefinieerd is als $x > 0$. Kort de propositie $x > 3$ af tot f. Onder de onderstelling f kan nu over $\ln x$ gesproken worden, en worden vastgesteld dat $\ln x > 0$. Maar in dit geval mag geen beroep gedaan worden op de regel IN $\rightarrow$ om te concluderen tot $x > 3 \rightarrow \ln x > 0$. Men kan het wel proberen te schrijven, maar moet het dan een gegeneraliseerde implicatie noemen. Er mag niet alles mee wat er met een gewone implicatie mag. Men kan bijv. niet de contrapositie

$$\neg(\ln x > 0) \rightarrow (\neg(x > 3))$$

vormen, want zonder iets over x te weten kan het linkerlid niet gelezen worden.

Een voorbeeld uit het dagelijks leven: "als hij een horloge heeft zal het wel stilstaan" is niet om te vormen tot "als zijn horloge niet stilstaat, zal hij er wel geen hebben".

Iets dergelijks hebben we met gegeneraliseerde conjunctie. Als g pas betekenis heeft onder de onderstelling f, dan mogen we niet $f \wedge g$ op de gewone manier interpreteren. Het zou trouwens niet hetzelfde zijn als $g \wedge f$, want bij het lezen daarvan gaan we al bij het eerste stuk de mist in.

Hoe komt het dat we deze narigheid bij onze logische formules niet gemerkt hebben? Eenvoudig omdat die daar niet voorkwam. Wat daar de proposities zijn, lag al van te voren vast, voordat we ook maar iets begonnen af te leiden. De verrassing van de gegeneraliseerde implicatie en dito conjunctie komt doordat we vrijheden uit een eenvoudig systeem zonder meer proberen te handhaven voor een ingewikkelder systeem.

In dat ingewikkelder systeem kan men de regel IN $\rightarrow$ toch heel goed handhaven, maar men moet eerst constateren dat f en g proposities zijn, dan onder de onderstelling f de propositie g gaan afleiden en dan tot $f \rightarrow g$ concluderen.

HOOFDSTUK 3. PREDIKATEN

3.1. Inleiding

In de predikatenlogica krijgen we te maken met iets wat in de propositielogica nog niet bekeken behoefde te worden, nl. "gewone" variabelen. Het gaat dan over letters die wiskundige objecten voorstellen, en dat is wat anders dan wat er gebeurt bij de propositievariabelen uit de propositielogica.

Bij variabelen zal steeds een domein staan aangegeven in de vorm van een verzameling. Als S een verzameling is, kunnen we bij de letter x afspreken dat die elementen van S kan voorstellen. Wat dit betekent is niet gemakkelijk precies te zeggen, maar waar het om gaat is weer niet de vraag wat de dingen zijn, maar hoe we met de dingen omgaan.

Vaak komt het voor dat er bij elke x uit de verzameling S een propositie is aangegeven. Voorbeeld: als S de verzameling van de gehele getallen is, en $x \in S$, dan is $x > 6$ een propositie. We hebben dan een wat ongewoon soort afbeelding: aan elke x uit S is niet een element van een verzameling toegevoegd, maar een propositie. Zo'n afbeelding zullen we een predikaat noemen, en meer specifiek een predikaat over S (of, wat hetzelfde betekent, een predikaat met domein S).

We hanteren dezelfde gewoonten als bij functies. Als een functie f heet, wordt de door f aan het element x toegevoegde waarde met f(x) aangeduid. Evenzo stellen we een predikaat door een letter als P, Q, ... voor. Als P een predikaat over S is, en $x \in S$, dan is P(x) de aan x toegevoegde propositie.

Om een indruk te geven van wat we met predikaten doen, lopen we even wat vooruit. Als voor elke x uit S de propositie P(x) is afgeleid, willen we dat feit als een enkele propositie uitdrukken. Deze propositie kan worden genoemd:

"P is universeel geldig". (1)

Voorbeeld van zo'n P: als S weer de verzameling van de gehele getallen is, en voor elke x uit S met P(x) de propositie x + 1 > x wordt bedoeld, dan is P universeel geldig.

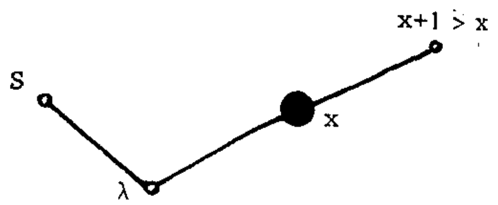
De propositie (1) wordt voorgesteld door $\forall P$. (Die ondersteboven A heet het al-symbool.) Erg gebruikelijk is deze notatie niet, meestal bedient men zich van een gebonden variabele.

3.2. Notatie met gebonden variabele

We hebben ook behoefte aan iets korters dan de zin: "Voor elke x uit S stelt P(x) de propositie x + 1 > x voor".We maken het korter door te zeggen dat P voorstelt

$$\lambda_{x \in S}\ (x + 1 > x) \qquad (2)$$

Hierin is x een gebonden variabele. In boomvorm zou men dit kunnen uitdrukken door wat in figuur 20 is getekend.



Figuur 20. De boomvorm van formule (2)

Heeft men eenmaal (2) opgeschreven dan is vaak het invoeren van de letter P niet meer nodig.

Overigens: de notatie (2) is wel heel goed bruikbaar maar zeker niet algemeen gangbaar.

Als (2) wordt afgekort tot P, dan kunnen we de propositie $\forall P$ beschouwen.

Met vermijding van die P wordt dit gewoonlijk geschreven als

$$\forall_{x \in S} \; (x + 1 > x) \; . \tag{3}$$

(Die ondersteboven A heet samen met het <u>subscript</u> $x \in S$ de <u>al-kwantor</u>.)

We kunnen zeggen dat (3) een afkorting is van

$$\forall(\lambda_{x \in S} \; (x + 1 > x)) \; . \tag{4}$$

De notatie (2) wordt gebruikt om van de (van x afhankelijke) propositie $x + 1 > x$ over te gaan op het predikaat. Heeft men dit predikaat door de letter P voorgesteld, dan betekent omgekeerd

$$P(x) \qquad \text{hetzelfde als} \qquad x + 1 > x.$$

In plaats van $\forall P$ schrijft men doorgaans

$$\forall_{x \in S} \; P(x) \; . \tag{5}$$

We spreken (5) uit als "voor alle x uit S geldt P(x)".

3.3. Afleidingen waarin objectvariabelen voorkomen

In onze behandeling van propositielogica konden we gewoon zeggen wat de formules waren waarmee we omgingen, de "logische formules". In onze behandeling van de predikatenlogica valt dit moeilijker: of we moeten eerst een taal voor een stuk wiskunde ontwikkelen, of we moeten ons op een erg formeel standpunt stellen waar we in de praktijk niet zo veel aan hebben. We zullen geen van beide doen: we zullen wel met wiskundige formules werken, maar niet grondig op de syntax daarvan ingaan.

Soms willen we in de één of andere context zeggen dat de letter x een element van de verzameling S zal gaan voorstellen. We zeggen ook wel dat daarmee de letter x als variabele (met domein S) is opgevoerd. Dat wil zeggen dat gedurende een stuk van de tekst de letter x gebruikt mag worden, maar dat kan ook weer eens ophouden. Dit kunnen we goed met een vlag en een vlaggestok aangeven. Wel moeten we even oppassen. Een vlag

$$\boxed{x \in S}$$

zou ook kunnen voorkomen in een context waar x al "leeft" (d.w.z. waar x al eerder als variabele was opgevoerd en nog niet afgevoerd), en in dat geval is "$x \in S$" een propositie, en de vlag zou als een nieuwe onderstelling over de oude x (die misschien een groter domein had) kunnen worden opgevat. Dit is de reden dat we voor het aangeven van opvoer van een variabele een ander soort vlag gebruiken, nl. een puntige:

$$x \in S$$

Zolang "we rechts van die vlaggestok zitten" mogen we de letter x gebruiken, en stelt die x een element van S voor.

Introductie van $\forall$ (IN $\forall$)

We geven nu de regel waarmee tot de geldigheid van $\forall_{x \in S}\ P(x)$ kan worden besloten.

Als in de een of andere context de letter S een verzameling voorstelt en P een predikaat met domein S, en als die context wordt uitgebreid met de opvoer $x \in S$, en als binnen die nieuwe context $P(x)$ geldig is, dan is daarmee de universele geldigheid van P in de eerstgenoemde context vastgesteld. Dus na

$x \in S$

$P(x)$

mag volgen

$$\forall_{x \in S}\ P(x)\ .$$

Wat vorm betreft lijkt dit op de regel IN $\rightarrow$ uit de propositielogica.

Eliminatie van $\forall$ (EL $\forall$)

Als in de een of andere context de letter S een verzameling voorstelt en P een predikaat over S, en als

$$\forall_{x \in S}\ P(x)$$

in die context geldig is, en als a een element van S is, dan is in die context P(a) geldig.

3.4. Voorbeelden

1	$x \in S$
2	$P(x)$
3	$Q(x)$
4	$P(x) \rightarrow Q(x)$
5	$\forall_{x \in S}\ (P(x) \rightarrow Q(x))$.

Commentaar: Tussen tekstregels 1 en 2 is op de een of andere manier vastgesteld dat P(x) en Q(x) proposities zijn, en tussen regels 2 en 3 is de afleiding van Q(x) gegeven. Hier stelt Z de verzameling der gehele getallen voor. De gewone regels over het rekenen daarmee zijn gebruikt.

1	$x \in Z$	
2	$x > 0$	
3	$x + x > x$	
4	$2x > x$	
5	$(x > 0) \rightarrow (2x > x)$	
6	$\forall_{x \in Z}\ ((x > 0) \rightarrow (2x > x))$	

Commentaar: In tekstregels 3 en 4 zijn wiskundige stellinkjes gebruikt.

1	$x \in Z$	
2	$y \in Z$	
3	$x - y \in Z$	
4	$(x - y)^2 \geq 0$	
5	$x^2 + y^2 \geq 2xy$	
6	$\forall_{y \in Z}\ ((x^2 + y^2) \geq 2xy)$	IN $\forall$ (5)
7	$\forall_{x \in Z}\ \forall_{y \in Z}\ ((x^2 + y^2) \geq 2xy)$	IN $\forall$ (6)

We geven tenslotte een samengesteld voorbeeld, waarin weer de letter Z de verzameling van de gehele getallen voorstelt. De inhoud van het voorbeeld is niet interessant, het gaat ons weer alleen om de handeling.

1	$p \in Z$	
2	$x \in Z$	
3	$x > 8$	
4	$\forall_{y \in Z}\ (y > 5 \rightarrow y^2 > p)$	
5	$x > 5 \rightarrow x^2 > p$	EL $\forall$ (4,2)
6	$x > 8$	HERHAAL (3)
7	$x > 5$	
8	$x^2 > p$	EL $\rightarrow$ (5,7)
9	$\forall_{p \in Z}\ \forall_{x \in Z}\ (x > 8 \rightarrow ((\forall_{y \in Z}\ (y > 5 \rightarrow y^2 > p)) \rightarrow x^2 > p))$	

We geven nog wat commentaar. In regel 7 is iets toegepast wat buiten de logica valt, nl. de transitiviteit van de ongelijkheid, losgelaten op regel 6 en de geldigheid van $8 > 5$.

Bij tekstregel 9 is heel wat tegelijk gebeurd: eerst is IN $\rightarrow$ (8) toegepast, daarop vervolgens nog eens IN $\rightarrow$, op dat weer IN $\forall$ en tenslotte nog eens IN $\forall$. Daarmee zijn achtereenvolgens de vlaggen 4, 3, 2 en 1 afgedankt.

3.5. Opmerking.

De al-kwantor maakt een soort conjunctie. Als bijv. S uit drie elementen a, b en c bestaat, dan betekent $\forall_{x \in S}\ P(x)$ hetzelfde als $P(a) \wedge P(b) \wedge P(c)$.

3.6. Lege verzameling

Als de verzameling S leeg is, is daarop elk predikaat universeel geldig. Leeg zijn betekent nl. dat wanneer we een element aanwezig veronderstellen we een contradictie hebben:

$x \in S$

F

en uit een contradictie is immers alles af te leiden. Dus ook

$x \in S$

$P(x)$

en daaruit volgt (met IN $\forall$) $\forall_{x \in S}\, P(x)$.

3.7. Existentie

Als (in de één of andere context) S een verzameling is, P een predikaat op S, en a een element van S zodanig dat P(a) geldig is, dan is

$$\neg \forall_{x \in S}\, (\neg P(x)) \qquad (6)$$

geldig in die context, wegens de volgende afleiding:

1	$a \in S$	
2	$P(a)$	
3	$\forall_{x \in S}\, (\neg P(x))$	
4	$\neg P(a)$	EL $\forall$ (3,1)
5	F	EL $\rightarrow$ (4,2)
6	$\neg(\forall_{x \in S}\, (\neg P(x)))$	IN $\rightarrow$ (5)

We zullen (6) afkorten tot

$$\exists_{x \in S}\ P(x) \tag{7}$$

en uitspreken als "er bestaat een x in S met P(x)". Het teken $\exists$ heet het <u>existentiesymbool</u>, en met het subscript $x \in S$ erbij heet het <u>existentie-kwantor</u>. Het maakt een soort disjunctie. Als bijv. S uit de drie elementen a, b, c bestaat, dan drukt (7) hetzelfde uit als

$$\neg((\neg P(a)) \wedge (\neg P(b)) \wedge (\neg P(c)))$$

en dat is equivalent met

$$P(a) \vee P(b) \vee P(c).$$

3.8. <u>Introductie van existentie</u> (IN $\exists$)

Dit is de regel die hierboven al "afgeleid" werd

$$\frac{a \in S \qquad P(a)}{\exists_{x \in S}\ P(x)}$$

3.9. <u>De zwakte van ons existentiebegrip</u>

Als we (7) hebben afgeleid zijn we niet altijd in staat werkelijk een x aan te wijzen waarvoor P(x) geldt. Dat er zo'n x is, is misschien wel "waar", maar ons afleidingssysteem levert zo'n x niet op.

We laten dit zien aan een bekend voorbeeld. Laat S de verzameling van de irrationale getallen voorstellen, en Q die van de rationale. We gaan afleiden

$$\exists_{x \in S}\ x^{\sqrt{2}} \in Q\ . \tag{8}$$

Wegens de regel van de uitgesloten derde is

$$(\sqrt{3})^{\sqrt{2}} \in Q \vee (\sqrt{3})^{\sqrt{2}} \in S \tag{9}$$

maar het is heel moeilijk uit te maken welke van de twee mogelijkheden geldt. Toch gebruiken we (9) om (8) af te leiden, nl. door gevalonderscheiding. In het geval $(\sqrt{3})^{\sqrt{2}} \in Q$ nemen we $a = \sqrt{3}$, we weten dat $a \in S$, en (8) volgt door IN $\exists$. In het geval $(\sqrt{3})^{\sqrt{2}} \in S$ nemen we $a = (\sqrt{3})^{\sqrt{2}}$, we weten weer dat $a \in S$, en $a^{\sqrt{2}} = ((\sqrt{3})^{\sqrt{2}})^{\sqrt{2}}$, wat in Q ligt, en ook nu volgt (8) weer door IN $\exists$.

We hebben dus (8) bewezen zonder ook maar één x uit S echt aan te wijzen waarvoor $x^{\sqrt{2}} \in Q$.

3.10. Eliminatie van existentie (EL $\exists$)

Zoals hierboven werd aangeduid zijn we niet in staat om uit (7) existentie te elimineren door een element x aan te wijzen waarvoor P(x) geldt. Maar we hebben een eliminatieregel die op dezelfde wijze is opgebouwd als de regel EL $\vee$ voor disjunctie.

Laat in zekere context b een propositie zijn, S een verzameling, en P een predikaat over S. Dan is de regel EL $\exists$:

$$\frac{\exists_{x\in S}\, P(x) \qquad \forall_{x\in S}(P(x) \to b)}{b} \;.$$

Voorbeeld: Laat p en q reële getallen zijn. We leiden uit

$$\exists_{x\in Q}\, (p < x \wedge x < q) \tag{10}$$

(waarin Q de verzameling van de rationale getallen is) af, dat $p < q$.

Deze propositie $p < q$ noemen we b, en de propositie $p < x \wedge x < q$ noemen we $P(x)$. We gaan nu als volgt te werk.

1	$\boxed{x \in Q}$	
2	$\quad \boxed{p < x \wedge x < q}$	
3	$\quad\quad p < q$	(transitiviteit van $<$)
4	$P(x) \rightarrow b$	IN $\rightarrow$ (3)
5	$\forall_{x \in Q}(P(x) \rightarrow b)$	IN $\forall$ (4)

Volgens EL $\exists$ kunnen we nu tot b concluderen.

Men kan ook toestaan de afleiding korter te schrijven:

$\boxed{x \in Q}$	
$\quad \boxed{p < x \wedge x < q}$	
$\quad\quad p < q$	
$p < q$	(wegens (10) en EL $\exists$).

In de praktijk spreekt men hierbij als volgt: We hebben (10). Neem nu zo'n x die aan $p < x \wedge x < q$ voldoet. Doordat de door het teken "$<$" uitgedrukte relatie transitief is, blijkt dat $p < q$.

Bij deze manier van spreken doet men eigenlijk hetzelfde als we in de afleiding hierboven deden. Alleen wordt er gepraat alsof het mogelijk zou zijn zo een x aan te wijzen.

Heel wezenlijk is dat het eindresultaat iets is dat van de "genomen" x niet afhangt. In de regel EL $\exists$ werd immers de b genoemd voordat er van de variabele x sprake was.

3.11. Niet-lege verzameling

Een bijzonder geval van existentie is

$$\exists_{x \in S} (\neg F)$$

hetgeen equivalent is met

$$\neg(\forall_{x \in S} F)$$

dus de ontkenning van "S is leeg". Als b een propositie is komen we tot de regel

$$\frac{S \text{ niet leeg} \qquad \forall_{x \in S}\, b}{b}.$$

Als S niet leeg is kan men dus als volgt redeneren

1	$x \in S$	
2	...	
3	b	
4	b	uit 3, wegens de geldigheid van "S niet leeg".

3.12. Eenduidige existentie

Op een verzameling S hanteren we een gelijkheidsbegrip.

Als $s \in S$, $t \in S$ dan is $s = t$ een propositie. Die voldoet aan (1) $s = s$ (reflexiviteit), (2) $s = t \rightarrow t = s$ (symmetrie) en (3) $s = t \wedge t = u \rightarrow s = u$ (transitiviteit).

Als P een predikaat is op S, en

$$\forall_{x \in S} (\forall_{y \in S} ((P(x) \wedge P(y)) \rightarrow y = x))$$

dan zeggen we dat er ten hoogste één $x \in S$ met $P(x)$ is. In overeenstemming met deze spreekwijze kan men tegen $\exists_{x \in S} P(x)$ zeggen "er is tenminste één $x \in S$ met $P(x)$". De conjunctie

$$\exists_{x \in S} P(x) \wedge \forall_{x \in S} \forall_{y \in S} (P(x) \wedge P(y) \rightarrow x = y)$$

wordt wel genoteerd met

$$\exists^{1}_{x \in S} P(x) \quad (\text{"er is precies één } x \in S \text{ met } P(x)\text{"}).$$

Het is equivalent met

$$\exists_{x \in S}(P(x) \wedge \forall_{y \in S} (P(y) \rightarrow y = x)).$$

3.13. Meer kwantoren achter elkaar

We zien vaak (zoals in 3.12) een rijtje kwantoren achter elkaar staan. Een bekend geval treedt op bij de convergentie van een rij reële getallen. Laat $a(1)$, $a(2)$,... een rij reële getallen zijn. Met R geven we de verzameling van reële getallen aan, met P de deelverzameling van de positieve, met N de verzameling van gehele positieve getallen, met $N(m)$ die van de gehele getallen groter dan m. We zeggen nu dat de rij convergent is als

$$\exists_{b \in R} \forall_{\varepsilon \in P} \exists_{m \in N} \forall_{n \in N(m)} |a(n) - b| < \varepsilon.$$

We kunnen nu bijv. gaan afleiden dat onder de onderstelling

$$\forall_{n\in N}\ |a(n)| < n^{-1}$$

de rij convergent is.

We passen IN $\exists$ toe door voor b het getal 0 te nemen, dat immers tot R behoort. Om IN $\exists$ toe te passen gaan we bewijzen dat

$$\forall_{\varepsilon\in P}\ \exists_{m\in N}\ \forall_{n\in N(m)}\ |a(n) - 0| < \varepsilon.$$

We gaan nu de variabele ε opvoeren, en definiëren vervolgens k als het kleinste positieve gehele getal dat groter is dan $1/\varepsilon$. Met deze k passen we weer IN $\exists$ toe, waar k voor de variabele m wordt ingevuld:

$\varepsilon \in P$

<1> (voorlopig gat)

$$\forall_{n\in N(k)}\ |a(n) - 0| < \varepsilon$$

en nu door IN $\exists$:

$$\exists_{m\in N}\ \forall_{n\in N(m)}\ |a(n) - 0| < \varepsilon .$$

Tenslotte vinden we het gewenste resultaat door toepassing van IN $\forall$. Het gat <1> is heel gemakkelijk te vullen door een variabele n op te voeren met domein N(k), en tot $|a(n) - 0| < \varepsilon$ te concluderen.

3.14. Relaties

Een relatie is een predikaat van twee variabelen. Als S en T verzamelingen zijn, en er aan elk paar (s,t) met $s \in S$ en $t \in T$ een propositie is toegevoegd, dan heet die toevoeging een relatie. Stellen we die relatie door R voor, dan is R(s,t) de aan (s,t) toegevoegde propositie.

Als

$$\forall_{x \in S}\ \exists^1_{y \in T}\ R(x,y)$$

dan zeggen we dat R <u>een functie vastlegt</u>. Er is dan een afbeelding f van S in T met

$$\forall_{x \in S}\ R(x,f(x)).$$

Als R een functie f vastlegt, en als bovendien

$$\forall_{y \in T}\ \exists_{x \in S}\ R(x,y)$$

dan heet f <u>surjectief</u>; men zegt dat f een surjectie is.

Als R een functie f vastlegt en als bovendien

$$\forall_{y \in T}\ \forall_{x \in S}\ \forall_{z \in S}\ ((R(x,y) \wedge R(z,y)) \rightarrow x = z)$$

(dus voor elke $y \in T$ is er ten hoogste één x met R(x,y)) dan heet f <u>injectief</u>; men zegt dat f een injectie is.

Als f zowel surjectief als injectief is dan heet f een <u>bijectie</u>. Dit gebeurt wanneer en slechts wanneer

$$\forall_{y \in T}\ \exists^1_{x \in S}\ R(x,y).$$

3.15. <u>Het vormen van de ontkenning van een rij kwantoren</u>

Als men een propositie gevormd door een rij kwantoren $\forall$ en $\exists$ wil ontkennen, dan vervangt men $\forall$'s door $\exists$'s en omgekeerd, en zet men de ontkenning direct achter de laatste kwantor. Dat kan doordat $\neg\exists$ hetzelfde is als $\neg\neg\forall\neg$, dus equivalent met $\forall\neg$, en $\neg\forall$ equivalent is met $\neg\forall\neg\neg$, wat hetzelfde is als $\exists\neg$. Door deze omzettingen kan de uitspraak dat de rij a(1), a(2),... niet convergent is, worden weergegeven door

$$\forall_{b\in R}\ \exists_{\varepsilon\in P}\ \forall_{m\in N}\ \exists_{n\in N(m)} \neg(|a(n) - b| < \varepsilon).$$

Een ander voorbeeld. De ontkenning van

$$\exists_{x\in S}\ \forall_{y\in S}\ (P(y) \rightarrow y = x)$$

wordt uitgedrukt door

$$\forall_{x\in S}\ \exists_{y\in S}\ (P(y) \wedge \neg(y = x)).$$

Dit is bijv. equivalent met

$$\exists_{y\in S}\ \exists_{z\in S}\ (P(y) \wedge P(z) \wedge \neg(y = z)) \quad \vee \quad (S \text{ leeg})$$

maar het is een heel werk om dat formeel te laten zien.

3.16. Implicaties bij rijen van kwantoren

Neem aan dat als $x \in S$, $y \in S$, $z \in S$, door $P(x,y,z)$ en $Q(x,y,z)$ proposities worden voorgesteld, en dat $P(x,y,z) \rightarrow Q(x,y,z)$ kan worden afgeleid. Stel de propositie

$$\forall_{x\in S}\ \exists_{y\in S}\ \forall_{z\in S}\ P(x,y,z)$$

door p voor, en het overeenkomstige ding met $Q(x,y,z)$ door q. Dan is ook $p \rightarrow q$ afleidbaar. Hetzelfde geldt voor andere series kwantoren.

3.17. Volgordeverwisseling van kwantoren

Laat R een relatie zijn die aan elk paar (s,t) met $s \in S$, $t \in T$ een propositie toevoegt. Dan gelden

$$\forall_{x \in S} \forall_{y \in T} R(x,y) \Leftrightarrow \forall_{y \in T} \forall_{x \in S} R(x,y)$$

$$\exists_{x \in S} \exists_{y \in T} R(x,y) \Leftrightarrow \exists_{y \in T} \exists_{x \in S} R(x,y)$$

$$\exists_{x \in S} \forall_{y \in T} R(x,y) \rightarrow \forall_{y \in T} \exists_{x \in S} R(x,y)$$

maar in het laatste geval mag in het algemeen de $\rightarrow$ niet door $\Leftrightarrow$ vervangen worden. Merk op dat

"er is een deksel dat op elk potje past" $\rightarrow$ "op elk potje past een deksel"

maar niet omgekeerd. Uit het feit dat er op elk potje een deksel past, volgt niet dat er een universeel deksel voor alle potjes is.

HOOFDSTUK 4. DE WAARDERINGSMETHODE IN DE PROPOSITIELOGICA

4.1. Inleiding

In onze propositielogica werkten we met logische formules, opgebouwd uit propositievariabelen, propositieconstanten en connectieven. We zullen een waarderingssysteem aangeven waarbij aan logische formules waarden 0 of 1 kunnen worden toegekend.

Zo'n waardering is vastgelegd, doordat we een waarde (0 of 1) van elke propositievariabele en van elke propositieconstante kiezen. Deze waardering wordt dan voortgezet tot de verzameling van alle logische formules.

We beperken ons tot één enkele propositieconstante, nl. de contradictie F. Deze geven we steeds de waarde 0.

Laten we de letter w gebruiken om een waardering aan te geven. Voor elke logische formule f is nu w(f) de waarde ervan, dus w(f) = 0 of 1. In het bijzonder is w(F) = 0.

We hebben eigenlijk maar met twee connectieven te maken, nl. $\rightarrow$ en $\wedge$ (de connectieven $\neg$, $\vee$ en $\Leftrightarrow$ zijn met behulp van $\rightarrow$ en $\wedge$ opgebouwd).

We nemen aan dat de logische formules f en g reeds gewaardeerd zijn, d.w.z. dat w(f) en w(g) al bepaald zijn. We gaan nu zeggen wat $w(f \rightarrow g)$ en $w(f \wedge g)$ zijn. Dat geven we aan met z.g. waarheidstafels:

w(f) \ w(g)	0	1
0	0	0
1	0	1

$w(f \wedge g)$

w(f) \ w(g)	0	1
0	1	1
1	0	1

$w(f \rightarrow g)$

Dit betekent bijv.: als w(f) = 0, w(g) = 1, dan is $w(f \wedge g) = 0$, $w(f \rightarrow g) = 1$.

Uitgaande van w(a), w(b), ... (waarin a, b, ... de propositievariabelen zijn), elk 0 of 1, kunnen we nu voor elke logische formule de waarde uitrekenen.

Vervolgens de uit $\rightarrow$ en $\wedge$ afgeleide connectieven.

Eerst de ontkenning: $\neg f$ stelt $f \rightarrow F$ voor, dus daar w(F) = 0 is $w(\neg f) = 0$ als w(f) = 1 en $w(\neg f) = 1$ als w(f) = 0 (beide uit de eerste kolom van de tafel voor $\rightarrow$).

Vervolgens de disjunctie $f \vee g$, gedefinieerd als $(\neg f) \rightarrow g$. We maken de volgende lijst van mogelijkheden:

$w(f)$	$w(g)$	$w(\neg f)$	$w((\neg f) \rightarrow g)$
0	0	1	0
0	1	1	1
1	0	0	1
1	1	0	1

en hieruit volgt de waarheidstafel voor de disjunctie:

$w(f)$ \ $w(g)$	0	1
0	0	1
1	1	1

$w(f \vee g)$

(dus $w(f \vee g) = 0$ wanneer en slechts wanneer $w(f) = w(g) = 0$).

We doen hetzelfde met de equivalentie (bedenk dat $f \Leftrightarrow g$ gedefinieerd is als $(f \rightarrow g) \wedge (g \rightarrow f)$).

$w(f)$	$w(g)$	$w(f \rightarrow g)$	$w(g \rightarrow f)$	$w(f \Leftrightarrow g)$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

De waarheidstafel voor de equivalentie wordt dus

w(f) \ w(g)	0	1
0	1	0
1	0	1

$w(f \Leftrightarrow g)$

(dus $w(f \Leftrightarrow g) = 1$ wanneer en slechts wanneer $w(f) = w(g)$).

4.2. Afleidbaarheid en waarde

Men kan het systeem van waarderingen gebruiken om van een gegeven logische formule f vast te stellen of die al dan niet tautoloog is. Daarom kan men het systeem van waarderingen als een afleidingsmethodiek gebruiken. Dat wil nog niet zeggen dat het afleiden van logische formules daarmee sneller, inzichtelijker of aantrekkelijker is geworden.

Als we in het vervolg spreken over "elke waardering w" dan heeft dat betrekking op alle waarderingen waarvoor $w(F) = 0$. Zo'n w is, wat f betreft, vastgelegd door de waarden die w heeft op de propositievariabelen die werkelijk in f optreden (bedenk dat F onze enige propositieconstante is). Als er n propositievariabelen in f voorkomen, is dus het aantal te beschouwen w's gelijk aan 2^n.

We komen nu tot het verband tussen waarderingen en afleidbaarheid.

Stelling 1 (Waarderingsstelling).

Als de logische formule f bij elke waardering de waarde 1 heeft, dan is f afleidbaar. Als er een waardering is waarbij $w(f) = 0$, dan is f niet afleidbaar.

We bewijzen deze stelling hier niet, ofschoon het niet onoverkomelijk moeilijk zou zijn. Wel moeten we bedenken dat het bewijzen van deze stelling een andere activiteit is dan het construeren van afleidingen voor onze logische formules.

We geven een toepassing. De vraag is of de propositie

$$(a \vee b) \rightarrow (c \vee (a \wedge b))$$

afleidbaar is. We noemen de formule f, en maken een lijst met de 8 gevallen die door de combinaties van waarden voor w(a), w(b) en w(c) worden opgeleverd.

w(a)	w(b)	w(c)	w(a ∨ b)	w(a ∧ b)	w(c ∨ (a ∧ b))	w(f)
0	0	0	0	0	0	1
1	0	0	1	0	0	0
0	1	0	1	0	0	0
1	1	0	1	1	1	1
0	0	1	0	0	1	1
1	0	1	1	0	1	1
0	1	1	1	0	1	1
1	1	1	1	1	1	1

De laatste kolom bestaat niet geheel uit enen, en volgens onze stelling is f dus niet afleidbaar.

Een ander voorbeeld: de formule van Peirce $((a \to b) \to a) \to a$:

w(a)	w(b)	w(a → b)	w((a → b) → a)	w(f)
0	0	1	0	1
1	0	0	1	1
0	1	1	0	1
1	1	1	1	1

Conclusie: daar de laatste kolom geheel uit enen bestaat is f een tautologie.

Met een beetje handigheid kan men zich heel wat werk bij deze tabellen besparen. Het gaat er immers niet om de laatste kolom geheel te bepalen: het is alleen van belang te weten of er al dan niet een nul in voorkomt. Als men zich erop gaat toeleggen dit handig te doen, komt men tot een methodiek die erg op die van onze natuurlijke deductie gaat lijken. We zullen er geen studie van maken.

4.3. Verdere stellingen over waarderingen

De waarderingsstelling leidt gemakkelijk tot verdere stellingen, waarvan we er enkele noemen:

Stelling 2.

Een equivalentie $f \leftrightarrow g$ is een tautologie wanneer en slechts wanneer $w(f) = w(g)$ voor alle waarderingen w.

Stelling 3

Een implicatie $f \rightarrow g$ is een tautologie wanneer en slechts wanneer $w(f) \leq w(g)$ voor alle waarderingen w.

Stelling 4

De logische formule g is in de context van de onderstellingen $f_1,\ldots,f_k$ afleidbaar wanneer en slechts wanneer $w(g) = 1$ voor elke waardering die aan $w(f_1) = \ldots = w(f_k) = 1$ voldoet.

We geven een voorbeeld van het gebruik van stelling 4. Gevraagd wordt of in de onderstelling $a \leftrightarrow b$ de formule $(a \rightarrow c) \leftrightarrow (b \rightarrow c)$ is af te leiden.

Een waardering w waarvoor $w(a \leftrightarrow b) = 1$ is, voldoet aan $w(a) = w(b)$ (zie waarheidstafel voor $\leftrightarrow$). Doordat w(a) en w(b) dezelfde waarde hebben, zullen ook $w(a \rightarrow c)$ en $w(b \rightarrow c)$ dezelfde waarde hebben. Weer volgens de waarheidstafel van $\leftrightarrow$ zien we dat $(a \rightarrow c) \leftrightarrow (b \rightarrow c)$ de waarde 1 heeft. Bij deze redenering hebben we de afzonderlijke w's niet behoeven te bekijken.

Opmerking bij stelling 4. Als men in een toepassing van stelling 1 een w heeft gevonden met $w(f) = 0$, dan is dat bijv. een w met $w(a) = 0$, $w(b) = 1$, $w(c) = 0$ (zie de derde regel in het eerste voorbeeld bij stelling 1). Nu zegt stelling 4 dat onder de onderstellingen $\neg a$, b en $\neg c$ de formule $\neg f$ is af te leiden.

4.4. Contradictievrijheid

Uit stelling 1 volgt dat de contradictie F niet in de lege context is af te leiden. Anders gezegd: F is geen tautologie. Het klinkt wat merkwaardig omdat er in F geen propositievariabelen voorkomen. Niettemin spelen propositievariabelen in deze uitspraak een rol: men zou toch kunnen denken dat men via allerlei propositievariabelen alsnog tot een afleiding van F zou kunnen komen.

TECHNISCHE HOGESCHOOL EINDHOVEN

Onderafdeling der Wiskunde en Informatica

AANVULLINGEN INLEIDING LOGICA

door

Prof.dr. N.G. de Bruijn

Tweede druk 1984

INHOUDSOPGAVE

WOORD VOORAF

Deze "aanvullingen" werden nodig toen in mei 1983 besloten werd de omvang van het college Logica in het 1^e trimester voor Informatica-studenten van 2 op 4 uur per week te brengen. De in 1982 gebruikte syllabus was op dat ogenblik reeds herdrukt, zodat moest worden gekozen voor het maken van een serie "aanvullingen"; het was niet meer mogelijk de beide delen tot één geheel te verwerken.

Hoewel in deze "aanvullingen" het begrip "hoofdstuk" niet steeds meer de afgeronde betekenis heeft die het in de syllabus Inleiding Logica 1982 had, is terwille van de eenheid in het verwijzingssysteem de indeling in hoofdstukken en paragrafen voortgezet.

TOEVOEGING AAN DE SYLLABUS INLEIDING LOGICA

blz. 42 : Na bovenste 7 regels, toevoegen:

Deze afleiding gebruikt DBNG niet, maar dat is wèl het geval met de hier volgende afleiding van de omkering, d.i. van $(\neg b) \to (\neg a)$ naar $a \to b$:

1	$\boxed{(\neg b) \to (\neg a)}$		
2	$\quad \boxed{a}$		
3	$\qquad \boxed{\neg b}$		
4	$\qquad \neg a$	EL→	(1,3)
5	$\qquad F$	EL→	(4,2)
6	$\quad \neg\neg b$	IN→	(5)
7	$\quad b$	DBNG	(6)
8	$a \to b$	IN→	(7)

Aanvulling aan het slot van 3.13:

Meestal wordt een opgave over limieten volgens het volgende schema opgelost.

$n \in \mathbb{N}$

a_n := <gegeven door steller>

b := <gegeven door steller of geraden door oplosser>

$\varepsilon \in \mathbb{P}$

$m(\varepsilon)$:= <gekozen door oplosser>

$n \in \mathbb{N}(m(\varepsilon))$

<bewijs gegeven door oplosser>

$|a_n - b| < \varepsilon$

Door achtereenvolgens IN∀, IN∃ en IN∀ toe te passen blijkt dat de rij de limiet b heeft; door daarna nog eens IN∃ te gebruiken zien we dat de rij convergent is.

In het bovenstaande betekent $\mathbb{P}$ de verzameling der positieve reële getallen, en $\mathbb{N}(m(\varepsilon))$ die van de gehele getallen groter dan $m(\varepsilon)$.

66_3: "predikaat van twee variabelen" moet zijn "predikaat op een verzameling die een cartesisch produkt van twee verzamelingen is".

(Zie voor "cartesisch produkt" 7.4.)

HOOFDSTUK 5. BINDING

5.1. Notaties van bindingsformules (Toevoeging aan par. 1.9 en par. 3.2.)

De bindingsformules uit de wiskunde kunnen alle worden voorgesteld door een unaire operator te laten werken op hetzij een functie hetzij een predikaat. Die functie of dat predikaat kunnen in een plaatje als Fig. 20 (in par. 3.2) worden voorgesteld. In een lijstje volgen hier wat voorbeelden. Steeds staat links een door ons gestyleerde vorm, rechts de gangbare. De (voor de hand liggende) operatornamen ("som, prod,...") zijn zeker niet algemeen gangbaar.

A. Gevallen waarbij de unaire operator op een functie werkt.

$\mathrm{som}(\lambda_{k\in \mathrm{int}(1,5)}\,(k+1))$	$\sum\limits_{k=1}^{5} (k+1)$
$\mathrm{prod}(\lambda_{k\in \mathrm{int}(1,5)}\,(k+1))$	$\prod\limits_{k=1}^{5} (k+1)$
$\mathrm{integr}(\lambda_{x\in[a,b]}\,(x+1))$	$\int_a^b (x+1)\,dx$
$\mathrm{beeld}(\lambda_{x\in[a,b]}\,(x^2+1))$	$\{x^2+1 \mid x \in [a,b]\}$

We zullen later nog "union" en "intersection" bespreken (7.11).

B. Gevallen waarbij de unaire operator op een predikaat werkt.

alle $(\lambda_{x\in[0,1]}(x+1<8))$	$\forall_{x\in[0,1]}\, x+1<8$ (voor alle x in [0,1] is ...)
er is $(\lambda_{x\in[0,1]}(x+1<8))$	$\exists_{x\in[0,1]}\, x+1<8$ (er is een x in [0,1] met ...)
er is precies één $(\lambda_{x\in[0,1]}(x+1<8))$	$\exists^{1}_{x\in[0,1]}\, x+1<8$ (er is precies één x in [0,1] met ...)
verz$(\lambda_{x\in[0,1]}(8x+1<2))$	$\{x \in [0,1] \mid 8x+1<2\}$ (de verzameling der x uit [0,1] met ...)
card$(\lambda_{x\in[0,1]}(8x^2-8x+1=0))$	$\#_{x\in[0,1]}(8x^2-8x+1=0)$ (het aantal x uit [0,1] met ...)
indiv$(\lambda_{x\in[0,1]}8x^2=1)$	$\downarrow_{x\in[0,1]} 8x^2=1$ (de x uit [0,1] met ...)

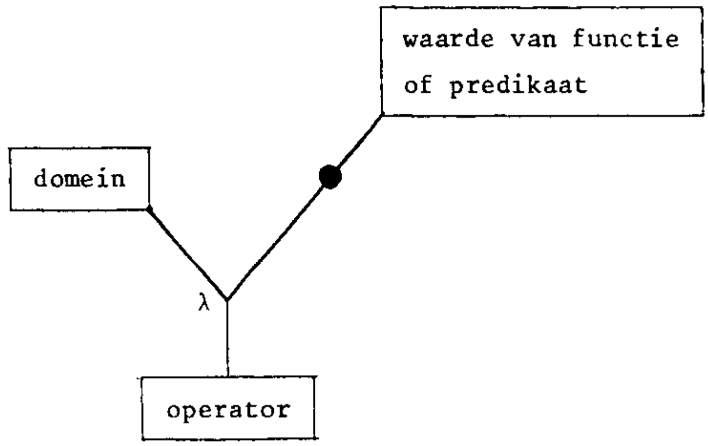
5.2. Opmerkingen

1. De notatie met $\downarrow$ is voorgesteld door Freudenthal maar niet algemeen gangbaar.
2. In plaats van λ heeft Freudenthal voorgesteld $\curlyvee$.
3. Als S een verzameling met precies één element is, dan duidt jota (S) dat element aan. (Zie 7.9.) In plaats van indiv(...) kan dan ook geschreven worden jota (verz(...)).

4. In plaats van "alle" was in 3.2 gebruikt ∀.
5. Men kan natuurlijk ook alle hier besproken unaire operatoren direct op een door één enkel symbool gegeven functie of predikaat laten werken: som(F), beeld(F), card(P), etc.

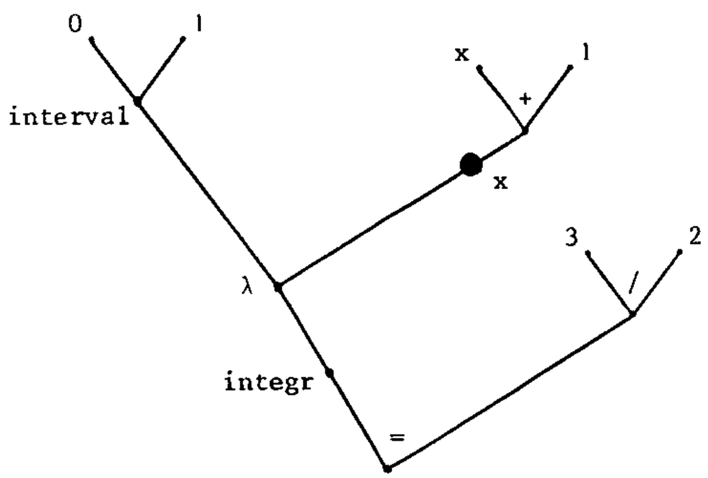
5.3. Notatie in boomvorm

Het systeem is

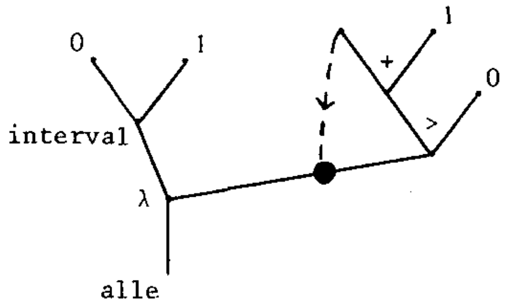


Voorbeelden

1. $\int_0^1 (x+1)dx = 3/2$ wordt voorgesteld door



2. "Voor alle x in [0,1] geldt x + 1 > 0" wordt voorgesteld door

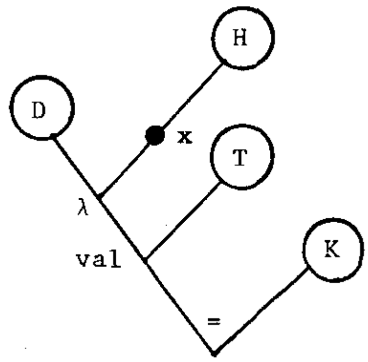


5.4. Functiewaarden

Het is niet altijd veilig om de waarde van de functie f in het punt a door f(a) aan te duiden. Als f meer is dan een enkele identificator (zoals sin, ln) kan het moeilijkheden opleveren. Het zou veiliger zijn een vaste binaire operator "val" (van "value") hiervoor te reserveren en val(f,a) te schrijven in plaats van f(a). Zo krijgen we gelijkheden als

$$\mathrm{val}(\lambda_{x \in S}(x/2),\ a+b) = (a+b)/2\ .$$

Merk op dat dit algemeen wordt uitgedrukt in boomvorm door



(D, H, T, K stellen bomen voor), waarbij K de boom is die uit H ontstaat door elke x door de boom T te vervangen.

5.5. Lambda calculus

Lambda calculus houdt zich bezig met de studie van λ-formules. In 3.2 en 5.3 hebben we gezien hoe λ-formules boomvormig getekend kunnen worden en in het bijzonder hoe de bindingen kunnen worden aangegeven.

We nemen nog even een voorbeeld: de formule

$$\lambda_{x \in S}\,(x^2 + x)$$

geeft de functie aan met domein S, en voor elke x uit het domein is de functiewaarde $x^2 + x$. Is bijv. $a + b \in S$, dan is die waarde genoteerd als

$$\mathrm{val}(\lambda_{x \in S}\,(x^2 + x),\ (a + b))$$

en dat is gelijk aan $(a + b)^2 + (a + b)$.

Als men een theorie over formules beschrijft moet men zeggen dat bijv.

$$\mathrm{val}(\lambda_{x \in S}\, f(x\ ,\ g(x))\ ,\ p(a,b)) \tag{1}$$

een andere formule is dan

$$f(p(a,b)\ ,\ g(p(a,b)))\ , \tag{2}$$

al is het dan misschien onze bedoeling om te gaan zeggen dat (1) en (2) "dezelfde waarde" hebben. We noemen de overgang van (1) naar (2) "beta-reductie". De letternaam "beta" is gekozen door A. Church ("The Theory of Lambda Conversion", Annals of Math. Studies 6, Princeton Univ. Press, 1941), die ook nog bijv. "alpha-reductie", "eta-reductie" gebruikte.

Meestal laat men de typeringen weg als men lambda calculus bestudeert ("ongetypeerde lambda calculus"), en men schrijft de formules bijv. in de vorm $\lambda x \cdot f(x, g(x))(p(a,b))$, maar wij zullen hier de stijl

$$\mathrm{val}(\lambda_x f(x, g(x)), p(a,b))$$

aanhouden.

In het algemeen is beta-reductie als volgt te beschrijven: laat F en G formules zijn; F mag de letter x bevatten. Laat H de formule zijn die ontstaat door in F alle x'en door G te vervangen. Dan is de overgang van

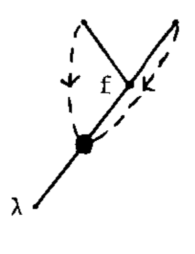
$$\mathrm{val}(\lambda_x F, G) \qquad \text{naar } H$$

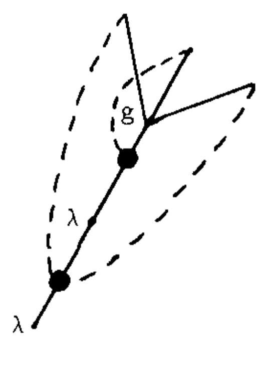
beta-reductie.

Beta-reductie kan ook ergens binnenin plaatsvinden ("interne reductie"), doordat de $\mathrm{val}(\lambda_x F, G)$ waarop de beta-reductie wordt toegepast, een fragment van een grotere formule is.

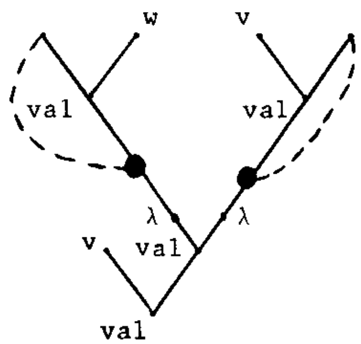
We zullen ons op het standpunt stellen dat de λ-formules eigenlijk met referentiepijlen (als in Figuur 14, §1.9) bedoeld zijn; de notatie met namen voor de binders dient alleen voor de leesbaarheid. Dus $\lambda_x f(x,x)$ is <u>dezelfde</u> formule als $\lambda_y f(y,y)$, en $\lambda_x \lambda_y g(x,y,x)$ is <u>dezelfde</u> formule als $\lambda_y \lambda_x g(y,x,y)$.

We tekenen ze als

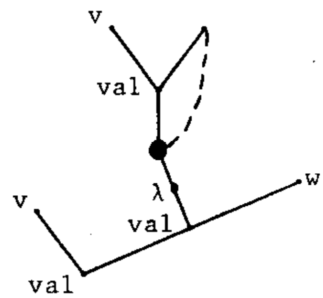




(In deze voorbeelden komen nog operatoren f, g voor, hoewel men zich in de lambda calculus meestal beperkt tot formules zonder dergelijke operatoren, met als enige uitzondering "val".) In de formules mogen nog wel vrije variabelen voorkomen, zoals v en w bij de volgende beta-reductie:



gaat door (interne) beta-reductie over in



In de vorm van formules is het de reductie van

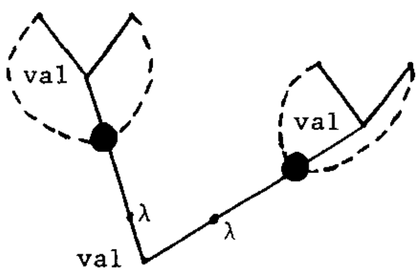
$$\mathrm{val}(v\ ,\ \mathrm{val}(\lambda_x\, \mathrm{val}(x,w)\ ,\ \lambda_y\, \mathrm{val}(v,y)))$$

naar

$$\mathrm{val}(v\ ,\ \mathrm{val}(\lambda_y\, \mathrm{val}(v,y)\ ,\ w))\ .$$

Men stelt zich misschien voor dat beta-reductie de formule vereenvoudigt, maar dat kan tegenvallen doordat er bij de overgang van val(λ_x F , G) naar de H (die uit F ontstaat door x overal door G te vervangen), er veel x'en in F voorkomen, terwijl G een lange formule is. Dan is H langer dan wat we eerst hadden.

Men hoopt vaak door herhaalde reducties een z.g. normaalvorm te bereiken, d.i. een vorm die geen verdere beta-reducties toelaat. Een bekend voorbeeld van Church laat zien dat dit niet altijd lukt: De formule



laat één beta-reductie toe, en daarmee gaat de formule in zichzelf over!

Dit soort formules komt in de gewone wiskundige praktijk niet voor! De eisen die men stelt ten aanzien van typeringen sluiten dingen als val(x,x) uit.

Een centrale stelling uit de lambda calculus is de stelling van Church-Rosser. Laat F, G, H λ-formules zijn, en wel zó dat er een serie (van nul of meer) beta-reducties is die F in G overvoert en ook een serie die F in H overvoert. Dan is er een λ-formule K zó dat zowel G als H door series (van nul of meer) beta-reducties in K kunnen worden overgevoerd.

Uit de stelling van Church-Rosser volgt: als een λ-formule via beta-reducties tot een normaalvorm kan worden gereduceerd, dan kan die λ-formule niet tot nog een andere normaalvorm worden gereduceerd. (Noem die twee normaalvormen G en H en pas de stelling van Church-Rosser toe.)

Als uitgewerkt voorbeeld geven we een stelling van Turing die uitspreekt dat er bij elke λ-formule F een λ-formule X is zó dat X door beta-reducties in val(F,X) kan overgaan. Als men bij F aan een functie denkt en val(F,X) als de waarde van de functie in het punt X interpreteert, wordt het een "fixed-point stelling" (een stelling van de vorm: "Er is een X die door de gegeven afbeelding F niet veranderd wordt").

Sterker nog: er is een universele λ-formule G zó dat voor elke F de λ-formule val(G,F) het probleem oplost, d.w.z. dat

$$\mathrm{val}(G,F) \quad \text{in} \quad \mathrm{val}(F\,,\mathrm{val}(G,F))$$

kan overgaan door een serie beta-reducties. We nemen

$$\lambda_x \lambda_y \mathrm{val}(y\,,\mathrm{val}(\mathrm{val}(x,x)\,,y))$$

en korten dat af tot H, en val(H,H) korten we af tot G. De F zelf is de afkorting van de een of andere (volledig willekeurige) λ-formule. Eerst zien we dat G door beta-reductie overgaat in

$$\lambda_y \mathrm{val}(y\,,\mathrm{val}(\mathrm{val}(H,H)\,,y))\,,$$

dus val(G,F) gaat door (interne) beta-reductie over in

$$\mathrm{val}(\lambda_y \mathrm{val}(y\,,\mathrm{val}(\mathrm{val}(H,H)\,,y))\,,F)\,.$$

Dit laatste laat wéér beta-reductie toe, en leidt tot

$$\mathrm{val}(F\,,\mathrm{val}(\mathrm{val}(H,H)\,,F))$$

en dat is, doordat met val(H,H) dezelfde formule bedoeld is als G, hetzelfde als val(F , val(G,F)).

HOOFDSTUK 6. NOG WAT UIT DE PROPOSITIELOGICA

6.1. De Sheffer-streep

In de klassieke logica werken we met de connectieven $\neg$, $\wedge$, $\vee$, $\rightarrow$ en $\leftrightarrow$, maar het kan ook met minder, omdat op grond van de tautologieën van de klassieke logica allerlei connectieven in andere kunnen worden uitgedrukt. Men kan bijv. met $\neg$ en $\rightarrow$ volstaan.

Het is ook mogelijk alles te doen met één enkel connectief, de Sheffer-streep. Als x en y proposities zijn, is $x|y$ een afkorting voor $\neg(x \wedge y)$. Men spreekt ook wel over "nand" (not and). Nu is bijv. $x|x$ equivalent met $\neg x$, en men kan nu alle andere connectieven eveneens voorstellen. Het is verre van overzichtelijk of elegant, maar het kan. We geven even een compleet overzicht bij twee letters. Links staan de definities, rechts equivalenten in ons meer vertrouwde vorm. De nummering van de afkortingssymbolen a0,a1,... is afkomstig van codering van de waarheidstafels. De waarheidstafel voor $x \rightarrow y$ heeft in de eerste rij 11 en in de tweede 01; we voegen er daarom het rijtje 1101 aan toe, en coderen dit door het als een binair getal te lezen, dus met 8 + 4 + 1, d.i. 13.

a3	:=	x			x
a5	:=	y			y
a12	:=	a3|a3	=	$x\|x$	$\neg x$
a10	:=	a5|a5	=	$y\|y$	$\neg y$
a14	:=	a3|a5	=	$x\|y$	$\neg(x \wedge y)$
a13	:=	a3|a14	=	$x \mid (x\|y)$	$x \rightarrow y$
a15	:=	a3|a12	=	$x \mid (x\|x)$	T
a11	:=	a5|a12	=	$y \mid (x\|x)$	$y \rightarrow x$
a7	:=	a10|a12	=	$(y\|y) \mid (x\|x)$	$x \vee y$
a1	:=	a14|a14	=	$(x\|y) \mid (x\|y)$	$x \wedge y$
a4	:=	a11|a11	=	$(y \mid (x\|x)) \mid (y \mid (x\|x))$	$\neg(y \rightarrow x)$
a2	:=	a13|a13	=	$(x \mid (x\|y)) \mid (x \mid (x\|y))$	$\neg(x \rightarrow y)$
a0	:=	a15|a15	=	$(x \mid (x\|x)) \mid (x \mid (x\|x))$	F
a6	:=	a11|a13	=	$(y \mid (x\|x)) \mid (x \mid (x\|y))$	$\neg(x \Leftrightarrow y)$
a9	:=	a7|a14	=	$((y\|y) \mid (x\|x)) \mid (x\|y)$	$x \Leftrightarrow y$
a8	:=	a7|a15	=	$((y\|y) \mid (x\|x)) \mid (x \mid (x\|x))$	$\neg(x \vee y)$

Voor ons is de Sheffer-streep op dit ogenblik niet meer dan een curiositeit en een gelegenheid om met connectieven te oefenen.

6.2. Rekenen in GF(2)

Ons uitgangspunt is dat we van twee gehele getallen u en v kunnen zeggen of som u + v en product uv even resp. oneven zijn zodra we dit van u en v weten. We zeggen kortweg: even + even = even, even + oneven = oneven, oneven + oneven = even, even × even = even, even × oneven = even, oneven × oneven = oneven. Als we ter afkorting "even" door 0 en "oneven" door 1 vervangen dan geldt voor het systeem van de twee elementen 0 en 1:

$$0 + 0 = 0 \qquad 0 + 1 = 1$$
$$1 + 0 = 1 \qquad 1 + 1 = 0$$
$$0 \times 0 = 0 \qquad 0 \times 1 = 0$$
$$1 \times 0 = 0 \qquad 1 \times 1 = 1 .$$

Dit wordt GF(2) genoemd (Galois-lichaam met 2 elementen). Voor alle x uit {0,1} geldt

$$x + x = 0 , \qquad x \times x = x .$$

Verder hebben we de gewone rekenregels voor de optelling en vermenigvuldiging, zoals bijv.

$$x + (y+z) = (x+y) + z$$
$$x(y+z) = xy + xz$$
$$x + 0 = x$$
$$x \times 1 = x .$$

Deze regels zijn gemakkelijk te begrijpen op grond van het rekenen met even en oneven gehele getallen.

We gaan nu een systeem van waardering invoeren voor proposities, waarbij aan elke propositie a als waarde v(a) wordt toegekend, gekozen uit de verzameling $\{0,1\}$. We geven (in tegenstelling tot de zaak bij w) aan geldige proposities de v-waarde 0, en aan ongeldige de v-waarde 1. Dus

$$w(a) = 1 - v(a)$$

voor alle proposities a. Nu blijkt dat

$$v(a \wedge b) = v(a)\,v(b) + v(a) + v(b)$$
$$v(a \to b) = (v(a) + 1)\,v(b) .$$

Ter afkorting laten we de v gewoon weg, en schrijven dus

$$a \wedge b = ab + a + b$$
$$a \to b = ab + b$$
$$F = 1 .$$

Een afleidbare formule, d.i. een formule f met $w(f) = 1$, krijgt in het nieuwe systeem de waarde 0.
Om te zien of iets een tautologie is, gaan we dus proberen de formule "op nul te herleiden".

Voorbeeld. $a \to (b \to a)$.

De v-waarde van $b \to a$ is $ba + a$, die van $a \to (b \to a)$ dus $(a+1)(b+1)a$, maar dit is nul omdat $(a+1)a = 0$.

We gaan vervolgens de afgeleide connectieven bekijken. We vinden

$$\neg a = a \to F = (a+1)1 = a + 1$$

$$a \vee b = (\neg a) \to b = (a+1+1)b = ab$$

$$a \leftrightarrow b = (a \to b) \wedge (b \to a) = (ab+b)(ba+a) + ab + b + ab + a = a + b .$$

We kunnen nu alle op tautologie te onderzoeken formules snel doorrekenen. Bijv.

$$((a \to b) \to (\neg a)) \leftrightarrow (\neg a) \vee (\neg b) .$$

Het linkerlid herleiden we als $(ab+b+1)(a+1) = ab + ab + a + ab + b + 1 = $ $= ab + a + b + 1 = (a+1)(b+1)$ en het rechterlid geeft hetzelfde. Het feit dat beide leden hetzelfde opleveren garandeert de equivalentie: $p \leftrightarrow q$ is te herleiden tot $p + q$ en dat is nul als $p = q$.

We kunnen ons systeem ook gebruiken om uitdrukkingen te vereenvoudigen.

Voorbeeld

We korten af $p := (a \vee b) \wedge (c \vee d)$, $q := a \vee c \vee (b \wedge d)$ en willen $p \to q$ onderzoeken. We berekenen

$$p = (ab)(cd) + ab + cd$$

$$q = ac(bd+b+d) .$$

We zien dat

$$q = pac .$$

Dit leert dat $(p+1)q = 0$, dus dat $p \to q$, maar ook dat q equivalent is met $p \vee a \vee c$, dus

$$((a \vee b) \wedge (c \vee d)) \vee a \vee c \leftrightarrow a \vee c \vee (b \wedge d) .$$

We kunnen een overzicht krijgen van alle logische uitdrukkingen met bijv. drie letters. Elke logische formule in termen van x, y, z is te herleiden tot een der veeltermen

$$a_1xyz + a_2xy + a_3xz + a_4yz + a_5x + a_6y + a_7z + a_8$$

waarin elk der coëfficiënten $a_1, \dots, a_8$ de waarde 0 of 1 kan hebben. Er zijn dus 2^8 mogelijkheden en elke logische uitdrukking in x, y, z is met één van deze 256 uitdrukkingen equivalent.

Voor twee letters, a en b, volgt hier een lijstje van alle gevallen. Het zijn er 2^4.

$T = 0$	$F = 1$
$a = a$	$\neg a = 1 + a$
$b = b$	$\neg b = 1 + b$
$a \Leftrightarrow b = a + b$	óf a óf b $= 1 + a + b$
$a \vee b = ab$	$(\neg a) \wedge (\neg b) = 1 + ab$
$b \rightarrow a = a + ab$	$b \wedge (\neg a) = 1 + a + ab$
$a \rightarrow b = b + ab$	$a \wedge (\neg b) = 1 + b + ab$
$a \wedge b = a + b + ab$	$\neg(a \wedge b) = 1 + a + b + ab$

We noemen nog twee uitdrukkingen met drie letters. Eerst

<u>if</u> a <u>then</u> b <u>else</u> c := a(b + c) + b .

Het linkerlid zou men kunnen definiëren als

$$(a \rightarrow b) \wedge (\neg a \rightarrow c) .$$

De tweede is

$$\text{trichotomie}(a , b , c) := abc + ab + ac + bc + 1 .$$

De betekenis hiervan is: van de proposities a, b, c is er precies één geldig. Zo geldt bijvoorbeeld voor alle x en y in $\mathbb{R}$:

$$\text{trichotomie}(x > y , x < y , x = y) .$$

HOOFDSTUK 7. VERZAMELINGEN EN AFBEELDINGEN

7.1. Inleiding

Aan de basis van de wiskunde moeten we een stel afspraken leggen over de manier waarop we met verzamelingen en afbeeldingen omgaan. De meest gangbare verzamelingstheorie is die van Zermelo-Fraenkel (afgekort tot ZF), die in het begin van deze eeuw werd gebouwd om de aan het eind van de 19de eeuw door Cantor opgezette verzamelingstheorie een hechte grondslag te geven, met vermijding van de rond de eeuwwisseling ontdekte paradoxen (zoals die van Russell, zie 7.14).

De meeste wiskundigen zullen, wanneer men er naar vraagt, zeggen dat hun wiskunde op ZF is gebouwd, maar doorgaans zijn ze niet gewend zich bij het wiskundige bedrijf rekenschap af te leggen van de manier waarop het dan wel uit ZF volgt. In feite zou alles wat ze doen ook op geheel andere systemen kunnen wortelen.

Het is er ons in deze cursus niet om begonnen inzicht te geven in de structuur van een axiomatisch systeem dat de wiskunde fundeert, maar wel om de student vertrouwd te maken met de gangbare werkwijzen betreffende verzamelingen en afbeeldingen. We doen geen enkele poging die tot ZF terug te brengen. Een aantal belangrijke grondeigenschappen zullen we axioma's noemen, zoals die over cartesische producten (zie 7.4), machtsverzameling (zie 7.5), gelijkheidsaxioma's (zie 7.8) en individualiteit (zie 7.9), hoewel ze bij een ZF-opbouw niet alle de rol van axioma's spelen.

Los van deze axioma's staat het keuzeaxioma (zie 7.13) dat niet tot het "standaardpakket" behoort: men is min of meer vrij het al dan niet aan te hangen.

7.2. Verzamelingen

Het staat voor ons vast dat er gesproken kan worden over verzamelingen. Een verzameling kan element zijn van een andere verzameling. Als A en B verzamelingen zijn, dan zijn $A \in B$ en $A = B$ proposities.

Door de fundamentele proposities van de vormen $A \in B$ en $A = B$ op alle mogelijke manieren te verbinden via logische connectieven en kwantoren ontstaat een grote klasse van proposities en predikaten waarmee we ons wiskundige bedrijf uitoefenen.

Een predikaat op een verzameling S is een afbeelding P die aan iedere x met $x \in S$ een propositie $P(x)$ toevoegt. Voorbeelden van predikaten zijn (vooruitlopende op 7.8) $\lambda_{x \in S}(x = x)$, $\lambda_{x \in S}(x = S)$, $\lambda_{x \in S}(\neg(S = S) \vee \neg(x = x))$.

Een belangrijke regel is dat er bij zo'n predikaat P gesproken kan worden over de verzameling van alle elementen van S die aan P voldoen. De gebruikelijke notatie hiervoor is

$$\{x \in S \mid P(x)\}.$$

(Omdat deze notatie onze gebruiken over het noteren van kwantoren geweld aandoet, heeft Freudenthal voorgesteld $\uparrow_{x \in S} P(x)$ te gebruiken, maar dat is niet algemeen gangbaar.) We hebben de equivalentie

$$(y \in S \wedge P(y)) \Leftrightarrow y \in \{x \in S \mid P(x)\}. \qquad (1)$$

voor alle y.

Verder dienen we te vermelden dat er, als A en B verzamelingen zijn, een verzameling is die de vereniging van A en B wordt genoemd, met $A \cup B$ wordt genoteerd en gekenmerkt is door

$$((x \in A) \vee (x \in B)) \Leftrightarrow (x \in A \cup B)$$

voor alle x.

7.3. Voortgezette opbouw

Als A en B verzamelingen zijn definiëren we de propositie $A \subset B$ als $\forall_{x \in A}\, x \in B$.

Een belangrijk axioma is dat van de extensionaliteit: als $A \subset B \wedge B \subset A$, dan is $A = B$.

Als A en B verzamelingen zijn dan is de doorsnede $A \cap B$ gedefinieerd als

$$\{x \in A \mid x \in B\}.$$

Elk element y van deze verzameling voldoet aan $(y \in A) \wedge (y \in B)$ en elke y die daaraan voldoet is element van $A \cap B$ (zie (1) uit (7.2)). Derhalve is $A \cap B = B \cap A$.

Het verschil $A \backslash B$ is te definiëren als $\{x \in A \mid \neg(x \in B)\}$ en het symmetrische verschil $A \div B$ als $(A \backslash B) \cup (B \backslash A)$.

Bijna steeds hebben we te maken met gevallen van $A \cup B$, $A \cap B$, $A \backslash B$, $A \div B$, $A = B$, $A \subset B$ waarbij A en B gegeven zijn als deelverzamelingen van een verzameling S (die soms voor lange tijd vast is, en wel het <u>universum</u> genoemd wordt). In dat geval hebben we predikaten P, Q met

$$A = \{x \in S \mid P(x)\} \quad , \quad B = \{x \in S \mid Q(x)\} .$$

(Zulke predikaten zijn er altijd: als $A \subset S$, dan is $A = \{x \in S \mid x \in A\}$, zodat we voor P kunnen nemen $\lambda_{x \in S}(x \in A)$.) Nu zijn allerlei dingen met behulp van logische connectieven uit te drukken:

$$\begin{aligned}
A \cup B &= \{x \in S \mid P(x) \vee Q(x)\} \\
A \cap B &= \{x \in S \mid P(x) \wedge Q(x)\} \\
A \backslash B &= \{x \in S \mid P(x) \wedge (\neg Q(x))\} \\
A \div B &= \{x \in S \mid P(x) \Leftrightarrow (\neg Q(x))\} \\
A = B &\text{ is equivalent met } \forall_{x \in S}(P(x) \Leftrightarrow Q(x)) \\
A \subset B &\text{ is equivalent met } \forall_{x \in S}(P(x) \rightarrow Q(x)) .
\end{aligned}$$

Met behulp van deze regels zijn vele betrekkingen over verzamelingen af te leiden. Als voorbeeld $A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C)$. Als aan A, B, C resp. de predikaten P, Q, R gehecht worden, gaat het om de equivalentie

$$(P(x) \wedge \neg(Q(x) \wedge R(x))) \Leftrightarrow (P(x) \wedge \neg(Q(x))) \vee (P(x) \wedge \neg(R(x)))$$

voor alle x. Wanneer men dit wil bewijzen d.m.v. geval-onderscheidingen kunnen zg. Venn-diagrammen zeer behulpzaam zijn voor het overzicht.

7.4. Cartesische producten

Een volgend stel axioma's gaat over cartesische producten. Als S en T verzamelingen zijn, dan is er daarbij een verzameling, genoteerd $S \times T$, en genaamd het cartesisch product van S en T, die de verzameling vormt van alle paren (s,t) met $s \in S$, $t \in T$. Als P een element van $S \times T$ is, dan is daarbij een "1e projectie" proj1(P) en een "2e projectie" proj2(P) met

$$\mathrm{proj1}(P) \in S\ , \quad \mathrm{proj2}(P) \in T\ , \quad (\mathrm{proj1}(P)\ , \mathrm{proj2}(P)) = P\ .$$

Ten aanzien van cartesische producten van meer dan twee verzamelingen werken we analoog. Het is natuurlijk op producten van twee terug te voeren, maar i.p.v. $(S\times T) \times U$ met elementen $((s,t),u)$ noteren we direct $S \times T \times U$ met elementen (s,t,u).

7.5. Machtsverzameling

Als S een verzameling is, dan is er een verzameling, met $\mathcal{P}(S)$ genoteerd, en machtsverzameling van S genaamd, waarvan de elementen precies alle deelverzamelingen van S zijn. Dus $A \in \mathcal{P}(S) \leftrightarrow A \subset S$ voor alle A.

Voorbeelden (eigenlijk vooruitlopend op materiaal dat nog ontwikkeld moet worden).

(i) Als $S = \{a,b\}$ dan is $\mathcal{P}(S) = \{S\ , \{a\}\ , \{b\}\ , \emptyset\}$.

(ii) $\mathcal{P}(\emptyset)$ is niet leeg, maar $\mathcal{P}(\emptyset) = \{\emptyset\}$.

(iii) Als S n elementen heeft, dan heeft $\mathcal{P}(S)$ er 2^n.

7.6. Nog wat over afbeeldingen

In 3.14 werden afbeeldingen van S in T beschreven als speciale deelverzamelingen in een cartesisch product. We gaan hier nog even op door.

De verzameling van deze afbeeldingen van S in T wordt vaak met T^S aangegeven (zie ook slot van 7.10). Het is een deelverzameling van $P(S \times T)$.

In plaats van $f \in T^S$ schrijft men vaak $f : S \to T$.

Als R een relatie op $S \times T$ is die een functie f vastlegt, en als de functiewaarde van f in het punt a (zoals gewoonlijk) door f(a) wordt voorgesteld, dan is

$$\forall_{x \in S}\, R(x, f(x)) \,,$$

$$\forall_{x \in S}\, (f(x) = \downarrow_{y \in T} R(x,y)) \qquad \text{(zie (5.1))} .$$

Als f een afbeelding van S in T is en g een afbeelding van T in U, dan is de <u>samengestelde afbeelding</u> $g \circ f$ een afbeelding van S in U, gedefinieerd door

$$g \circ f = \lambda_{x \in S}\, g(f(x)) \,.$$

Als f, g, h afbeeldingen zijn van resp. S in T, T in U, U in V, dan is

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

In een punt a van S hebben beide leden de waarde

$$h(g(f(x))) \,.$$

Als f een afbeelding van S in T is die een bijectie is, dan is er precies één inverse afbeelding h van T in S, met

$$\forall_{x\in S}\, h(f(x)) = x\,,$$

$$\forall_{y\in T}\, f(h(y)) = y\,.$$

Deze h is gedefinieerd door

$$h = \lambda_{y\in T}\,(\downarrow_{x\in S}\, f(x) = y)\,.$$

7.7. Equivalentierelaties

Laat S een verzameling zijn en R een relatie op $S \times S$. Om R een equivalentie te mogen noemen zijn drie voorwaarden vereist die als volgt met kwantoren zijn uit te drukken.

1. $\forall_{x\in S}\, R(x,x)$ (reflexiviteit)

2. $\forall_{x\in S}\,\forall_{y\in S}\,(R(x,y) \rightarrow R(y,x))$ (symmetrie)

3. $\forall_{x\in S}\,\forall_{y\in S}\,\forall_{z\in S}\,((R(x,y) \wedge R(y,z)) \rightarrow R(x,z))$ (transitiviteit).

De eenvoudigste voorbeelden zijn resp. gedefinieerd door

(i) $R(x,y) \Leftrightarrow (x = y)$

(ii) $R(x,y)$ geldt voor alle x en y uit S.

7.8. Gelijkheidsbegrip

Nu we wat meer vertrouwd zijn geraakt met verzamelingen en afbeeldingen kunnen we het gelijkheidsbegrip (zie 3.12 en ook 7.3) nader belichten.

Als S een verzameling is en $s \in S$, $t \in S$, dan is $s = t$ een propositie. Als axioma's hebben we in de eerste plaats de in 3.12 genoemde reflexiviteit, symmetrie en transitiviteit.

Ook als S en T verzamelingen zijn, dan is $S = T$ een propositie en weer gelden reflexiviteit, symmetrie en transitiviteit. Dezelfde dingen kunnen gezegd worden over $f = g$ als f en g functies zijn.

Maar er is nog heel wat meer aan axioma's over gelijkheid op te schrijven. Het valt ons niet gemakkelijk ons van alles rekenschap te geven, doordat wij dat in onze wiskundige praktijk niet gewend zijn. We zullen er geen ernstige studie van maken. Het zou trouwens moeilijk zijn systematischer te werk te gaan zonder zich vast te leggen op een speciale onderbouwing (zoals bijv. ZF) van ons wiskundige bedrijf.

In het kader van deze cursus zullen we met gelijkheid "intuïtief" omgaan, wat wil zeggen dat we er goed mee omgaan zonder aldoor rekenschap af te leggen van de gebruikte regels.

We noemen nu nog wat eigenschappen over gelijkheid en laten in het midden of men die "axioma's", "stellingen" of nog wat anders wil noemen.

(i) Als P een predikaat is en $x = y$, dan is $P(x) \Leftrightarrow P(y)$.

(ii) Als $s_1 \in S$, $s_2 \in S$, $t_1 \in T$, $t_2 \in T$, dan is

$$((s_1,t_1) = (s_2,t_2)) \Leftrightarrow ((s_1 = s_2) \wedge (t_1 = t_2)) .$$

(iii) Als $f : S \to T$, $g : S \to T$, $x \in S$, $y \in S$, $x = y$ en $f = g$, dan is $f(x) = g(y)$.

(iv) Als $f : S \to T$, $g : S \to T$ en

$$\forall_{x \in S}\, (f(x) = g(x))$$

dan is $f = g$. (Dit is het principe van de extensionaliteit voor functies; de extensionaliteit bij verzamelingen was al in 7.3 genoemd.)

(v) Als f en g zijn beschreven door middel van lambda-expressies en als daarvan de ene door beta-reductie (zie 5.5) in de andere overgaat, dan is $f = g$.

De gelijkheidsaxioma's kunnen nog worden versterkt door ook de equivalentie van proposities ($a \Leftrightarrow b$) als gelijkheid te beschouwen. Zijn verder P en Q predikaten op een verzameling S en voor alle $x \in S$ is $P(x) \Leftrightarrow Q(x)$, dan beschouwen we P en Q als gelijk. Met deze nieuwe gelijkheden werken we weer op dezelfde vrije manier als met de gewone. Als er binnen in een lange uitdrukking het predikaat P staat en we vervangen die P door Q, dan krijgen we een nieuwe uitdrukking die gelijk is aan de oude.

7.9. Het individualiteitsaxioma

Dit door Peano geformuleerde axioma spreekt uit: Als S een verzameling is met

$$S \neq \emptyset \quad , \quad \forall_{x \in S} \forall_{y \in S}\, (x = y) \tag{1}$$

dan kunnen we spreken over het element van S. Dit wordt met jota(S) genoteerd.

Een verzameling die aan (1) voldoet heet een singleton: het heeft precies één element. Als T een verzameling is en $u \in T$, dan is $\{x \in T \mid x = u\}$ een singleton; het wordt met $\{u\}$ aangeduid.

Als $u \in T$, dan is jota($\{u\}$) = u. En als S een singleton is, dan is $S = \{\text{jota}(S)\}$ en $\forall_{x \in S}\,(x = \text{jota}(S))$.

Pas wanneer men een overzicht van het totaal der grondslagen van de wiskunde heeft, kan men de niet-trivialiteit van het axioma van Peano inzien. Niettemin zullen de notaties jota(S) en $\{u\}$ duidelijk moeten zijn.

We vermeldden reeds in 5.1 de unaire operator "indiv": als P een predikaat op S is zó dat P(x) geldt voor precies één $x \in S$, dan is indiv(P) die ene x. Dus

$$\text{indiv}(P) = \downarrow_{x \in S} P(x) = \text{jota}(\{x \in S \mid P(x)\}) \; .$$

Analoog aan de singleton-notatie is de notatie met $\{a,b\}$, $\{a,b,c\}$, etc. Als S een verzameling is en $a \in S$, $b \in S$, $c \in S$, dan spreken we af

$$\{a,b,c\} = \{x \in S \mid (x=a) \vee (x=b) \vee (x=c)\} \; .$$

Er is niet geëist dat a, b en c twee aan twee verschillend zijn. Dus bijv. $\{a,b,a\} = \{a,b\}$, zelfs als $a = b$.

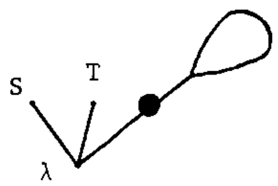
7.10. Notatie van functies met domein en "range"

Als S, T, U verzamelingen zijn met $T \subset U$ en als

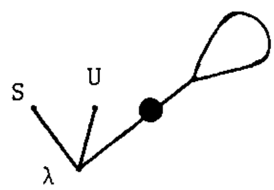
$$f : S \to T \quad , \quad g : S \to U$$

en als voor alle $x \in S$ $f(x) = g(x)$, dan zullen de meeste wiskundigen zeggen dat f dezelfde functie is als g, omdat ze hetzelfde domein hebben en op dat domein overeenstemmende waarden. Sommige anderen vinden echter, dat de T resp. U, die men dan de "range" (of "beeldruimte") van f resp. g noemt, een wezenlijk bestanddeel van de functie is,en daarom willen ze f en g niet gelijk noemen.

Onze λ-notatie gaf tot nu toe de "range" niet aan. Men zou een notatie kunnen invoeren, waarbij als binder $\lambda^{T}_{x\in S}$ resp. $\lambda^{U}_{x\in S}$ gebruikt wordt,en in de bomen zou men dat met



resp.



kunnen aangeven.

Voorbeeld.

$$\lambda^{\mathbb{Z}}_{x\in\mathbb{Z}}\ x$$

is de identiteit op $\mathbb{Z}$ en

$$\lambda^{\mathbb{R}}_{x\in\mathbb{Z}}\ x$$

is wat men wel de injectie van $\mathbb{Z}$ in $\mathbb{R}$ noemt. Het is inderdaad een injectie in de zin van 3.14.

De range wordt niet als erg essentieel beschouwd, maar het domein is belangrijk. Als $S \subset W$, en

$$f : S \to T \qquad g : W \to T$$

met $\forall_{x\in S}\, f(x) = g(x)$, dan zegt men niet dat f hetzelfde is als g (natuurlijk tenzij $S = W$), maar men noemt f de restrictie van g tot S. Notatie $f = g|S$.

Er zijn dus twee opvattingen t.a.v. een afbeelding $f : S \to T$:

(i) De afbeelding is eigenlijk een paar (S,f): het gaat om het domein en de waarden die op dat domein worden aangenomen.

(ii) De afbeelding is eigenlijk een <u>tripel</u> (S,T,f), dus ook de beeldruimte is een essentieel deel van de functie.

Bij opvatting (i) mag men <u>niet</u> zeggen dat de functie surjectief of bijectief is; men dient termen als "f is surjectief t.o.v. T", "f is een surjectie van S op T", etc. te gebruiken. Bij opvatting (ii) mag men rustig over surjectieve functies spreken.

De meeste wiskundigen zullen opvatting (i) prefereren, maar zeggen ook rustig "f is surjectief" of "f is injectief" als al eerder iets was gezegd van de strekking $f : S \to T$.

Als $S = \emptyset$, dan is er precies één afbeelding $S \to T$; dat is nl. de lege deelverzameling van $\emptyset \times T$, en laatstgenoemde is zèlf al leeg. We zullen dit een <u>lege functie</u> of <u>lege afbeelding</u> noemen. Erg belangrijk is deze natuurlijk niet, maar het komt als "randgeval" nog wel eens in stellingen voor (bijv. bij: "elke injectie van een eindige verzameling in zichzelf is een surjectie"). Laat ons even oefenen.

De lege afbeelding van $\emptyset$ naar T is injectief, en surjectief alleen als $T = \emptyset$. De beeldverzameling van een lege afbeelding is leeg. Als $f : S \to T$, dan is $f|\emptyset$ een lege afbeelding. Als $f : S \to T$ en $\forall_{x \in S} \forall_{y \in S}\, f(x) \neq f(y)$, dan is S leeg. Als $f : S \to P(T)$ en als voor alle $x \in S$ geldt $f(x) = \emptyset$, dan is f niet leeg, tenzij S leeg is. Als $f : S \to \emptyset$, dan is S leeg, en f is een lege afbeelding.

De verzameling van alle afbeeldingen van een verzameling S in een verzameling T wordt wel met T^S aangeduid (zie 7.6), terwille van de gelijkheid $|T^S| = |T|^{|S|}$ als T en S eindig zijn en $|X|$ het aantal elementen van X is (zie 9.6). Let nu op de gevallen met S of T leeg:

$$|\emptyset^S| = 0 \text{ als } S \neq \emptyset \quad , \quad |\emptyset^\emptyset| = 1 \quad , \quad |T^\emptyset| = 1 \text{ voor elke } T \, ,$$

en vergelijk dit (als $n \in \mathbb{N}$) met

$$0^n = 0 \text{ als } n \neq 0 \quad , \quad 0^0 = 1 \quad , \quad n^0 = 1 \text{ voor elke } n \, .$$

Twee functies waarvan de domeinen disjunct zijn, kunnen tot één worden verenigd. Laat S, T verzamelingen zijn en $S = A \cup B$ met $A \cap B = \emptyset$ en

$$f : A \to T \quad , \quad g : B \to T \, .$$

Dan is er precies één functie $h : S \to T$ met

$$h|A = f \quad , \quad h|B = g$$

d.w.z. als $x \in S$, dan geldt

$$h(x) = \begin{cases} f(x) & \text{als } x \in A \, , \\ g(x) & \text{als } x \in B \, . \end{cases}$$

Vaak is A gegeven door een predikaat P, nl. $A = \{x \in S \mid P(x)\}$. Dan zegt men bijv. zoiets als "h(x) = <u>if</u> P(x) <u>then</u> f(x) <u>else</u> g(x)".

<u>Voorbeeld.</u>

De functie abs : $\mathbb{R} \to \mathbb{R}$ is gedefinieerd door

$$\text{abs} := \lambda_{x \in \mathbb{R}} \; \underline{\text{if}} \; x > 0 \; \underline{\text{then}} \; x \; \underline{\text{else}} \; -x \, .$$

Men schrijft doorgaans $|x|$ i.p.v. abs(x).

7.11. Doorsnede en vereniging van een stel verzamelingen

Laat S en W verzamelingen zijn en F een afbeelding van S in $\mathcal{P}(W)$. Dan hebben we de unaire operatoren "union" en "intersection":

$$\text{union}(F) := \{w \in W \mid \exists_{x\in S}\,(w \in F(x))\}$$
$$\text{intersection}(F) := \{w \in W \mid \forall_{x\in S}\,(w \in F(x))\}\ .$$

Evenals bij de andere unaire operatoren uit 5.1 worden weer nieuwe binders ingevoerd. We schrijven

$\bigcup_{x\in S} \ldots$ in plaats van $\text{union}(\lambda_{x\in S} \ldots)$

$\bigcap_{x\in S} \ldots$ in plaats van $\text{intersection}(\lambda_{x\in S} \ldots)$

dus ook

$$\text{union}(F) = \bigcup_{x\in S} F(x) \quad , \quad \text{intersection}(F) = \bigcap_{x\in S} F(x)\ .$$

Als bijv. $S = \{1,2,3\}$, $F(1) = A$, $F(2) = B$, $F(3) = C$, met $A \subset W$, $B \subset W$, $C \subset W$, dan is

$$\bigcup_{x\in\{1,2,3\}} F(x) = A \cup B \cup C\ ,$$
$$\bigcap_{x\in\{1,2,3\}} F(x) = A \cap B \cap C\ .$$

We moeten "union" goed onderscheiden van "beeld":

$$\text{beeld}(F) = \{F(x) \mid x \in S\} = \{y \in \mathcal{P}(W) \mid \exists_{x\in S}\, y = F(x)\}\ .$$

Als bijv. $S = \{1,2,3,4,5\}$, $W = \{6,7,8\}$ en

$$F(1) = \{6,7\},\ F(2) = \emptyset,\ F(3) = \{6,8\},\ F(4) = \{6,7\},\ F(5) = \{6\}$$

dan is

$$\text{union}(F) = \bigcup_{x\in S} F(x) = \{6,7,8\}\ ,$$
$$\text{beeld}(F) = \{\emptyset\ , \{6\}\ , \{6,7\}\ , \{6,8\}\}\ .$$

We spreken nog even af wat we doen als $S = \emptyset$:

$$\mathrm{union}(\lambda_{x\in\emptyset} F(x)) = \{w \in W \mid \exists_{x\in\emptyset} (w \in F(x))\} = \emptyset\ ,$$

$$\mathrm{intersection}(\lambda_{x\in\emptyset} F(x)) = \{w \in W \mid \forall_{x\in\emptyset} (w \in F(x))\} = W\ ,$$

$$\mathrm{beeld}(\lambda_{x\in\emptyset} F(x)) = \{y \in P(W) \mid \exists_{x\in\emptyset}\, y = F(x)\} = \emptyset\ .$$

Die uitkomst W bij intersection is griezelig. Niet omdat men als uitkomst $\emptyset$ zou verwachten en het dat niet hoeft te zijn, maar veel meer omdat de uitkomst afhangt van W en die W in het linkerlid niet genoteerd is. Daarom zou hier de notatie

$$\mathrm{intersection}(\lambda^{W}_{x\in\emptyset}\ F(x))$$

(zie 7.10) goed van pas komen.

De kwestie komt ook aan het daglicht als we intersection en union via complementvorming met elkaar in verband willen brengen: Als $F : S \to P(W)$, dan is

$$W\backslash(\mathrm{intersection}(F)) = \mathrm{union}(\lambda_{x\in S}\ (W\backslash F(x)))\ .$$

Als $S = \emptyset$, staat links $W\backslash W$, rechts $\emptyset$.

Bijzondere gevallen van "union" en "intersection" krijgen we als S een deelverzameling van $P(W)$ is en $F(x) = x$ voor alle $x \in S$ (dus F is de injectie van S in $P(W)$). Dan zijn de vereniging en de doorsnede van alle x uit S resp. beschreven door

$$\bigcup_{x\in S} x = \mathrm{union}(\lambda_{x\in S}\ x) = \{w \in W \mid \exists_{x\in S}\ w \in x\}\ ,$$

$$\bigcap_{x\in S} x = \mathrm{intersection}(\lambda_{x\in S}\ x) = \{w \in W \mid \forall_{x\in S}\ w \in x\}\ .$$

Voorbeeld.

$W = \{0,1,2,3,4,5\}$, $S = \{\{0,1,2\}, \{0,3,4\}, \{0,2,4\}\}$.

Dan is de vereniging $\{0,1,2,3,4\}$ en de doorsnede $\{0\}$.

Als S leeg is dan moet worden vastgesteld dat $\bigcap_{x\in S} x = W$.

7.12. Beeld en volledig origineel

Als $f : S \to T$ en $A \in P(S)$, dan heet de verzameling van alle $f(x)$ met $x \in A$ het beeld van A onder de afbeelding f. We zullen het met $f^{bd}(A)$ noteren. Dus

$$f^{bd} \quad : P(S) \to P(T) ,$$

$$f^{bd}(A) = \{f(x) \mid x \in A\} = \text{beeld}(\lambda_{x\in A}\, f(x))$$

$$= \{y \in T \mid \exists_{x\in A}\; y = f(x)\} \quad \text{(vgl. 5.1).}$$

Voorbeelden van gebruik.

(i) $f^{bd}(\emptyset) = \emptyset$, $f^{bd}(S) \subset T$.

(ii) Als $x \in S$, dan is $f^{bd}(\{x\}) = \{f(x)\}$.

(iii) Als $A \in P(S)$, $B \in P(S)$, dan is

$$f^{bd}(A \cup B) = f^{bd}(A) \cup f^{bd}(B)$$

$$f^{bd}(A \cap B) \subset f^{bd}(A) \cap f^{bd}(B)$$

$$f^{bd}(A \backslash B) \supset f^{bd}(A) \backslash f^{bd}(B) .$$

Als $f : S \to T$ en $U \in \mathcal{P}(T)$, dan is het <u>volledig origineel</u> van U gedefinieerd als $\{x \in S \mid f(x) \in U\}$. We zullen het met $f^{vo}(U)$ noteren. Dus

$$f^{vo} : \mathcal{P}(T) \to \mathcal{P}(S) .$$

<u>Voorbeelden van gebruik</u>.

(i) Als $f : S \to T$ bijectief is, met inverse functie h (vgl. 7.6), dan is

$$f^{vo}(\{y\}) = \{h(y)\} \quad \text{voor alle } y \in T , \quad \text{en} \quad f^{vo}(\{f(x)\}) = \{x\}$$

voor alle $x \in S$.

(ii) Als $f : S \to T$ injectief is en $y \in T$, dan is $f^{vo}(\{y\})$ òf leeg òf een singleton.

(iii) Als $f : S \to T$, dan is

$$f \text{ surjectief} \Leftrightarrow \forall_{y \in T}\ f^{vo}(\{y\}) \neq \emptyset .$$

(iv) Als $f : \emptyset \to T$, dan is $f^{vo}(U) = \emptyset$ voor elke deelverzameling U van T.

(v) Als $f : S \to T$, dan is $f^{vo}(\emptyset) = \emptyset$ en $f^{vo}(T) = S$.

(vi) Als $f : S \to T$, $U \in \mathcal{P}(T)$, $V \in \mathcal{P}(T)$, dan is

$$f^{vo}(U \cup V) = f^{vo}(U) \cup f^{vo}(V)$$

$$f^{vo}(U \cap V) = f^{vo}(U) \cap f^{vo}(V)$$

$$f^{vo}(U \setminus V) = f^{vo}(U) \setminus f^{vo}(V) .$$

(vii) Als $f : S \to T$, $y \in T$, dan is de verzameling van alle $x \in S$ die y als beeld hebben niet $f^{vo}(y)$ maar $f^{vo}(\{y\})$.

Opmerkingen over deze notaties.

Laat ons naar analogie met de notaties f^{bd} en f^{vo} even de inverse functie van f (in het geval dat $f : S \to T$ bijectief is) met f^{inv} aanduiden.

In verschillende delen van de wiskunde bestaat de slordige gewoonte om f^{bd} gewoon als f te noteren. En evenzo wordt vaak geen verschil gemaakt tussen f^{vo} en f^{inv}. Sommigen noteren zowel f^{vo} als f^{inv} met $f^{\leftarrow}$ en anderen noteren beide met f^{-1}.

De notatie f^{-1} voor f^{inv} is goed te verdedigen op grond van de notatie $f^2 = f \circ f$, $f^3 = f \circ f \circ f$, enz.

7.13. Het keuzeaxioma

Men kan pas inzien wat het keuzeaxioma uitspreekt wanneer men zich precies aan de regels van de verzamelingstheorie houdt en niet intuïtief of emotioneel te werk gaat.

Laat S en T verzamelingen zijn en Φ een afbeelding van S in $\mathcal{P}(T)$ met

$$\forall_{x \in S}\ \Phi(x) \neq \emptyset \qquad (1)$$

(dus: aan elk element van S is een niet-leeg deel van T toegevoegd). Dan zegt het keuzeaxioma dat er een afbeelding $f : S \to T$ bestaat zo dat voor elke $x \in S$ het beeld $f(x)$ ligt in de door Φ aan x toegevoegde verzameling:

$$\forall_{x \in S}\ (f(x) \in \Phi(x)) . \qquad (2)$$

We kunnen (2) werkelijk afleiden als we over een middel beschikken om simultaan in elke $\Phi(x)$ een element aan te wijzen. Dit kan bijv. als $T = \mathbb{N}$, want dan kan men voor $f(x)$ het kleinste getal uit $\Phi(x)$ nemen.

Het gebruik van het keuzeaxioma geeft in de wiskunde tot allerlei "niet-constructieve" bewijzen aanleiding. Zo kon met het keuzeaxioma in de hand door Zermelo worden bewezen dat elke verzameling A kan worden welgeordend, d.w.z. dat er op A een ordeningsrelatie $<$ bestaat zó dat elke niet-lege deelverzameling van A een kleinste element heeft. Pogingen om zich voor te stellen hoe zo'n welordening eruit ziet, brengen het niet verder dan aftelbare verzamelingen.

Tegenwoordig weet men (K. Gödel - P. Cohen) dat noch het keuzeaxioma noch de ontkenning ervan in strijd is met de andere axioma's van de verzamelingstheorie.

Het hierna nog volgende materiaal zou eigenlijk pas nà Hoofdstuk 9 besproken kunnen worden; terwille van de samenhang doen we het hier.

In de gewone analyse gebruikt men vaak het "aftelbare keuzeaxioma", d.i. het geval dat $S = \mathbb{N}$. Dit is minder "griezelig" dan het algemene.

Wat ook vaak wordt gebruikt is het principe der successieve keuzen: Er is een verzameling W en we hebben een rij $a_0, a_1, \ldots$ van elementen van W op te bouwen waarbij voor elke n de a_{n+1} moet worden gekozen uit een door n en a_n aangewezen deelverzameling. We beschrijven die deelverzamelingen met een afbeelding $\Psi : (\mathbb{N} \times W) \to P(W)$ met

$$\forall_{n\in\mathbb{N}} \forall_{w\in W}\ \Psi(n,w) \neq \emptyset .$$

Er is een startverzameling A $(A \subset W, A \neq \emptyset)$ gegeven. Het principe der successieve keuzen zegt dat er een afbeelding $f : \mathbb{N} \to W$ is met

$$f(0) \in A , \quad \forall_{n\in\mathbb{N}}\, f(\mathrm{succ}(n)) \in \Psi(n,f(n)) .$$

Een wat algemener formulering is te krijgen door die deelverzameling niet alleen door n en $f(n)$ te laten bepalen maar door n en $f(0), f(1), \ldots, f(n)$.

Een voorbeeld: Elke niet-eindige verzameling W bevat een aftelbare deelverzameling. We nemen als startverzameling W zelf en de verzameling waaruit $f(n+1)$ moet worden gekozen is $W \setminus \{f(0), \ldots, f(n)\}$. Deze is niet leeg, want anders was W eindig.

7.14. De paradox van Russell

Het is mogelijk de gehele wiskunde te bouwen op de verzamelingstheorie. Het begrip "verzameling" staat daarbij primair. Alle wiskundige objecten zijn verzamelingen. Er is een grote klasse van dingen die men verzamelingen noemt en als x en y verzamelingen zijn dan is $x \in y$ een propositie. Heeft men een predikaat P dat aan elke verzameling x een propositie $P(x)$ toevoegt, dan is het verleidelijk te denken dat $\{x \mid P(x)\}$ een verzameling is. Dit zou echter het verzamelingsgebouw in elkaar doen storten, zoals Russell in 1902 als volgt liet zien. Kort even $\neg(x \in y)$ af tot $P(x,y)$ en stel

$$u := \{x \mid P(x,x)\} .$$

Nu is voor elke v

$$v \in u \Leftrightarrow P(v,v) .$$

Als we hierin voor v de u invullen, komt er $u \in u \Leftrightarrow \neg(u \in u)$ en daarmede is een contradictie afgeleid.

In formele beschrijvingen van wat er met verzamelingen mag, zoals in het axiomasysteem van Zermelo-Fraenkel, laat men $\{x \mid P(x)\}$ dan ook niet als verzameling toe. Alleen als y een verzameling is, laat men $\{x \in y \mid P(x)\}$ als verzameling toe.

Men mag niet spreken over de verzameling van alle verzamelingen. Er is nl. geen verzameling U zó dat voor elke verzameling y geldt $y \in U$. Neem in navolging van Russell $u := \{x \in U \mid \neg x \in x\}$. Voor elke v is nu $v \in u$ equivalent met $v \in U \wedge \neg(v \in v)$. In de onderstelling $u \in U$ geldt nu $u \in u \Leftrightarrow \neg(u \in u)$ en dat is een contradictie. Dus $\neg(u \in U)$.

We komen deze argumentatie nog eens tegen in 9.9.

HOOFDSTUK 8. BESCHOUWINGEN OVER PROPOSITIES, WAARDERINGEN EN BOOLESE WAARDEN

8.1. Twee begrippen "propositie"

Zo ongemerkt hebben we twee verschillende begrippen "propositie" opgebouwd:

(i) De proposities uit Hoofdstuk 2. We gingen uit van letters die "propositievariabelen" genoemd werden en bouwden nieuwe proposities op met behulp van connectieven. We zullen ze hier "logische formules" blijven noemen.

(ii) De proposities uit de wiskunde, die bijv. in Hoofdstuk 7 optraden, maar ook al in Hoofdstuk 3 bij de voorbeelden over predikaten.

Het zijn eigenlijk twee verschillende werelden. In (i) is geen verzamelingstaal, geen gevoel voor "waarheid". In (ii) zijn er geen propositievariabelen. Een gewoon wiskundig betoog houdt zich daar niet mee bezig.

Het is heel goed mogelijk wiskundige talen te ontwikkelen die (i) en (ii) overkoepelen, dus waarin zowel propositievariabelen als gewone "wiskundige" variabelen worden gebruikt, maar dat wordt (nog) zo goed als nergens formeel gedaan (informeel gebeurt het op grote schaal!). We zullen het hier ook niet doen, maar moeten wèl verbanden leggen tussen (i) en (ii). Overigens: de wereld van (i) wordt wel "formele logica" genoemd en die van (ii) "wiskunde".

Het belangrijkste verband is dit: de formele logica levert bewijsschema's voor de wiskunde. We hebben hier stilzwijgend al eerder aan gedacht. In de formele logica hebben we bijv. een tautologie

$$(p \to (q \to r)) \to (q \to (p \to r)) . \tag{1}$$

Daarnaast bekijken we de wiskundige uitspraak

$$((a > b) \to ((b > c) \to (a > c))) \to ((b > c) \to ((a > b) \to (a > c))) . \tag{2}$$

Wanneer we een taal zouden hebben die formele logica en wiskunde overkoepelt, dan zouden we zeggen: (2) volgt uit (1) door de substitutie waarbij p, q, r resp. door $a > b$, $b > c$, $a > c$ worden vervangen. Hebben we zo'n taal niet, dan wordt die substitutie een goocheltruc. Wat we echter wel kunnen doen is dit: elke ND afleiding van (1) kan worden omgewerkt tot een afleiding voor (2), door overal p, q, r te vervangen door $a > b$, $b > c$, $a > c$. De afleiding van (1) hoeft dus alleen op het kladpapier te staan.

We gaan een stap verder als we ons ter behandeling van (1) niet van echte ND-afleidingen bedienen, maar van de waarderingen uit Hoofdstuk 4. Onze conclusie is dan dat er voor (1) een ND-afleiding moet bestaan. En dat er dus ook een afleiding voor (2) moet bestaan. We zouden kunnen afspreken hiermee genoegen te nemen.

8.2. Twee begrippen "waardering"

In Hoofdstuk 4 hebben we functies w beschouwd die aan elke propositievariabele een 0 of 1 toekenden, en lieten we zien hoe deze afbeeldingen konden worden voortgezet tot alle logische formules uit de propositielogica. Zo'n w heet een waardering.

Naast deze w's uit de formele logica kunnen we ook de in de wiskunde iets invoeren dat we waardering noemen. We zullen het symbool W gebruiken. Aan iedere wiskundige propositie wordt door W 0 of 1 toegevoegd en wel 1 als die propositie geldt en 0 als de ontkenning van die propositie geldt. (We bedrijven onze wiskunde met gebruikmaking van de regel DBNG.)

Om te laten zien dat W ècht in de wiskundige taal zelf (en niet uitsluitend in de een of andere metataal) kan worden gebruikt, drukken we W uit in symbolen die we al hebben. We nemen een vaste verzameling A met precies één element. Aan een wiskundige propositie als $a < 5$ (die de letter x niet bevat) voegen we het predikaat $\lambda_{x \in A}(a < 5)$ toe en laten daar "card" op los (zie 5.1). Dit heeft de waarde 1 als $a < 5$ geldt (dan is er één x in A waarvoor $a < 5$ geldt) en anders de waarde 0. Dus

$$W(a < 5) = \#_{x \in A}(a < 5) .$$

8.3. Het verband tussen w en W

We volstaan met een voorbeeld. In de een of andere context zijn $a > b$ en $b > 2$ wiskundige proposities. In de formele logica nemen we propositievariabelen p en q en een waardering w vastgesteld door

$$w(p) = W(a > b) \quad , \quad w(q) = W(b > 2) .$$

Nu vormen we een logische formule, zoals $(p \to q) \to q$, en beschouwen de wiskundige formule die ontstaat door overal p door $a > b$ en q door $b > 2$ te vervangen. Dan concluderen we tot

$$W(((a>b) \to (b>2)) \to (b>2)) = w((p \to q) \to q) .$$

Om dit in te zien is het voldoende na te gaan wat er gebeurt bij de "primitieve" logische formules $p \to q$, $p \wedge q$, $\neg p$. Men zou kunnen zeggen dat de waarheidstabellen voor de connectieven in Hoofdstuk 4 juist zo gemaakt zijn om deze correspondentie in orde te krijgen.

8.4. Boolese waarden en boolese functies

De verzameling $\{0,1\}$ die we als beeldruimte voor w en W gebruikten wordt in dat verband de verzameling der boolese waarden (spreek uit "boelse waarden") genoemd. Een afbeelding van een verzameling S naar $\{0,1\}$ heet een boolese functie op S.

Laat S een verzameling zijn en P een predikaat op S. Met P correspondeert de afbeelding $\lambda_{x \in S} W(P(x))$ van S naar $\{0,1\}$; dit is een boolese functie op S. We korten die af tot f:

$$f := \lambda_{x \in S} W(P(x)) .$$

Verder hebben we de verzameling T van alle elementen van S die "aan P voldoen":

$$T := \{x \in S \mid P(x)\} .$$

De functie f is gelijk aan de zg. karakteristieke functie van T. Die wordt vaak met χ_T genoteerd:

$$\chi_T(x) = 1 \quad \text{als } x \in T \quad , \quad \chi_T(x) = 0 \quad \text{als } x \in S \backslash T .$$

Elk van de drie objecten P, f, T bepaalt de beide andere eenduidig. We maken er een lijstje van:

$$f = \lambda_{x\in S}\, W(P(x)) \quad , \quad T = \{x \in S \mid P(x)\}$$

$$P = \lambda_{x\in S}\, (f(x) = 1) \quad , \quad T = \{x \in S \mid f(x) = 1\}$$

$$f = \chi_T \quad , \quad P = \lambda_{x\in S}\, (x \in T) .$$

Passen we het een en ander toe op een vaste x uit S, dan krijgen we

$$P(x) \Leftrightarrow x \in T \Leftrightarrow f(x) = 1$$

$$\neg P(x) \Leftrightarrow x \notin T \Leftrightarrow f(x) = 0$$

$$W(P(x)) = W(x \in T) = f(x) .$$

8.5. Connectieven bij proposities, predikaten, boolese waarden en boolese functies

We hebben met vier situaties te maken waarin er van iets als connectieven sprake is: (i) bij proposities in formele logica en in wiskunde, (ii) bij boolese waarden, (iii) bij predikaten, (iv) bij boolese functies. Het is verleidelijk maar gevaarlijk om voor overeenkomstige connectieven in de vier situaties dezelfde tekens te gebruiken.

We hebben iets dergelijks bij de som van twee functies: als $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}$, dan wordt $\lambda_{x\in\mathbb{R}}(f(x) + g(x))$ wel door $f + g$ voorgesteld: hetzelfde teken dat een afbeelding $(\mathbb{R} \times \mathbb{R}) \to \mathbb{R}$ voorstelde, wordt nu in een nieuwe situatie gebruikt.

Als P en Q predikaten zijn op S, dan zijn ook

$$\lambda_{x\in S}\, (P(x) \wedge Q(x)) \quad , \quad \lambda_{x\in S}\, (P(x) \vee Q(x))$$

predikaten op S. Laat ons ze even met P en Q, P of Q aanduiden. Het kan niet zo erg veel kwaad om rustig en door $\wedge$ te vervangen, hoewel het natuurlijk niet in de haak is.

Het is gevaarlijker met of en met

$$\lambda_{x\in S}\,(P(x) \to Q(x)) \quad , \quad \lambda_{x\in S}\,(P(x) \Leftrightarrow Q(x)) ,$$

want $P \to Q$ en $P \Leftrightarrow Q$ zouden door velen geïnterpreteerd kunnen worden als

$$\forall_{x\in S}\,(P(x) \to Q(x)) \quad \text{resp.} \quad \forall_{x\in S}\,(P(x) \Leftrightarrow Q(x)) .$$

Bij $\wedge$ is een zekere nonchalance mogelijk, doordat

$$(\forall_{x\in S}\,(P(x)) \wedge (\forall_{x\in S}\,Q(x))$$

equivalent is met

$$\forall_{x\in S}\,(P(x) \wedge Q(x)) ,$$

dus met $\forall$(P en Q). Bij $\vee$, $\to$, $\Leftrightarrow$ is zoiets niet meer het geval.

Als er naast x nog andere variabelen in het spel zijn, wordt de zaak nog verwarrender.

Het is beter die notaties $P \wedge Q$, $P \vee Q$, $P \to Q$, $P \Leftrightarrow Q$ geheel te vermijden.

We kijken nu even naar de connectieven op de boolese waarden. Daar beschouwen we afbeeldingen van $\{0,1\} \times \{0,1\}$ naar $\{0,1\}$ resp. van $\{0,1\}$ naar $\{0,1\}$, die we even door $\underline{\wedge}$, $\underline{\vee}$, $\underline{\to}$, $\underline{\Leftrightarrow}$, $\underline{\neg}$ voorstellen en die de waarheidstafels voor $\wedge$, $\vee$, $\to$, $\Leftrightarrow$ en $\neg$ uitdrukken. Als a en b boolese waarden zijn, dan is

$$(a \,\underline{\wedge}\, b) = \min(a,b) = W(a=1 \wedge b=1) ,$$

$$(a \,\underline{\vee}\, b) = \max(a,b) = W(a=1 \vee b=1) ,$$

$$(a \,\underline{\to}\, b) = 1 - a + ab = W(a \le b) ,$$

$$(a \,\underline{\Leftrightarrow}\, b) = 1 - a - b + 2ab = W(a=b) ,$$

$$\underline{\neg} a = 1 - a = W(a=0) .$$

Als p en q logische formules zijn, dan is voor elke waardering w:

$$w(p \wedge q) = w(p) \underline{\wedge} w(q) ,$$

$$w(p \vee q) = w(p) \underline{\vee} w(q) ,$$

$$w(p \rightarrow q) = w(p) \underline{\rightarrow} w(q) ,$$

$$w(p \Leftrightarrow q) = w(p) \underline{\Leftrightarrow} w(q) ,$$

$$w(\neg p) = \underline{\neg} w(p) .$$

Als p en q door wiskundige proposities worden vervangen en w door W, dan blijft het lijstje van kracht.

Nadat we het onderscheid tussen $\wedge$ en $\underline{\wedge}$ etc. weten, gebruiken we rustig $\wedge$, $\vee$, $\rightarrow$, $\Leftrightarrow$, $\neg$ op de boolese waarden.

We weten dat W proposities in boolese waarden overvoert. Omgekeerd is uit een boolese waarde weer een propositie te maken: als b een boolese waarde is, dan is $b = 1$ een propositie. En

$$W(b=1) = b ,$$

$$W(b=0) = 1 - b .$$

Nog een paar voorbeelden (ter vermijding van moeilijkheden over de fijne verschillen tussen "propositievariabelen", "letters die logische formules voorstellen" en "letters die wiskundige proposities voorstellen" nemen we hier de speciale wiskundige proposities $x > y$ en $u \in S$):

$$x > y \Leftrightarrow (W(x > y) = 1)$$

$$\neg(x > y) \Leftrightarrow (W(x > y) = 0)$$

$$((x > y) \leftrightarrow (u \in S)) \leftrightarrow (W(x > y) = W(u \in S))$$

$$W(W(x > y) = W(u \in S)) = W((x > y) \leftrightarrow u \in S) .$$

Als het over de connectieven bij boolese functies gaat hebben we natuurlijk iets dat analoog is aan de situatie met predikaten. Men moet goed weten wat men doet en zich niet laten bedriegen door notaties die men zelf heeft ingevoerd om op schrijfwerk te bezuinigen.

8.6. Kunnen we niet met boolese waarden volstaan?

Men kan proberen de gehele klassieke propositiecalculus naar het rekenen met boolese waarden te verschuiven, maar men blijft altijd nog met één soort echte proposities zitten, nl. die van de vorm "b = 0" of "b = 1". Men kan zeggen dat het door het overgaan op boolese waarden lukt om ervoor te zorgen dat er nog maar met één soort proposities gewerkt hoeft te worden, nl. de proposities die de vorm hebben van gelijkheden op de verzameling der boolese waarden.

Bij de propositiecalculus kan de boolese interpretatie nog plezierig gevonden worden, maar bij de predikatencalculus is dat niet meer het geval: de kwesties van introductie en eliminatie van het al- en existentiesymbool worden er niet eenvoudiger door.

HOOFDSTUK 9. NATUURLIJKE GETALLEN, INDUCTIE EN RECURSIE

9.1. De axioma's van Peano

Deze axioma's vormen de basis waarop de theorie van het natuurlijk getal kan worden opgebouwd. Er wordt gepostuleerd dat er een verzameling is, met daarin een met de naam 0 aangeduid element, en een afbeelding succ van $\mathbb{N}$ in $\mathbb{N}$. Hiervan wordt geëist

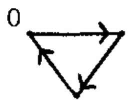
Axioma 1. $\forall_{x\in\mathbb{N}}\ \mathrm{succ}(x) \neq 0$.

Axioma 2. $\forall_{x\in\mathbb{N}} \forall_{y\in\mathbb{N}}\ ((\mathrm{succ}(x) = \mathrm{succ}(y)) \rightarrow (x = y))$.

Axioma 3. $\forall_{S\in P(\mathbb{N})}\ ((0 \in S \wedge \forall_{n\in\mathbb{N}} (n \in S \rightarrow \mathrm{succ}(n) \in S)) \rightarrow \forall_{x\in\mathbb{N}}\ x \in S)$.

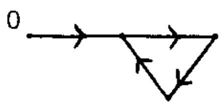
Om wat gevoel voor de axioma's van Peano op te brengen laten we zien wat er te verwachten is als we Axioma 1, 2 of 3 weglaten. We tekenen elementen van $\mathbb{N}$ als punten en bij elke n een pijltje van n naar succ(n).

Als we Axioma 1 weglaten, dan voldoet bijv.

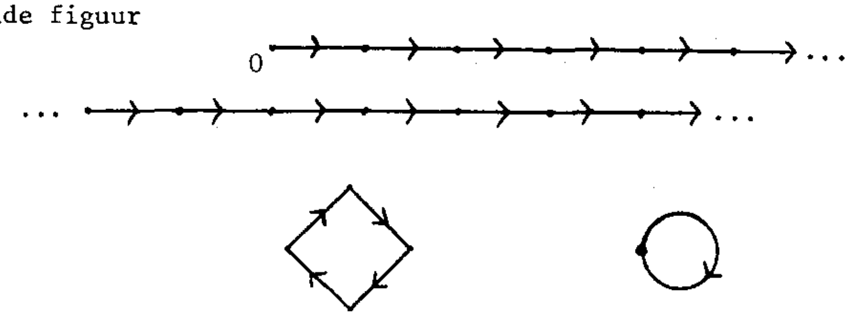


en zelfs

Als we Axioma 2 weglaten, dan voldoet bijv.



Als we Axioma 3 weglaten, dan voldoet bijv. de uit 4 losse stukken bestaande figuur



9.2. Volledige inductie

Uit Axioma 3 volgt dat als P een predikaat op $\mathbb{N}$ is en als

$$P(0) \wedge \forall_{n\in\mathbb{N}} (P(n) \to P(\mathrm{succ}(n))) ,$$

dan geldt $\forall_{n\in\mathbb{N}} P(n)$. Dit heet het principe van de <u>volledige inductie</u>.

Vaak zegt men gewoon "inductie" i.p.v. "volledige inductie". Het principe geeft aanleiding tot het volgende <u>bewijsschema</u>:

<bewijs voor P(0)>

| $n \in \mathbb{N}$
| | $P(n)$
| | <bewijs voor P(succ(n))>

conclusie $\forall_{n\in\mathbb{N}} P(n)$.

Een voorbeeld (dat een beetje rekenkunde gebruikt en in het bijzonder $\mathrm{succ}(n) = n+1$):

$$P(n) := 5 \cdot 3^{4n+1} - 2^{2n} \text{ is deelbaar door } 7 .$$

P(0) betekent 15 - 1 is deelbaar door 7,en dat is in orde. Nu

| $n \in \mathbb{N}$
| | $5 \cdot 3^{4n+1} - 2^{2n}$ is deelbaar door 7
| | <bewijs>
| | $5 \cdot 3^{4(n+1)+1} - 2^{2(n+1)}$ is deelbaar door 7 .

Het in te vullen bewijs gaat als volgt.
$3^4 \cdot (5 \cdot 3^{4n+1} - 2^{2n})$ is een 7-voud. En $3^4 \cdot 2^{2n} - 2^{2(n+1)}$ is gelijk aan $(3^4 - 4)2^{2n} = 77 \cdot 2^{2n}$ en is dus ook een 7-voud. De som van deze twee 7-vouden is $5 \cdot 3^{4(n+1)+1} - 2^{2(n+1)}$.

Een tweede voorbeeld:

$$P(n) \quad := \quad n \neq 0 \to \exists^1_{k \in \mathbb{N}} (\mathrm{succ}(k) = n) \, .$$

$P(0)$ is duidelijk daar $0 \neq 0$ onwaar is. Neem nu $P(n)$ aan en noem $\mathrm{succ}(n) = m$. We willen $P(m)$ bewijzen, waartoe voldoende is

$$\exists^1_{k \in \mathbb{N}} (\mathrm{succ}(k) = m) \, .$$

Er is inderdaad zo'n k, nl. n. En er is geen tweede, wegens het desbetreffende axioma van Peano. Dus $P(m)$ is bewezen.

9.3. Opbouw van de theorie van $\mathbb{N}$

Op grond van de axioma's van Peano kan de theorie van $\mathbb{N}$ worden ontwikkeld. Men kan bijv. beginnen met op $\mathbb{N}$ een relatie $<$ in te voeren die voldoet aan:

(i) Voor elk paar $x \in \mathbb{N}$, $y \in \mathbb{N}$ geldt precies één van de proposities $x < y$, $x = y$, $y < x$ ("trichotomie").

(ii) Voor elke $x \in \mathbb{N}$ geldt $(x = 0) \vee (0 < x)$.

(iii) Voor elke $x \in \mathbb{N}$ geldt $x < \mathrm{succ}(x)$.

(iv) Als $x \in \mathbb{N}$, $y \in \mathbb{N}$, dan geldt niet zowel $x < y$ als $y < \mathrm{succ}(x)$.

(v) Als $x \in \mathbb{N}$, $y \in \mathbb{N}$, $z \in \mathbb{N}$, dan geldt $((x < y) \wedge (y < z)) \to x < z$ ("transitiviteit").

Het is een heel werk om de relatie te construeren en deze uitspraken te bewijzen. In het kader van deze cursus zullen we dat niet doen.

Vervolgens kan de optelling worden ingevoerd (bijv. door recursie, zie 9.7) en daarna de vermenigvuldiging en dan kunnen ook de over optelling, vermenigvuldiging en ordening bekende grondeigenschappen worden afgeleid. Ook hier gaan we niet op in.

9.4. Versterkte inductie

Nu we eenmaal ordening op $\mathbb{N}$ hebben, kunnen we het "versterkte" inductieprincipe formuleren. Laat P een predikaat op $\mathbb{N}$ zijn en stel voor elke $n \in \mathbb{N}$ de uitspraak

$$\forall_{m \in \mathbb{N}} (m < n \to P(m))$$

door Q(n) voor. Dan zegt het versterkte inductieprincipe dat als

$$\forall_{n \in \mathbb{N}} (Q(n) \to P(n)) \qquad (1)$$

dat dan $\forall_{n \in \mathbb{N}} P(n)$. Dit geeft het volgende bewijsschema:

$n \in \mathbb{N}$

  $\forall_{m \in \mathbb{N}} (m < n \to P(m))$

    <bewijs voor P(n)>

conclusie $\forall_{n \in \mathbb{N}} P(n)$.

Men zal zich afvragen waarom de P(0) niet meer afzonderlijk hoeft te worden bewezen. Welnu: dat is in (1) vervat. Q(0) geldt eenvoudig omdat voor $m \in \mathbb{N}$ altijd $\neg(m < 0)$ geldt, dus ook $m < 0 \to P(m)$. En uit Q(0) volgt P(0) wegens (1).

Om in te zien dat het versterkte principe uit het gewone volgt, merken we eerst op dat voor elke $n \in \mathbb{N}$

$$(Q(n) \to P(n)) \Leftrightarrow (Q(n) \to Q(\mathrm{succ}(n))) . \tag{2}$$

(Bij de afleiding daarvan gebruiken we dat er geen m tussen n en succ(n) ligt, zodat

$$m < \mathrm{succ}(n) \Leftrightarrow (m < n) \vee (m = n) .)$$

We merkten al op dat Q(0) geldt. Volgens het gewone inductieprincipe leidt (1) dus tot $\forall_{n\in\mathbb{N}} Q(n)$. Nog eens (1) toepassende, komen we nu tot $\forall_{n\in\mathbb{N}} P(n)$.

Een voorbeeld: Men neemt voor P(n) de uitspraak: "als $n > 1$, dan is n een priemgetal of een product van priemgetallen". (Om het voorbeeld snel af te kunnen handelen, laten we het bij deze ruwe formulering.) Neem $n \in \mathbb{N}$ en onderstel Q(n). We willen P(n) bewijzen. Als $n \leq 1$ is dit in orde. Nu $n > 1$. Als n een priemgetal is, is P(n) juist. Neem nu aan dat n geen priemgetal is. Dan is $n = km$ met $1 < k < n$, $1 < m < n$. Wegens Q(n) geldt P(k) zowel als P(m), dus zowel k als m zijn priem of product van priemgetallen. Derhalve is n een product van priemgetallen, dus P(n) geldt.

Soms wordt de versterkte inductie in negatieve zin gebruikt. Laat R(n) de uitspraak zijn dat n^3 som van twee gehele positieve derde machten is. Men wil bewijzen $\forall_{n\in\mathbb{N}} (\neg R(n))$. Aannemende dat voor de een of andere n geldt R(n), construeert men een natuurlijk getal m met $m < n$ waarvoor wéér R(n). Deze redeneervorm wordt wel "descente infinie" genoemd, omdat een tegenvoorbeeld een oneindige afdalende rij natuurlijke getallen zou opleveren.

9.5. Iets over de methodiek van inductie

Laat P_1 en P_2 predikaten zijn, waarbij P_2 "sterker" is dan P_1, d.w.z.

$$\forall_{n\in\mathbb{N}}(P_2(n) \to P_1(n)) .$$

(Eigenlijk moeten we zeggen "minstens even sterk".) Dan kan het voorkomen dat we als doel hebben $\forall_{n\in\mathbb{N}} P_1(n)$, maar dat $\forall_{n\in\mathbb{N}} P_2(n)$, hoewel het sterker kan zijn, tòch gemakkelijker door inductie te bewijzen is. De implicatie

$$P_1(n) \to P_1(\text{succ}(n)) \tag{1}$$

kan moeilijker te bewijzen zijn dan

$$P_2(n) \to P_2(\text{succ}(n)) . \tag{2}$$

Weliswaar is bij (2) de "bewijslast" $P_2(\text{succ}(n))$ sterker dan bij (1), maar er is bij (2) ook meer om van uit te gaan (nl. $P_2(n)$ i.p.v. $P_1(n)$) en dat kan de doorslag geven.

Vaak is P_1 ons doel en moeten we als (1) niet goed lukt een versterking P_2 vinden waarvoor (2) wèl lukt. Dit kan lastig zijn. Een algemene regel zou kunnen zijn: probeer zoveel mogelijk eenvoudige informatie over de situatie te ontdekken (vermoedenderwijs) en stop die in P_2.

Een voorbeeld: $P_1(n)$ is

$$\sum_{k=0}^{n} k^3 \quad \text{is een kwadraat} \tag{1}$$

(met "kwadraat" is bedoeld "kwadraat van een natuurlijk getal"). We zien niet in hoe $P_1(n)$ tot $P_1(\text{succ}(n))$ leidt. We proberen daarom eerst te ontdekken wèlk kwadraat het wel zou zijn en experimenteren als volgt: $0^3 = 0^2$, $0^3 + 1^3 = 1^2$,

$0^3 + 1^3 + 2^3 = 3^2$, $0^3 + 1^3 + 2^3 + 3^3 = 6^2$, $0^3 + \ldots + 4^3 = 10^2$, $0^3 + \ldots + 5^3 = 15^2$, $0^3 + \ldots + 6^3 = 21^2, \ldots$. Wat is de rij 0, 1, 3, 6, 10, 15, 21,...? Het lijkt uit de formule $\frac{1}{2}n(n+1)$ te komen voor $n = 0,1,2,\ldots$. Probeer dus voor $P_2(n)$ te nemen

$$\sum_{k=0}^{n} k^3 = (\tfrac{1}{2}n(n+1))^2$$

en dan gaat $P_2(n) \rightarrow P_2(\mathrm{succ}(n))$ heel gemakkelijk.

9.6. Een moeilijker voorbeeld

Voor elke $n \in \mathbb{N}$ definiëren we

$$\mathbb{N}_n := \{k \in \mathbb{N} \mid k < n\} ,$$

zodat $\mathbb{N}_0 = \emptyset$, $\mathbb{N}_1 = \{0\}$, $\mathbb{N}_2 = \{0,\mathrm{succ}(0)\} = \{0,1\}$, etc. De uitspraak $P(n)$, die door inductie moet worden bewezen is:

Voor elke afbeelding $f : \mathbb{N}_n \rightarrow \mathbb{N}_n$ geldt

$$(f \text{ is injectief}) \Leftrightarrow (f \text{ is surjectief}) . \qquad (1)$$

We geven hier geen uitgewerkt bewijs, maar vermelden slechts de belangrijkste bouwstenen. Laat $f : \mathbb{N}_{\mathrm{succ}(n)} \rightarrow \mathbb{N}_{\mathrm{succ}(n)}$ en definieer $g : \mathbb{N}_{\mathrm{succ}(n)} \rightarrow \mathbb{N}_{\mathrm{succ}(n)}$ als een samengestelde afbeelding: $g = h \circ f$, waarin

$$h(n) = f(n) \quad , \quad h(f(n)) = n \quad , \quad h(k) = k \quad \text{als} \quad (k \neq n \wedge k \neq f(n)) .$$

Nu valt te bewijzen, dat

$$f \text{ is surjectief} \Leftrightarrow g \text{ is surjectief}$$
$$f \text{ is injectief} \Leftrightarrow g \text{ is injectief}$$

en daarmee is het inductiebewijs voor $P(n)$ af te ronden.

De stelling, dat (1) voor alle $n \in \mathbb{N}$ geldt, vormt een sleutel voor allerlei kennis over de $\mathbb{N}_n$'s. We noemen wat gevolgen.

(i) Als $n > m$ en $f : \mathbb{N}_n \to \mathbb{N}_m$ dan is f <u>niet</u> injectief.

(ii) Als $n < m$ en $f : \mathbb{N}_n \to \mathbb{N}_m$ dan is f <u>niet</u> surjectief.

(iii) Als $f : \mathbb{N}_n \to \mathbb{N}_m$ een bijectie is, dan is $n = m$.

Op grond van (iii) kan men over het <u>aantal</u> elementen van een eindige verzameling spreken. We noemen een verzameling S <u>eindig</u> als er een $n \in \mathbb{N}$ is en een bijectie $f : S \to \mathbb{N}_n$. Blijkens (iii) is n hierdoor eenduidig bepaald en die n noemen we het <u>aantal elementen</u> van S (soms met $|S|$ genoteerd, soms met $\#S$).

De eigenschap (i) leidt tot het zg. ladenprincipe ("Schubfachprinzip", "pigeon hole principle"): Als $m > n$, en m objecten worden in n vakjes geplaatst, dan is er ten minste één vakje dat twee objecten bevat.

Een beroemd voorbeeld: Laat ϑ een reëel getal zijn. We bewijzen dat er bij elke $n \in \mathbb{N}$ met $n > 0$ een breuk a/b is ($a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $0 < b < n$) met $|\vartheta - a/b| < (bn)^{-1}$. We bewijzen dit met het ladenprincipe. Als α een reëel getal is, dan is α^* het (eenduidig bepaalde) reële getal met $(0 \le \alpha^* < 1) \wedge (\alpha - \alpha^* \in \mathbb{Z})$. We zien nu de getallen $0^*, \vartheta^*, (2\vartheta)^*, \ldots, (n\vartheta)^*$ verdeeld over de n vakken $L_0, \ldots, L_{n-1}$, waarbij

$$L_k = \left\{ x \in \mathbb{R} \,\middle|\, \frac{k}{n} \le x < \frac{k+1}{n} \right\}.$$

Er zitten er dus tenminste twee in hetzelfde vak, bijv. $(p\vartheta)^*$ en $(q\vartheta)^*$ met $0 \le p < q \le n$. Neem $b := q - p$, $a := (p\vartheta)^* - (q\vartheta)^* - p\vartheta + q\vartheta$, dan is $0 < b \le n$, $0 \le (b\vartheta)^* < n^{-1}$, $a \in \mathbb{Z}$ en we komen snel tot het gewenste resultaat.

9.7. Recursie

Recursie is evenals inductie een doorgeefprincipe, maar waar bij inductie in zekere zin een bewijs wordt doorgegeven, wordt bij recursie een object, of zo men wil, een constructie doorgegeven. Het gaat om de constructie van een rij. (Het woord "rij" betekent niets anders dan "afbeelding met domein $\mathbb{N}$".)

Men zegt bijv. dat n! recursief gedefinieerd is door

$$0! = 1 \quad , \quad n! = n \cdot (n-1)! \quad \text{als } n > 0 \, .$$

Een ander voorbeeld: 2^n is gedefinieerd door

$$2^0 = 1 \quad , \quad 2^n = 2 \cdot 2^{n-1} \quad \text{als } n > 0 \, .$$

De rij Fibonacci-getallen is recursief vastgelegd door

$$a_0 = 1 \quad , \quad a_1 = 1 \quad , \quad a_n = a_{n-1} + a_{n-2} \quad \text{als } n > 1 \, .$$

Vaak berust de recursie op zg. iteratie, d.i. herhaling van eenzelfde afbeelding. We gaan uit van een verzameling S en een afbeelding $F : S \to S$ en vormen de rij $F_1, F_2, \ldots$ door

$$F_1 = F \quad , \quad F_n = F \circ F_{n-1} \, .$$

(Dus bijv. $F_3(x) = F(F(F(x)))$.)

We kunnen recursie in het algemeen als volgt beschrijven. S is een verzameling, g een afbeelding van $\mathbb{N} \times S$ in S. Deze g zorgt voor het doorgeven: er gaat een rij f geconstrueerd worden en als $f(n) = u$, dan wordt $f(n+1) = g(n,u)$. (In het geval van de recursieve definitie van n! is dus $g(n,u) = (n+1)u$.)

Verder is er een startwaarde a, die vastlegt wat f(0) is. Nu geldt de volgende recursiestelling:

Er is precies één afbeelding $f : \mathbb{N} \to S$ met

$$f(0) = a \wedge \forall_{n \in \mathbb{N}} (f(n+1) = g(n, f(n))) .$$

Deze stelling kan uit de axioma's van Peano worden afgeleid, waarbij ook het individualiteitsaxioma (Peano's jota) wordt gebruikt. Het is een heel gedoe en wij zullen het hier overslaan.

9.8. Constructie door recursie, bewijs door inductie

We geven een voorbeeld van een recursief geconstrueerde rij waarvoor vervolgens door inductie iets bewezen wordt. We gebruiken vrijelijk de theorie van het reëele getal. Laat

$$\mathbb{R}_+ := \{x \in \mathbb{R} \mid x > 0\}$$
$$F := \lambda_{x \in \mathbb{R}_+} (\tfrac{1}{2}x + \tfrac{1}{x}) .$$

We nemen een willekeurige startwaarde a ($a \in \mathbb{R}_+$) en itereren: a , F(a) , F(F(a)),... . We willen laten zien dat deze rij hard naar $\sqrt{2}$ convergeert. De S en g uit de recursiestelling zijn respectievelijk

$$S = \mathbb{R}_+ \quad , \quad g = \lambda_{(n,u) \in \mathbb{N} \times S} F(u) .$$

Er komt f(0) = a, f(1) = F(a), f(2) = F(F(a)),... . Volgens de recursiestelling ligt de rij f nu vast. Om te laten zien dat $|f(n) - \sqrt{2}|$ klein is als n groot is, stellen we $u_n := f(n) - \sqrt{2}$ en komen snel tot

$$u_{n+1} = u_n^2/(2(u_n + \sqrt{2})) .$$

We hebben $u_n + \sqrt{2} \in \mathbb{R}_+$, zodat $u_{n+1} > 0$. Voor $n > 0$ is dus $u_{n+1} < u_n^2/(2\sqrt{2})$, dus als we stellen

$$v_n := u_n/(2\sqrt{2}) = \frac{f(n)}{2\sqrt{2}} - \frac{1}{2},$$

dan is

$$v_{n+1} < v_n^2 .$$

Laten we de startwaarde even beperken door $\sqrt{2} < a < 2\sqrt{2}$, dan is $0 \leq v_0 < 2^{-1}$ en door inductie bewijzen we

$$0 \leq v_n < 2^{-2^n} .$$

Inderdaad convergeert v_n dus zeer snel naar 0.

9.9. Aftelbare verzamelingen

Een verzameling A heet <u>aftelbaar</u> als er een bijectie $A \to \mathbb{N}$ bestaat. Zo'n bijectie heet een <u>aftelling</u> van A.

We vermelden wat feiten zonder op argumenten in te gaan.

(i) Een deelverzameling van een aftelbare verzameling is eindig of aftelbaar.

(ii) Het cartesisch product van twee aftelbare verzamelingen is aftelbaar.

(iii) De vereniging van eindig of aftelbaar vele aftelbare verzamelingen is aftelbaar.

(iv) $\mathcal{P}_e(\mathbb{N})$, d.i. de verzameling van alle eindige deelverzamelingen van $\mathbb{N}$, is aftelbaar. Een aftelling wordt verkregen door aan elke $X \in \mathcal{P}_e(\mathbb{N})$ toe te voegen $f(X) := \sum_{k\in X} 2^k$.

(v) $\mathcal{P}(\mathbb{N})$ is <u>niet</u> aftelbaar. Algemener: als S een verzameling is en $f : S \to \mathcal{P}(S)$, dan is f <u>niet</u> surjectief (dus zeker geen bijectie). Bewijs: neem

$$T := \{x \in S \mid \neg(x \in f(x))\} .$$

Deze T komt niet in het beeld van f voor. Was nl. $y \in S$ en $f(y) = T$, dan was

$$y \in f(y) \Leftrightarrow y \in T \quad \text{en} \quad y \in T \Leftrightarrow \neg(y \in f(y)) ,$$

dus $(y \in f(y)) \Leftrightarrow \neg(y \in f(y))$ en dat levert een contradictie.

(vi) Als S eindig is, dan is elke injectie $f : S \to S$ een surjectie (zie 9.6). Bij aftelbare verzamelingen is dit niet meer het geval. De afbeelding $\lambda_{n \in \mathbb{N}}\, \mathrm{succ}(n)$ is wèl injectief maar niet surjectief.

9.10. <u>Verschil tussen "rij" en "verzameling"</u>

Als S een verzameling is, dan is "aftelbare deelverzameling van S" niet hetzelfde als "rij van elementen uit S". Een rij van elementen uit S is een afbeelding $f : \mathbb{N} \to S$. Het beeld ervan hoeft niet aftelbaar te zijn: het kan eindig zijn en zelfs een singleton.

Ook bij eindige verzamelingen en eindige rijtjes was de verwarring al mogelijk. Een rij van n reële getallen is een afbeelding van de verzameling $\{0,\dots,n-1\}$ in $\mathbb{R}$. Het beeld van die afbeelding is een deelverzameling van $\mathbb{R}$, die wel eens minder dan n elementen kan hebben. En omgekeerd, ook al heeft een deelverzameling n elementen, dan is het nog geen rij; er ontstaat pas een rij als uit de n! mogelijke bijecties op $\{1,\dots,n\}$ een keuze gemaakt wordt.

Soms heeft men de behoefte om aan elk element van een verzameling een multipliciteit toe te kennen. Men wil bijv. de deelverzameling $\{a,b,c,d,e\}$ van een verzameling S (a, b, c, d, e twee aan twee verschillend) beschouwen en daarin b en d elk dubbel tellen en e voor drie. Dit wil zeggen dat men een afbeelding $f : S \to \mathbb{N}$ beschouwt met $f(a) = 1$, $f(b) = 2$, $f(c) = 1$, $f(d) = 2$, $f(e) = 3$ en $f(x) = 0$ voor alle x buiten $\{a,b,c,d,e\}$. Zo'n afbeelding $f : S \to \mathbb{N}$ heet wel een multiset.

Aan elke rij van n elementen uit S kan men een multiset toevoegen, d.i. de multiset die aangeeft hoe vaak elk element van S in de rij optreedt. Deze multiset wordt wel de gewogen inhoud van de eerstgenoemde rij genoemd. Beschouw bijv. de rij h gegeven door $h(0) = 5$, $h(1) = 3$, $h(2) = 5$, $h(3) = 2$, $h(4) = 1$ (en h wordt als een rij elementen van $\mathbb{R}$ beschouwd), dan wordt de gewogen inhoud f beschreven door: $f(1) = 1$, $f(2) = 1$, $f(3) = 1$, $f(4) = 0$, $f(5) = 2$, $f(6) = f(7) = \ldots = 0$.

HOOFDSTUK 10. AFSLUITING VAN EEN VERZAMELING MET BETREKKING TOT ZEKERE OPERATIES

10.1. Inleiding

Een situatie die erg vaak voorkomt in de moderne wiskunde is de volgende. We hebben een verzameling U (en alles wat we gaan doen speelt zich binnen U af). En er is een operatie, die aan elk paar elementen a,b uit U een element $\varphi(a,b)$ van U toevoegt. (Een simpel voorbeeld: $U = \mathbb{R}$ en aan het paar a,b wordt $a + b$ toegevoegd.)

Een deelverzameling A van U heet <u>gesloten</u> t.o.v. φ als $\forall_{x\in A}\forall_{y\in A}(\varphi(x,y)\in A)$. Voorbeeld: de verzameling der positieve getallen in $\mathbb{R}$ is gesloten t.o.v. de optelling en ook die der gehele getallen < -5 is gesloten.

Wat nu vaak voorkomt is, dat we uitgaan van een deel R van U dat <u>niet</u> gesloten is en dat we die R door uitbreiding gesloten willen maken. De uitbreiding geschiedt stap voor stap en steeds zo dat we aan de uitgegroeide R elementen toevoegen die er in elk geval in moeten zitten als we tot een gesloten verzameling willen komen. Om precies te zijn: een element dat we toevoegen is steeds van de vorm $\varphi(a,b)$ waarbij a en b al in de uitgegroeide verzameling zitten. We willen tot een stabiele toestand komen, waarbij er niets meer uit te breiden valt,en dat wil zeggen dat de verzameling is uitgegroeid tot een verzameling die gesloten is t.o.v. φ. Deze zal onafhankelijk blijken te zijn van de volgorde der toevoegingen en de <u>afsluiting</u> van R (t.o.v. φ) worden genoemd.

In vele gevallen duurt dit groeiproces oneindig lang en dan moet de gesloten verzameling als een soort limiet worden gezien.

10.2. <u>Een voorbeeld</u>

Laat U het platte vlak zijn en R de omtrek van een cirkel met middelpunt P en straal 1. Als a en b punten zijn, dan is $\varphi(a,b)$ het punt met de eigenschap dat b het midden is van het lijnstuk met uiteinden a en $\varphi(a,b)$. We gaan R stapsgewijs uitbreiden en noemen daarom de oorspronkelijke R nu R_0 en de uitbreidingen $R_1, R_2, \ldots$.

R_1 bestaat uit de punten van R_0 plus alle punten $\varphi(a,b)$ met $a \in R_0$, $b \in R_0$. R_2 bestaat uit de punten van R_1 plus alle punten $\varphi(a,b)$ met $a \in R_1$, $b \in R_1$, enz. (De rij $R_0, R_1, R_2, \ldots$ is zo dus recursief gedefinieerd.) R_1 bestaat uit alle punten die tot P een afstand d hebben met $1 \leq d \leq 3$. R_2 uit alle punten die tot P een afstand d hebben met $d \leq 9$. R_3 idem met $d \leq 27$, enz. De vereniging van $R_0, R_1, R_2, \ldots$ is het gehele vlak U. En dat is inderdaad gesloten!

Met dezelfde operatie φ, toegepast op een andere R_0, kan soms als limietsituatie iets bereikt worden dat niet uit de gehele U bestaat. Probeer maar eens

i) R_0 bestaat slechts uit één punt ,

ii) R_0 is een puntenpaar ,

iii) R_0 bestaat uit vier punten, die de hoekpunten van een vierkant vormen ,

iv) R_0 is leeg .

In de gevallen i) en iv) is $R_0 = R_1 = R_2 = \ldots$, doordat uit die R_0 niets nieuws kan worden gebouwd.

10.3. Afsluiting met een algemener soort operatie

In de vorige paragraaf werd het begrip "gesloten" geformuleerd met een φ die aan elk paar a,b uit U een $\varphi(a,b)$ toevoegt. Met zulke $\varphi(a,b)$'s werd een verzameling als R_k uitgebreid. We generalizeren dit in verschillende richtingen.

i) We nemen bij a en b niet één $\varphi(a,b)$, waarmee we aan het uitbreiden slaan, maar een gehele verzameling $\Phi(a,b)$ van "nieuwe" elementen.

ii) In plaats van uit te gaan van paren a,b , kunnen we ook van verzamelingen van één, drie of meer elementen uitgaan.

iii) In plaats van aan te nemen dat Φ aan elke verzameling een nieuwe toevoegt, eisen we slechts, dat Φ aan sommige verzamelingen een nieuwe toevoegt.

We komen nu tot de volgende beschrijving. U is een verzameling. $P(U)$ is de verzameling van alle deelverzamelingen van U. H is een deel van $P(U)$ en Φ is een afbeelding van H in $P(U)$:

$$\Phi : H \to P(U) .$$

Voor elke $V \in H$ is dus $\Phi(V)$ een deelverzameling van U.

Voorbeelden.

(i) Het geval van 10.1 (en daarmee het voorbeeld van 10.2) laat zich onderbrengen door af te spreken, dat H de verzameling is van alle deelverzamelingen van U met één of twee elementen en dat

$$\Phi(\{x,y\}) = \{\varphi(x,y) , \varphi(y,x)\} .$$

(Deze afspraak houdt in dat $\Phi(\{x\}) = \{\varphi(x,x)\}$.)

(ii) Laat U het platte vlak zijn en H de verzameling van alle deelverzamelingen van U met precies twee elementen. Als $p \in U$, $q \in U$, $p \neq q$, nemen we voor $\Phi(p,q)$ de verzameling van alle punten die tussen p en q liggen op het lijnstuk dat p en q verbindt. Als we de hieronder volgende definitie van geslotenheid toepassen zijn de gesloten verzamelingen de verzamelingen die men gewoonlijk convex noemt. Als $R = \{p,q,r\}$, waarbij p, q, r twee aan twee verschillen, dan is de in 10.4 te bespreken rij $R_0, R_1, R_2, \ldots$ vastgelegd door $R_0 = R$, R_1 is de omtrek van de driehoek met hoekpunten p, q, r; R_2 bestaat uit omtrek verenigd met het inwendige en $R_2 = R_3 = R_4 = \ldots$. R_2 is gesloten en $R_2 = \mathrm{afsl}(R,\Phi)$, met de notatie die na Stelling 1 wordt ingevoerd.

Definitie.

Met de eerder beschreven U, H, Φ heet een deel A van U gesloten (t.o.v. Φ) als voor elke $V \in H$ met $V \subset A$ geldt dat ook $\Phi(V) \subset A$.

We kunnen nu de volgende stelling uitspreken.

Stelling 1.

Bij elke $R \in \mathcal{P}(U)$ bestaat er precies één $S \in \mathcal{P}(U)$ zó dat

i) $R \subset S$,

ii) S is gesloten t.o.v. Φ,

iii) voor elke T (met $T \in \mathcal{P}(U)$) die gesloten is t.o.v. Φ geldt

$$R \subset T \rightarrow S \subset T .$$

Men vat deze uitspraken wel samen door te zeggen dat S de minimale gesloten uitbreiding van R is. We noemen deze S kortweg de afsluiting van R en we noteren dat als

$$S = \mathrm{afsl}(R,\Phi) .$$

Het bewijs van deze stelling is niet lang, maar vereist vertrouwdheid met het werken met verzamelingsconcepten. We nemen

$$S := \{x \in U \mid \forall_{T \in \mathcal{P}(U)} (((T \text{ gesloten}) \wedge (R \subset T)) \rightarrow x \in T)\} .$$

Eerst laten we zien dat $R \subset S$: als $x \in R$, $R \subset T$, dan is $x \in T$. Ook iii) is triviaal. Nu ii). We nemen een $V \in H$ met $V \subset S$ en gaan bewijzen dat $\Phi(V) \subset S$. Laat y een element van $\Phi(V)$ zijn. Bewezen moet worden dat $y \in S$, dus dat

$$\forall_{T \in \mathcal{P}(U)} (((T \text{ gesloten}) \wedge (R \subset T)) \rightarrow y \in T) .$$

Laat $T \in P(U)$, T gesloten en $R \subset T$. Blijkens iii) is $S \subset T$, dus $V \subset T$. Daar T gesloten is en $V \in H$, is ook $\Phi(V) \subset T$ en derhalve $y \in T$. Hiermee is bewezen dat S aan ii) voldoet.

Dat er maar één S is die aan i), ii), iii) voldoet, blijkt door toepassing van iii). Als S_1 en S_2 beide voldoen, kan men eerst S_1 de rol van S en S_2 die van T laten spelen (zodat $S_1 \subset S_2$) en daarna de rollen verwisselen (zodat $S_2 \subset S_1$).

10.4. Afsluiting verkregen door recursie

We bewijzen vervolgens een stelling die in 10.2 al door voorbeelden werd gesuggereerd. We zullen ons beperken door de eis te stellen dat elke V uit H een eindige verzameling is. (In onze voorbeelden was dat al steeds het geval.) We maken met behulp van Φ nu een afbeelding Ψ die $P(U)$ afbeeldt in $P(U)$:

$$\Psi : P(U) \to P(U)$$

en die als volgt gedefinieerd is: als $A \in P(U)$, dan is $\Psi(A)$ de vereniging van A met alle $\Phi(V)$, waarbij V de deelverzamelingen van A doorloopt die ook tot H behoren:

$$\Psi(A) = A \cup \bigcup_{V \in P(A) \cap H} \Phi(V) , \tag{1}$$

of, in andere vorm opgeschreven:

$$\Psi(A) = A \cup \{x \in U \mid \exists_{V \in H} (V \subset A \wedge x \in \Phi(V))\} .$$

We laten de betekenis van Ψ even aan een voorbeeld zien. Neem $U = \mathbb{R}$, H is de verzameling van alle deelverzamelingen van $\mathbb{R}$ met precies twee elementen. We definiëren Φ door af te spreken: als $\{a,b\} \in H$, dan is $\Phi(\{a,b\}) = \{a+a\ ,\ a+b\ ,\ b+b\}$. Is nu $A \in P(U)$, dan is $\Psi(A)$ hetgeen men krijgt door aan A alle sommen van de vorm $p + q$ (met $p \in A$, $q \in A$, $p \neq q$) toe te voegen.

Terug naar het algemene geval. Als R een deelverzameling van U is, kunnen we nu recursief de rij $R_0, R_1, \ldots$ definiëren:

$$R_0 = R\ ,\ R_{n+1} = \Psi(R_n) \qquad (n \geq 0)\ . \tag{2}$$

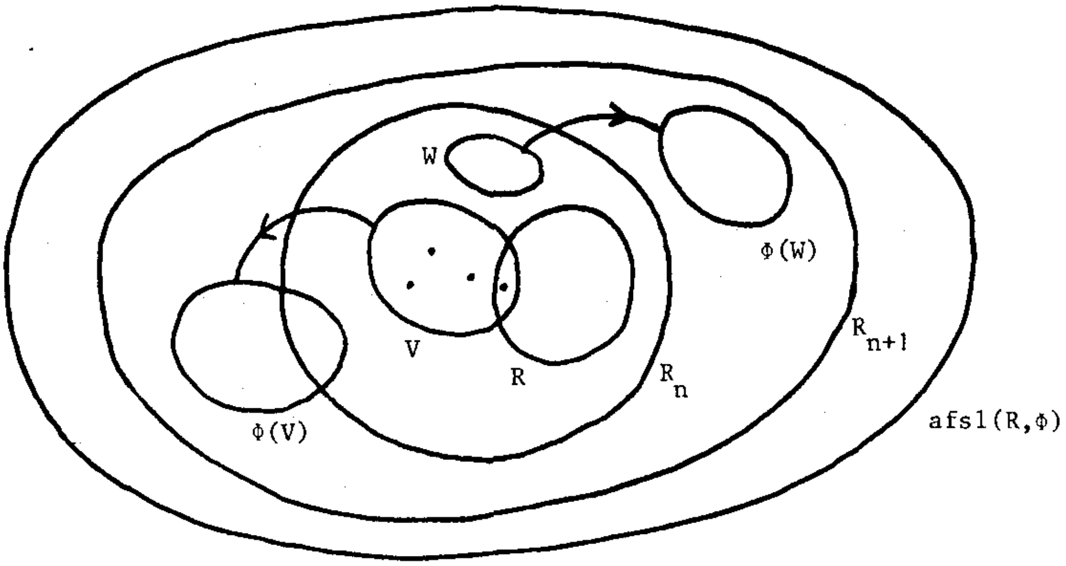
Merk op dat $R_0 \subset R_1 \subset R_2 \subset \ldots$.

Een voorbeeld hebben we al in 10.2 en 10.3 gezien.

De stelling waarop we aansturen zegt dat de vereniging van $R_0, R_1, \ldots$ precies de afsluiting van R t.o.v. Φ is. Die vereniging is

$$\{x \in U \mid \exists_{n\in\mathbb{N}}\ x \in R_n\}\ .$$

We zetten nu alles bij elkaar; in de figuur staat het een en ander geïllustreerd.



Stelling 2.

Laat U een verzameling zijn en H een verzameling van eindige deelverzamelingen van U. Laat Φ een afbeelding $H \to P(U)$ zijn, en bouw daarmee Ψ (met $\Psi : P(U) \to P(U)$) door middel van (1). Laat R een deel van U zijn en definieer $R_0, R_1, \ldots$ door (2). Dan is

$$\mathrm{afsl}(R,\Phi) = \bigcup_{n\in\mathbb{N}} R_n .$$

Om deze stelling te bewijzen, stellen we $\bigcup_{n\in\mathbb{N}} R_n$ door S voor en we controleren de punten i), ii), iii) van Stelling 1. Daar $R = R_0 \subset R_1 \subset \ldots$ is kennelijk $R \subset S$. Nu ii): We nemen een $V \in H$ met $V \subset S$ en moeten laten zien dat $\Phi(V) \subset S$. Als y een element van V is, dan zit y in de vereniging van $R_0, R_1, \ldots$, dus bij y is een $n \in \mathbb{N}$ te vinden met $y \in R_n$. Daar V een eindige verzameling is, kunnen we van alle n's die bij de y's uit V optreden, de grootste nemen. Noemen we die N, dan is $y \in R_N$ voor alle $y \in V$. Dus $V \subset R_N$. Hieruit volgt (zie (1)) dat $\Phi(V) \subset \Psi(R_N)$, dus $\Phi(V) \subset R_{N+1}$, dus $\Phi(V) \subset S$.

Tenslotte kijken we naar iii). Laat T gesloten zijn t.o.v. Φ, en $R \subset T$. Ons doel is $S \subset T$. Daartoe bewijzen we dat

$$\forall_{n\in\mathbb{N}}\, R_n \subset T . \tag{3}$$

We doen dat door volledige inductie. Om te beginnen $R_0 \subset T$ (want $R \subset T$ en $R_0 = R$). Laat vervolgens $n \in \mathbb{N}$ en $R_n \subset T$. We zullen aan onze plicht voldaan hebben als we $R_{n+1} \subset T$ hebben afgeleid. Dit betekent $\Psi(R_n) \subset T$. Om dat te laten zien, kijken we naar (1). Het is voldoende om te bewijzen dat $R_n \subset T$ (maar dat weten we al) en dat voor elke $V \in P(R_n) \cap H$ geldt $\Phi(V) \subset T$. Zo'n V voldoet aan $V \in H$ en aan $V \subset R_n$, dus wegens $R_n \subset T$ ook aan $V \subset T$. Daar T gesloten is t.o.v. Φ (zie de definitie in 10.3) is nu ook $\Phi(V) \subset T$. Daarmee is het bewijs voltooid.

Geruststelling. Er wordt niet verwacht dat de student in het eerste trimester bewijzen als die van Stelling 1 en Stelling 2 kan reproduceren of zelf kan vinden. De wat meer geoefende wiskundige heeft er weinig moeite mee.

10.5. Enkele toepassingen

Er zijn verschillende consequenties van Stelling 1 en 2, die minder moeite kosten dan die stellingen zelf. We noemen

1. Als $S_1 \subset S_2 \subset U$, dan is

$$\mathrm{afsl}(S_1,\Phi) \subset \mathrm{afsl}(S_2,\Phi) .$$

2. Als R gesloten is t.o.v. Φ, dan is

$$\mathrm{afsl}(R,\Phi) = R .$$

3. Als $R \subset U$, dan is

$$\mathrm{afsl}(\mathrm{afsl}(R,\Phi),\Phi) = \mathrm{afsl}(R,\Phi) .$$

4. Als $\Phi(\emptyset) = \emptyset$, dan is

$$\mathrm{afsl}(\emptyset,\Phi) = \emptyset .$$

5. Als voor alle $V \in H$ geldt $\Phi(V) \in V$, dan is

$$\mathrm{afsl}(R,\Phi) = R \quad \text{voor alle } R \in \mathcal{P}(U) .$$

6. Als $U = \mathbb{N}$, $H = \{\{n\} \mid n \in \mathbb{N}\}$, $\Phi(\{n\}) = \{n+1\}$, $R = \{0\}$, dan zijn de R_n (gedefinieerd met (2)) te vinden:

$$R_n = \{k \in \mathbb{N} \mid 0 \le k \le n\}$$

en $\mathrm{afsl}(R,\Phi) = \mathbb{N}$.

7. Als $R \in P(U)$, $V \in H$, $V \subset \mathrm{afsl}(R,\Phi)$, dan is

$$\mathrm{afsl}(V,\Phi) \subset \mathrm{afsl}(R,\Phi) .$$

8. Als naast $\Phi : H \to P(U)$ ook $\theta : H \to P(U)$, en als voor alle $V \in H$ geldt $\Phi(V) \subset \mathrm{afsl}(V,\theta)$, dan geldt voor elke $R \in P(U)$ dat $\mathrm{afsl}(R,\theta)$ gesloten is t.o.v. Φ en $\mathrm{afsl}(R,\Phi) \subset \mathrm{afsl}(R,\theta)$. (Aanwijzing: om te laten zien dat $\mathrm{afsl}(R,\theta)$ gesloten is t.o.v. Φ nemen we een $V \in H$, $V \subset \mathrm{afsl}(R,\theta)$ en laten we zien dat $\Phi(V) \subset \mathrm{afsl}(R,\theta)$; wegens $\Phi(V) \subset \mathrm{afsl}(V,\theta)$ is het voldoende Voorbeeld 7 toe te passen (met vervanging van Φ door θ).)

9. Onderstel

(i) $\Phi(\emptyset) = \emptyset$,

(ii) voor alle $V \in H$ en alle V_1 met $V_1 \subset V$ geldt $V_1 \in H$, $V \setminus V_1 \in H$,
$\Phi(V) \subset \Phi(V_1) \cup \Phi(V \setminus V_1)$,

dan hebben we ook

(iii) $\emptyset$ en U zijn gesloten,

(iv) de vereniging van twee gesloten verzamelingen is gesloten,

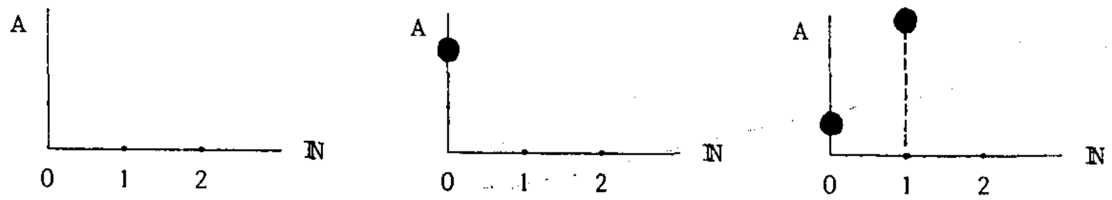
(v) de doorsnede van willekeurig veel gesloten verzamelingen is gesloten.

("Gesloten" betekent hier "gesloten t.o.v. Φ".) De eigenschappen (iii), (iv), (v) karakteriseren de situatie die men een "topologie" noemt.

HOOFDSTUK 11. DE VRIJE MONOÏDE A^* GEGENEREERD DOOR EEN VERZAMELING A

11.1. De verzameling A^*

Laat A een verzameling zijn. Als $n \in \mathbb{N}$ $(\mathbb{N} = \{0,1,\ldots\})$, dan beschouwen we de verzameling $\mathbb{N}_n$ van de elementen $k \in \mathbb{N}$ met $0 \leq k < n$. Onder A^*_n verstaan we de verzameling van alle afbeeldingen van $\mathbb{N}_n$ in A. Zo'n afbeelding stellen we door een griekse letter φ voor; als bijv. resp. $n = 0,1,2$, zijn voorbeelden:



φ_0 φ_1 φ_2

We hebben $\varphi_0 \in A^*_0$, $\varphi_1 \in A^*_1$, $\varphi_2 \in A^*_2$. Laat ons afbeeldingen als $\varphi_0, \varphi_1, \varphi_2, \ldots$ opvatten als deelverzamelingen van het cartesisch product $\mathbb{N} \times A$. Dan kunnen we zeggen dat φ_0 de lege deelverzameling van $\mathbb{N} \times A$ is (zie 7.10). We zullen meestal ε schrijven i.p.v. φ_0. En als $n \in \mathbb{N}$, dan kan A^*_n beschreven worden als de verzameling van alle deelverzamelingen φ van $\mathbb{N} \times A$ met de eigenschap dat bij elke $k \in \mathbb{N}$ met $0 \leq k < n$ er precies één $a \in A$ is met $(k,a) \in \varphi$, en bij elke $k \in \mathbb{N}$ met $k \geq n$ er geen enkele $a \in A$ is met $(k,a) \in \varphi$.

A^*_0 is de verzameling die slechts uit ε bestaat, dus $A^*_0 = \{\varepsilon\}$. De ε is een lege verzameling, maar A^*_0 is niet leeg. A^*_0 bevat precies één element.

De vereniging van $A^*_0, A^*_1, A^*_2, \ldots$ noemen we A^*.

De A^*_i hebben onderling niets gemeen:

$$\forall_{i \in \mathbb{N}} \forall_{j \in \mathbb{N}} (i \neq j \rightarrow A^*_i \cap A^*_j = \emptyset) .$$

Als $\varphi \in A^*$, dan is er precies één $k \in \mathbb{N}$ zó dat $\varphi \in A^*_k$. Deze k noemen we de lengte van φ, notatie $\ell(\varphi)$. Dus met Peano's jota-notatie:

$$\ell(\varphi) \;=\; \text{jota}(\{k \in \mathbb{N} \mid \varphi \in A^*_k\}) \;.$$

Duidelijk is

$$\ell(\varepsilon) = 0 \;.$$

De elementen van A^*_1 moeten niet met die van A verward worden. Er is wèl een eenvoudige bijectie σ van A op A^*_1, gegeven door

$$\sigma(a) = \{(0,a)\}$$

voor alle $a \in A$.

Duidelijk is dat

$$\ell(\sigma(a)) = 1$$

voor alle $a \in A$.

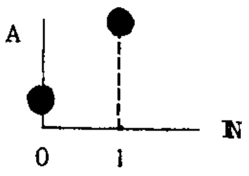
We zullen later i.p.v. $\sigma(a)$ steeds "string(a)" schrijven, omdat dit laatste overeenstemt met een nog te bespreken notatie string(a,b), string(a,b,c), enz.

11.2. Concatenatie

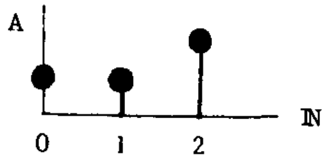
Laat $n \in \mathbb{N}$, $m \in \mathbb{N}$, $\varphi \in A^*_n$, $\psi \in A^*_m$. We vormen nu een $\vartheta \in A^*_{n+m}$ door

$$\vartheta(k) = \begin{cases} \varphi(k) & \text{als } 0 \le k < n \\ \psi(k-n) & \text{als } n \le k < n+m \,. \end{cases}$$

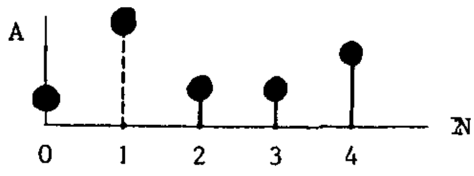
Voorbeeld (met $n=2$, $m=3$).



φ



ψ



ϑ

Deze ϑ heet de concatenatie van φ en ψ, notatie

$$\vartheta = \text{concat}(\varphi,\psi) \ .$$

In het algemeen is $\text{concat}(\varphi,\psi) \neq \text{concat}(\psi,\varphi)$.

Als ε weer het element van A_0^* is, dan geldt voor alle $\varphi \in A^*$

$$\text{concat}(\varepsilon,\varphi) = \text{concat}(\varphi,\varepsilon) = \varphi \ .$$

Uit de definitie van "concat" volgt, dat voor alle $\varphi \in A^*$, $\psi \in A^*$

$$\ell(\text{concat}(\varphi,\psi)) = \ell(\varphi) + \ell(\psi) \ .$$

11.3. Associativiteit

Als $\xi \in A^*$, $\eta \in A^*$, $\zeta \in A^*$, en we stellen

$$\varphi := \text{concat}(\xi,\eta) \ , \qquad \psi := \text{concat}(\eta,\zeta) \ ,$$

$$\vartheta := \text{concat}(\varphi,\zeta) \ , \qquad \rho := \text{concat}(\xi,\psi) \ ,$$

dan is $\vartheta = \rho$. Met andere woorden

$$\text{concat}(\xi,\text{concat}(\eta,\zeta)) = \text{concat}(\text{concat}(\xi,\eta),\zeta) \ . \qquad (1)$$

Dit noemen we de <u>associatieve eigenschap</u>. We kunnen dit precies nagaan door af te korten $p := \ell(\xi)$, $q := \ell(\eta)$, $r := \ell(\zeta)$ en in elk der intervallen

$$0 \le i < p \quad , \quad p \le i < p+q \quad , \quad p+q \le i < p+q+r$$

te laten zien dat $\vartheta(i) = \rho(i)$. We laten de volledige controle hier achterwege.

We zullen de leden van (1) voorstellen door

$$\text{concat}(\xi,\eta,\zeta) \tag{2}$$

op dezelfde manier als we bij reële getallen $x + y + z$ schrijven en dat naar believen als $(x+y) + z$ of als $x + (y+z)$ kunnen opvatten.

We kunnen ook verder gaan en definiëren

$$\text{concat}(\xi,\eta,\zeta,\omega) \;:=\; \text{concat}(\text{concat}(\xi,\eta,\zeta),\omega) \;,$$

maar in plaats van het rechterlid kunnen we ook andere dingen schrijven, evenals bij $x + y + z + w = (x+y+z) + w = x + (y+z+w) = (x+y) + (z+w)$, enz. Men bedenke echter dat de optelling ook nog commutatief is en dat dit voor de concatenatie niet geldt.

Men "overtuige" zich nog van bijv.

$$\text{concat}(\xi_1,\ldots,\xi_{n+m}) = \text{concat}(\text{concat}(\xi_1,\ldots,\xi_n),\text{concat}(\xi_{n+1},\ldots,\xi_{n+m})) .$$

Wanneer men A^* beschouwt met de binaire operatie "concat", noemt men het "de <u>vrije monoïde</u> over A", of "de vrije monoïde gegenereerd door A".

We bekijken nog even twee triviale gevallen:

(i) Als A zelf leeg is, dan zijn $A_1^*, A_2^*, \ldots$ leeg, maar A_0^* is niet leeg: $A_0^* = \{\varepsilon\}$.

(ii) Als A precies één element heeft, dus bijv. $A = \{a\}$, dan heeft voor elke $n \in \mathbb{N}$ de A_n^* precies één element, nl. de φ met domein $\mathbb{N}_n$ en daarop de constante waarde a: $\varphi(k) = a$ als $0 \le k < n$.

11.4. De notatie "string"

Als $x \in A$, dan is $\sigma(x) \in A_1^*$. Als x, y, z elementen van A zijn, dan kunnen we $\sigma(x)$, $\sigma(y)$, $\sigma(z)$ concateneren en het resultaat noemen we string(x,y,z):

$$\text{string}(x,y,z) \;:=\; \text{concat}(\sigma(x)\,,\,\sigma(y)\,,\,\sigma(z))\;. \tag{1}$$

Analoog

$$\text{string}(x,y) \;:=\; \text{concat}(\sigma(x)\,,\,\sigma(y)) \tag{2}$$

en algemeen voor $n \geq 1$

$$\text{string}(x_1,\ldots,x_n) \;:=\; \text{concat}(\sigma(x_1),\ldots,\sigma(x_n))\;. \tag{3}$$

Als consequentie van (3) noteren we (bij $n = 1$)

$$\text{string}(x) \;=\; \sigma(x)\;. \tag{4}$$

Het geval $n = 0$ is bij (3) echter uitgesloten.

Ter oefening met deze notatie geven we wat voorbeelden:

$$\text{string}(x,y,z) = \{(0,x),(1,y),(2,z)\}\,, \tag{5}$$

$$\text{string}(x,y,x,y) = \text{concat}(\text{string}(x,y),\text{string}(x,y))\,, \tag{6}$$

$$\ell(\text{string}(x_1,\ldots,x_n)) = n \qquad (n \geq 1)\,, \tag{7}$$

$$\text{concat}(\text{string}(x),\varepsilon) = \text{string}(x)\;. \tag{8}$$

11.5. Inhoud en gewogen inhoud

Als $\varphi \in A^*$ en $\ell(\varphi) = n$, dan is φ een afbeelding die aan $0,\dots,n-1$ resp. $\varphi(0),\dots,\varphi(n-1)$ toevoegt. De verzameling van deze elementen wordt de inhoud van φ genoemd:

$$\text{inhoud}(\varphi) \ := \ \{\varphi(0),\dots,\varphi(n-1)\} \ .$$

Zodra er onder $\varphi(0),\dots,\varphi(n-1)$ twee gelijke voorkomen, heeft deze verzameling minder dan n elementen. Voorbeeld:

$$\text{inhoud}(\text{string}(x,y,x,z)) \ = \ \{x,y,x,z\} \ = \ \{x,y,z\} \ .$$

Hiermee is nog niet gezegd dat deze verzameling drie elementen heeft. Als bijv. $x = y = z$, heeft zij maar één element.

We merken nog op dat $\text{inhoud}(\varepsilon) = \emptyset$.

De gewogen inhoud van de in het begin van deze paragraaf genoemde φ is een afbeelding $f : A \to \mathbb{N}$, dus een multiset (zie 9.10). Deze functie geeft voor elke $x \in A$ aan hoe vaak x in φ "voorkomt", d.w.z. voor hoeveel k (met $k \in \mathbb{N}$, $0 \le k < n$) geldt dat $\varphi(k) = x$:

$$f(x) = \#_{k \in \mathbb{N} \mid 0 \le k < \ell(\varphi)} (\varphi(k) = x) \ ,$$

of, nu eens met λ-notatie:

$$f \ = \ \lambda_{x \in A} \#_{k \in \mathbb{N} \mid 0 \le k < \ell(\varphi)} (\varphi(k) = x) \ .$$

Ter oefening met deze notatie nog:

(i) Als f de gewogen inhoud van φ is en S de inhoud van φ, dan is

$$S \ = \ \{x \in A \mid f(x) > 0\} \ .$$

(ii) Als f, g, h resp. de gewogen inhoud van φ, ψ en concat(φ,ψ) zijn, dan is

$$\forall_{x\in A}(f(x)+g(x) = h(x)) ,$$

en verder is

$$\text{inhoud}(\varphi) \cup \text{inhoud}(\psi) = \text{inhoud}(\text{concat}(\varphi,\psi)) .$$

(iii) De inhoud van ε is leeg en de gewogen inhoud is $\lambda_{x\in A}0$ ("de gewogen inhoud is identiek nul").

(iv) Als $\varphi \in A^*$, $\psi \in A^*$, dan hebben concat(φ,ψ) en concat(ψ,φ) dezelfde inhoud en dezelfde gewogen inhoud.

(v) Als $A = \{p\}$, $\varphi \in A^*$, dan is

$$\text{inhoud}(\varphi) = \begin{cases} A & \text{als} \quad \ell(\varphi) > 0 , \\ \emptyset & \text{als} \quad \ell(\varphi) = 0 \end{cases}$$

en als f de gewogen inhoud van φ is, dan is $f = \lambda_{x\in A}\ell(\varphi)$.

(vi) Als $A = \{p,q,r\}$ en p, q, r zijn twee aan twee verschillend en $\varphi \in A^*$, met gewogen inhoud f, dan is

$$\ell(\varphi) = f(p) + f(q) + f(r) .$$

(vii) Als $A = \{p,q,r\}$ en p, q, r zijn twee aan twee verschillend, en als f de afbeelding van A in $\mathbb{N}$ is met $f(p) = 3$, $f(q) = 0$, $f(r) = 2$, dan zijn er 10 verschillende $\varphi \in A^*$ die f als gewogen inhoud hebben. Het zijn string(p,p,p,r,r), string(p,p,r,p,r), string(p,p,r,r,p), string(p,r,p,p,r), string(p,r,p,r,p), string(p,r,r,p,p), string(r,p,p,p,r), string(r,p,p,r,p), string(r,p,r,p,p), string(r,r,p,p,p).

(viii) Als $p \in A$, $q \in A$ en als concat(string(p,q),string(q,p)) dezelfde gewogen inhoud heeft als string(p,p,q,p), dan is $p = q$.

(ix) Als $n \geq 1$, $p_1 \in A,\ldots,p_n \in A$, $q_1 \in A,\ldots,q_n \in A$ en

$$\text{string}(p_1,\ldots,p_n) = \text{string}(q_1,\ldots,q_n) ,$$

dan is $(p_1 = q_1) \wedge \ldots \wedge (p_n = q_n)$.

11.6. De operatie CONCAT

Laat S en T deelverzamelingen van A^* zijn. Dan definiëren we CONCAT(S,T) als de verzameling van alle concat(φ,ψ) met $\varphi \in S$, $\psi \in T$:

$$\text{CONCAT}(S,T) = \{\text{concat}(\varphi,\psi) \mid \varphi \in S,\ \psi \in T\} .$$

We vermelden enkele consequenties:

(i) Als $S = \emptyset$ is, dan is CONCAT(S,T) $= \emptyset$, want er kunnen nu geen paren φ,ψ met $\varphi \in S$, $\psi \in T$ worden gevormd.

(ii) CONCAT(A_0^*,T) = CONCAT(T,A_0^*) = T aangezien concat(ε,ψ) = concat(ψ,ε) = ψ.

(iii) Als $\varphi \in A^*$, $\psi \in A^*$, dan is

$$\text{CONCAT}(\{\varphi\},\{\psi\}) = \{\text{concat}(\varphi,\psi)\} .$$

(iv) Als S, T, U deelverzamelingen van A^* zijn, dan is

$$\text{CONCAT}(S,\text{CONCAT}(T,U)) = \text{CONCAT}(\text{CONCAT}(S,T),U) . \qquad (1)$$

Op grond van deze nieuwe associatieve regel schrijven we nu ook weer

CONCAT(S,T,U)

in plaats van de beide leden van (1).

Als toepassingen van de notatie CONCAT merken we op dat $\mathrm{CONCAT}(A_n^*, A_m^*) = A_{n+m}^*$ en $\mathrm{CONCAT}(A^*, A^*) = A^*$.

Tenslotte nog een voorbeeldje. Als $A = \{p,q,r,s\}$ en

$$U = \{\mathrm{string}(p,p)\ ,\ \mathrm{string}(q,p,r)\}$$

$$V = \{\mathrm{string}(p,p)\ ,\ \mathrm{string}(p,q,r)\}\ ,$$

dan is

$$\mathrm{CONCAT}(U,V) = \{\mathrm{string}(p,p,p,p)\ ,\ \mathrm{string}(p,p,p,q,r)\ ,\ \mathrm{string}(q,p,r,p,p)\ ,\ \mathrm{string}(q,p,r,p,q,r)\}\ .$$

Deze verzameling CONCAT(U,V) heeft 3 of 4 elementen. Als $p = q = r$, zijn het er 3. In alle andere gevallen zijn het er vier.

11.7. Taal en metataal

We komen nu tot een netelige kwestie: we willen de elementen van A interpreteren als "letters" en die van A^* als "woorden": Het is netelig omdat we met behulp van onze wiskundige taal over taal willen spreken en daarbij worden de zaken gemakkelijk door elkaar gehaald.

Een moeilijkheid is hierbij dat we van onze wiskundige taal slechts een paar fragmenten (zoals propositie- en predikatenlogica, contextvlaggen) goed hebben beschreven. Voor de rest hebben we ons (bijv. in de voorafgaande paragrafen 11.1 - 11.6) bij het gewone wiskundige gebruik aangesloten. Niettemin geeft die gewone wiskundige ervaring wel het gevoel dat er naast de wiskundige taal, waarin we over wiskundige objecten spreken (of denken te spreken), een taal is ("metataal" genaamd), waarmee we over dat wiskundige taalbedrijf spreken. Een dergelijke metataal hebben we in Hoofdstuk 1 (Syntactische Aangelegenheden) zoveel mogelijk vermeden door het gesprek over bomen e.d. aan de informele kant te houden, maar zodra er wiskundige redeneringen, definities, stellingen over die bomen nodig zijn, komt er een formele wiskundige metataal tot stand.

Zowel in de taal als in de metataal gelden duidelijk afspreekbare spelregels. Men dient zich in elk van die talen aan de eigen spelregels te houden, ondanks de verleidingen die opkomen doordat (i) de spelregels uit de verschillende talen soms een bedrieglijke gelijkenis vertonen of doordat (ii) vaak eenzelfde symbool in beide talen gebruikt wordt.

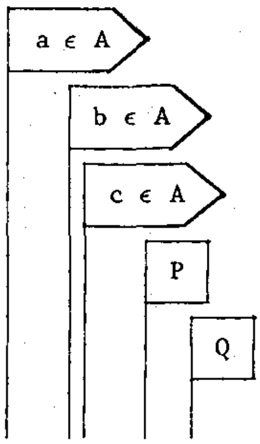
Het is vaak moeilijk of zelfs ondoenlijk taal en metataal goed uit elkaar te houden. We zijn er nl. aan gewend geraakt, ons in de wiskundige taal slap uit te drukken: wanneer we op de vingers getikt worden, trekken we ons snel op een veiliger basis terug. "Als a, b, c proposities zijn, dan zijn tenminste twee ervan equivalent". Dit is al metatalig, doordat we de letters a, b, c aan het tellen zijn, door iets te zeggen over twee van de drie. Het woord "equivalent" daarentegen, behoort tot de taal en niet tot de metataal. Wanneer we hierover op de vingers getikt worden, trekken we ons snel terug op de veiliger formulering: "als a, b, c proposities zijn, dan is $(a \Leftrightarrow b) \vee (b \Leftrightarrow c) \vee (c \Leftrightarrow a)$. Een ander voorbeeld: "laat n een natuurlijk getal zijn, $n > 1$, en laat $x_1, \ldots, x_n$ reële getallen zijn". We zijn niet in staat om n vlaggen te tekenen als we niet weten hoe groot n is. De ervaren wiskundige zet zoiets dan ook onmiddellijk om in: "laat v een element van R^n zijn", zodat er nog maar één vlag over is.

Wanneer we op formele wijze over formules willen redeneren, gaan we de metataal ernstig nemen en er wiskunde in gebruiken. De wiskunde, die we erin gebruiken is een stukje theorie over vrije monoïden zoals die in de Paragrafen 11.1 - 11.6 werd besproken.

11.8. Taalinterpretatie van de vrije monoïde

We zullen de elementen van A "symbolen" noemen en die van A^* "symboolrijen". Vaak spreekt men over "letters" i.p.v. "symbolen" en over "woorden" i.p.v. "symboolrijen" maar dat zullen we voorlopig vermijden. Ook spreekt men over A als over "het alfabet".

Hoe moeten we nu in onze monoïde-theorie bijv. over een alfabet met drie elementen spreken? De moeilijkheid is niet speciaal aan monoïden gebonden, maar treedt algemeen op bij verzamelingen. Probeer: "Laat A een verzameling zijn met drie elementen. Noem die a, b, c". Dit laatste is merkwaardig. Welk van de drie noemen we a? In fysische situaties kunnen we een element uit een groepje van drie aanwijzen, maar in wiskundige taal gaat dat niet. We moeten niet doen of we een element aanwijzen en daaraan de naam a hechten, want het aanwijzen kan alleen maar gebeuren nà dat we namen hebben! Bevredigender is het om met vlaggen te werken en drie variabelen op te voeren:



waarin P uitdrukt:

$$(a \neq b) \wedge (b \neq c) \wedge (c \neq a)$$

en Q voorstelt

$$\forall_{x \in A} (x = a \vee x = b \vee x = c) \, .$$

Binnen deze context van vijf vlaggen leven we nu met een verzameling A, die de drie verschillende elementen a , b, c bevat en geen andere.

De elementen van A^{*} zijn, voor zover hun lengte > 1 is, allemaal te krijgen door concatenatie van symboolrijen met lengte 1. Laatstgenoemde werden in II.1 met $\sigma(x)$ aangeduid: als $x \in A$, dan is $\sigma(x)$ $(= \{(0,x)\})$ een symboolrij met lengte 1.

Vervolgens kunnen we (binnen de bovengenoemde vijfvlaggencontext) symboolrijen bouwen als string(b,c), string(b,a,a).

Binnen onze vijfvlaggencontext kunnen we drie verschillende symboolrijen van de lengte 1 maken, 3^2 van de lengte 2, enz. Een symboolrij met lengte 4 is bijv. string(a,b,a,a).

Nu gaan we de symboolrijen waarover in onze wiskundige taal (binnen de vijf vlaggen) gesproken wordt, interpreteren, hetgeen wil zeggen dat we ze verbinden met wat er in een fysische werkelijkheid te zien valt. We nemen fysische objecten waarvan we naar willekeur copieën kunnen maken; die copieën kunnen we rangschikken in rijtjes, waarbij duidelijk is wat "links" en wat "rechts" is. Neem bijv. de duidelijk verschillende objecten Δ, □, $ (maar het zouden ook de Vesuvius, de stad Amsterdam en de planeet Mars mogen zijn en we zeggen dit om duidelijk te maken dat we het over objecten hebben en niet over symbolen die objecten aanduiden).

Binnen onze vijfvlaggencontext gaan we nu interpreteren. We interpreteren a als Δ, b als □, c als $ en vervolgens bijv.

string(a,b,a)	als	Δ□Δ
string(c,c,c,b)	als	$$$□

enz. "Concatenatie" wordt dus geïnterpreteerd als het "gewoon naast elkaar zetten" van rijtjes van objecten.

Meestal denkt men aan gewone lettertekens i.p.v. de symbolen Δ, $\square$, \$. Dat heeft het grote gevaar, dat die lettertekens moeilijk te onderscheiden zijn van de letters die we in onze wiskundige taal gebruiken. Om de verwarring compleet te maken gaat men vaak in de wiskundige vlaggentekst precies diezelfde letters gebruiken, zodat de bovengenoemde interpretatie een identificatie schijnt te worden. Bovendien gaat men concatenatie door gewoon naastelkaarschrijven noteren.

Als afkortende notaties zijn deze gevaarlijke gewoonten misschien te tolereren, maar men moet eerst weten wáár het de afkortende notaties van zijn. Vaak helpt het om weer even te denken aan de Δ, $\square$, \$.

Het gewoon naast elkaar schrijven (i.p.v. concatenatie serieus te noteren) heeft vele bezwaren, zeker als men het zowel voor string(x,y,z) als voor concat(ξ,η,ζ), als voor CONCAT(S,T,U) doet.

Het gebruik van letters i.p.v. de symbolen Δ, $\square$, \$ heeft niets te maken met de vrijheid om in de wiskundige taal letters als variabelen te gebruiken. We kunnen binnen onze vijfvlaggencontext bijv. zeggen: laat x een element van A zijn. Neem aan dat $x \neq b$. Met "neem aan dat $x \neq \square$" zijn we daarentegen taal en interpretatie aan het vermengen. Wanneer men i.p.v. Δ, $\square$, \$ gewone letters neemt wordt het nog gekker. Bijv. "laat A het Latijnse alfabet van 26 letters zijn. Laat x een element van A zijn en onderstel dat $x \notin \{u,v,w,x,y,z\}$". Links is x een variabele, rechts een object.

Ook wanneer men in de interpretatie van A symbolen neemt die geen letters zijn, maar die wel in de wiskundige taal een vaste betekenis hebben (zoals 0,1,2,3,4,5,6,7,8,9), is verwarring mogelijk. Men kan rustig in de wiskundige taal der vrije monoïden zeggen: laat A de deelverzameling van $\mathbb{N}$ zijn gegeven door $A = \{0,1,2\}$. Vervolgens hecht men dan aan het natuurlijke getal 0 als interpretatie het cijfersymbool 0, aan het natuurlijke getal 1 als interpretatie het cijfersymbool 1, enz. Dit geeft allerlei verwarring tussen het begrip "natuurlijk getal" en "getalrepresentatie", met als gevaarlijke tussenvorm "natuurlijk getal in decimale representatie"! Wanneer men de zaken goed wil scheiden, zal het helpen om aan de kant van de interpretatie symbolen als □, Δ, $ te gebruiken i.p.v. symbolen die in de wiskundige taal al iets voorstellen. Men interpreteert dan bijv. string(2,0,1,2) als het rijtje $□Δ$.

Dit soort kwesties zal opkomen in 12.7.

We hebben behoefte aan korte termen in plaats van "element van A" en "element van A^*". Uit het voorafgaande zal duidelijk zijn dat de termen "letter" en "woord" misverstanden kunnen oproepen, doordat ze in meer dan één taal kunnen worden gebruikt. Toch zijn het handzame termen en daarom zullen we als een soort compromis deze termen wèl vaak gebruiken, maar steeds tussen aanhalingstekens zetten. In gevallen met gevaar voor misverstand (zoals bij: neem aan dat de "letter" x verschilt van de "letters" a, b en c), kunnen we altijd weer terugvallen op de terminologie die A en A^* gebruikt.

De notaties met string, concat en CONCAT geven nogal wat schrijfwerk. Om dit wat te verminderen, stellen we voor toe te laten als notaties

$\lceil a \mid b \mid c \rceil$	voor	string(a,b,c)
$\overline{\lceil \alpha \mid \beta \mid \gamma \rceil}$	voor	concat(α,β,γ)
$\boxed{U \mid V \mid W}$	voor	CONCAT(U,V,W)

en natuurlijk evenzo in gevallen met 1,2,4,... symbolen. In het bijzonder is

$\lceil a \rceil = \sigma(a)$, $\overline{\lceil \alpha \rceil} = \alpha$, $\boxed{U} = U$.

In het begin van deze paragraaf hebben we de vlaggeninterpretatie gegeven van "Laat A een verzameling zijn met drie elementen. Noem die a, b, c". We noemen hier twee alternatieven voor deze vlaggeninterpretatie.

(i) "Laat A een verzameling zijn met drie elementen. Laat f een bijectie $\{0,1,2\} \to A$ zijn. Kort af $a := f(0)$, $b := f(1)$, $c := f(2)$". Nu speelt zich alles af binnen de context van f.

(ii) Waarom zouden we die moeite met een ongespecificeerde verzameling A nemen? Eenvoudiger is: "$A := \{0,1,2\}$; definieer a, b, c door $a := 0$; $b := 1$; $c := 2$". Het invoeren van a, b, c is natuurlijk overbodig, maar het brengt ons weer in de sfeer van het "Noem die a, b, c".

HOOFDSTUK 12. CONTEXTVRIJE GRAMMATICA'S

12.1. Locale vervanging

Laat A^* de vrije monoïde over de verzameling A zijn. We nemen een $\varphi \in A^*$, $\varphi \neq \varepsilon$, een natuurlijk getal i met $0 \leq i < \ell(\varphi)$ en een $\beta \in A^*$. We maken nu een nieuw element van A^*, aan te duiden met $\mathrm{lv}(\varphi,i,\beta)$ (lv te lezen als "locale vervanging"). Het ontstaat door de "letter" op plaats i in het "woord" φ te vervangen door het "woord" β. Een precieze beschrijving is als volgt. We kunnen schrijven

$$\varphi = \mathrm{concat}(\alpha,\mathrm{string}(b),\gamma) \qquad \left(= \boxed{\;\alpha\; \mid \boxed{b} \mid \;\gamma\;}\right)$$

met $\alpha \in A^*$, $\gamma \in A^*$, $b \in A$, $\ell(\alpha) = i$, $\ell(\gamma) = \ell(\varphi) - i - 1$. Deze α, γ en b zijn hierdoor eenduidig bepaald. Het kan gebeuren dat $\alpha = \varepsilon$ (als $i = 0$, dus $\ell(\alpha) = 0$) en ook dat $\gamma = \varepsilon$ (als $i = \ell(\varphi) - 1$, dus $\ell(\gamma) = 0$) en ook kan het voorkomen dat $\alpha = \gamma = \varepsilon$ (als $\ell(\varphi) = 1$, $i = 0$). Nu definiëren we

$$\mathrm{lv}(\varphi,i,\beta) := \mathrm{concat}(\alpha,\beta,\gamma)\ .$$

We merken nog op dat voor de lengten steeds geldt

$$\ell(\mathrm{lv}(\varphi,i,\beta)) = \ell(\varphi) + \ell(\beta) - 1 .$$

<u>Voorbeelden</u>. Laat $p \in A$, $q \in A$, $r \in A$, $\varphi \in A^*$. Dan is

$$\mathrm{lv}(\boxed{p\mid q\mid r}\ , 1\ , \boxed{p\mid p}) = \boxed{p\mid p\mid p\mid r}$$

$$\mathrm{lv}(\boxed{p\mid q\mid r}\ , 0\ , \varepsilon) = \boxed{q\mid r}$$

$$\mathrm{lv}(\boxed{p\mid q\mid r}\ , 2\ , \varepsilon) = \boxed{p\mid q}$$

$$\mathrm{lv}(\boxed{p}\ , 0\ , \varphi) = \varphi$$

$$\mathrm{lv}(\boxed{p\mid p\mid p}\ , 1\ , \varphi) = \mathrm{concat}(\mathrm{string}(p)\ , \varphi\ , \mathrm{string}(p)) .$$

Uit het laatste voorbeeld zien we, dat het niet aangaat te zeggen dat we een met name genoemd element van A (hier p) door φ vervangen. Er staan in $\boxed{p\mid p\mid p}$ drie p's en we moeten duidelijk maken dat slechts de middelste ervan door φ moet worden vervangen. Dit verklaart onze voorkeur voor het gebruik van de parameter i in $\mathrm{lv}(\varphi,i,\beta)$.

Vaak wordt een operatie van locale vervanging niet beschreven door een i aan te geven, maar door een $p \in A$ te noemen die vervangen dient te worden. Daarmee wordt dus niet één locale vervanging, maar een <u>klasse</u> van locale vervangingen aangeduid. Laat dus $x \in A$ en $\beta \in A^*$ (x is een "letter" en β is een "woord"). Hierbij maken we nu de verzameling van alle $\mathrm{lv}(\varphi,i,\beta)$ met $0 \le i < \ell(\varphi)$, $\varphi(i) = x$. Het geval dat $\varphi = \varepsilon$ kan nu rustig worden toegelaten: dan is de verzameling der locale vervangingen leeg, omdat er geen i is met $\varphi(i) = x$.

We zullen de verzameling van de zo ontstane "woorden" met $LV(\varphi,x,\beta)$ aanduiden. Dus

$$LV(\varphi,x,\beta) = \{lv(\varphi,i,\beta) \mid 0 \le i < \ell(\varphi),\ \varphi(i) = x\}.$$

<u>Voorbeelden.</u>

1. Als $p,q,r \in A$ met $q \neq p$, $r \neq p$, $\varphi = \boxed{p \mid q \mid p \mid r}$, $\beta = \boxed{p \mid q}$, dan is

$$LV(\varphi,p,\beta) = \{\boxed{p \mid q \mid q \mid p \mid r}\,,\ \boxed{p \mid q \mid p \mid q \mid r}\}.$$

2. Als $\varphi \in A^*$, $p \in A$, dan is

$$LV(\boxed{p}\,, p\,, \varphi) = \{\varphi\}\,,$$

$$LV(\varphi\,, p\,, \boxed{p}) = \{\varphi\} \quad \text{als } p \in \text{inhoud}(\varphi)\,.$$

Merk op, dat er in het laatste geval verschillende i's kunnen zijn met $\varphi(i) = p$, maar dat die allemaal tot hetzelfde element van LV leiden.

3. Als de "letter" x niet in het "woord" φ voorkomt (dus $\varphi(i) \neq x$ voor $0 \le i < \ell(\varphi)$), dan is $LV(\varphi,x,\beta) = \emptyset$.

12.2. <u>Contextvrije generatie</u>

We gaan weer een stap verder. In plaats van één stel x,β waarmee we $LV(\varphi,x,\beta)$ bouwden, gaan we een klasse van paren (x,β) toelaten. Die paren (x,β) liggen in het cartesische product $A \times A^*$.

We nemen een verzameling van zulke paren (x,β), d.w.z. we nemen een deelverzameling W van $A \times A^*$. Bij vaste $\varphi \in A^*$ vormen we voor elk paar (x,β) uit W de $LV(\varphi,x,\beta)$ en van al deze nemen we de vereniging. Die vereniging heet $CG(\varphi,W)$ (CG is afkorting van "contextvrije generatie"; men noemt het "context-vrij" omdat de regels voor locale vervanging van een letter in een woord geformuleerd zijn op een manier die onafhankelijk is van wat er verder in dat woord staat). Dus

$$CG(\varphi,W) = \bigcup_{(x,\beta)\in W} LW(\varphi,x,\beta) .$$

<u>Voorbeelden.</u>

1. Laat $a \in A$, $b \in A$, laat $\varphi = \boxed{a \mid b}$ en laat W bestaan uit de paren (a,ε), $(a,\boxed{b})$ en $(b,\boxed{a \mid b})$. Dan is

$$CG(\varphi,W) = \{\boxed{b} , \boxed{b \mid b} , \boxed{a \mid a \mid b}\} .$$

Merk op, dat het er voor dit voorbeeld niet toe doet of al dan niet $a = b$.

2. Als W leeg is, dan is er niets te genereren, dus

$$CG(\varphi,\emptyset) = \emptyset .$$

3. Als W de verzameling is van alle paren $(x,\boxed{x \mid x})$ met $x \in A$, en als $\varphi \in A^*$, $\psi \in CG(\varphi,W)$, dan is inhoud(ψ) = inhoud(φ) en $\ell(\psi) = \ell(\varphi) + 1$.

12.3. <u>Afsluiting van contextvrije generatie</u>

Laat weer W een deel van $A \times A^*$ zijn.

We gaan Stelling 1 uit 10.3 toepassen. Voor de U uit die stelling nemen we A^*. Voor H nemen we de verzameling van alle singletons $\{\beta\}$ met $\beta \in A^*$. We leggen de afbeelding $\Phi : H \to P(A^*)$ vast door

$$\Phi(\{\beta\}) = CG(\beta,W)$$

voor alle $\beta \in A^*$.

De stelling zegt nu dat er bij elke deelverzameling R van A^* een afsluiting afsl(R,Φ) is.

Deze afsluiting heeft de eigenschap gesloten te zijn t.o.v. Φ. Hieruit volgt dat voor elke $\beta \in$ afsl(R,Φ) geldt dat CG(β,W) geheel tot afsl(R,Φ) behoort. Er is door contextvrije generatie uit afsl(R,Φ) dus niets nieuws te maken. De andere delen van de stelling zeggen dat R $\subset$ afsl(R,Φ) en dat afsl(R,Φ) de kleinst mogelijke gesloten verzameling is die R bevat.

De Φ is geheel door W bepaald en dat maakt het mogelijk om afsl(R,Φ) met ACG(R,W) aan te duiden (ACG te lezen als "afgesloten contextvrije generatie"). De zoëven genoemde eigenschappen kunnen we vertalen naar W. Als $R \subset A^*$, dan is

i) $\quad R \subset ACG(R,W) \subset A^*$

ii) $\quad \forall_{\varphi \in ACG(R,W)} \forall_{x \in A} \forall_{\beta \in A^*} ((x,\beta) \in W \rightarrow (LV(\varphi,x,\beta) \subset ACG(R,W)))$.

De minimaliteitseigenschap iii) zullen we maar niet meer vertalen.

De verzameling W belichaamt een stel regels om uit "woorden" nieuwe "woorden" te maken door locale vervanging (daarom noemt men W wel de verzameling der vervangingsregels of herschrijfregels) en ii) zegt dat de herschrijfregels uit W niets nieuws meer opleveren als ze op ACG(R,W) toegepast worden.

We kijken ook even naar Stelling 2 uit 10.3. Aan de daar gestelde eis dat elke V uit H een eindige verzameling is, is hier voldaan, want elke V uit H is een singleton. Stelling 2 zegt dat ACG(R,W) de vereniging is van $R_0, R_1, R_2, \ldots$, waarbij $R_0 = R$ en

$$R_{n+1} = \Psi(R_n) \qquad (n \in \mathbb{N}) .$$

$\Psi(R_n)$ ontstaat uit R_n door er alle locale vervangingen LV(φ,x,β) aan toe te voegen, waarbij $\varphi \in R_n$, $x \in A$, $\beta \in A^*$, $(x,\beta) \in W$.

Voorbeeld. Laat $a \in A$, $b \in A$ en laat W bestaan uit de paren $(a, \boxed{a \mid b})$ en $(a, \boxed{b \mid a})$. Ruwweg betekent dit, dat een a door één der "tweeletterwoorden" $\boxed{a \mid b}$ of $\boxed{b \mid a}$ vervangen mag worden. Laat $R = \{\boxed{a}\}$. Dan zal R_n bestaan uit alle "woorden" met eenzelfde gewogen inhoud: één a en $n-1$ b's. En $ACG(R,W)$ is de verzameling van alle "woorden" die één a bevatten en verder alleen maar b's.

12.4. Terminals en non-terminals

Bij gegeven W ($W \subset A \times A^*$) splitsen we A in twee stukken waarvan de elementen resp. terminals en non-terminals heten. Een element $x \in A$ heet een non-terminal als er tenminste één $\beta \in A^*$ is met $(x,\beta) \in W$; als er bij deze x geen enkele β met $(x,\beta) \in W$ is, dan heet x een terminal.

We stellen de verzameling der terminals door T voor en die der non-terminals door NT. Dus $T \cup NT = A$, $T \cap NT = \emptyset$.

Een "woord" φ uit A^* heet een "eindwoord" als alle "letters" van φ in T liggen; dus $\varphi(i) \in T$ voor $0 \leq i < \ell(\varphi)$. We kunnen φ dus ook als een element van T^* opvatten. In het bijzonder is ε een eindwoord.

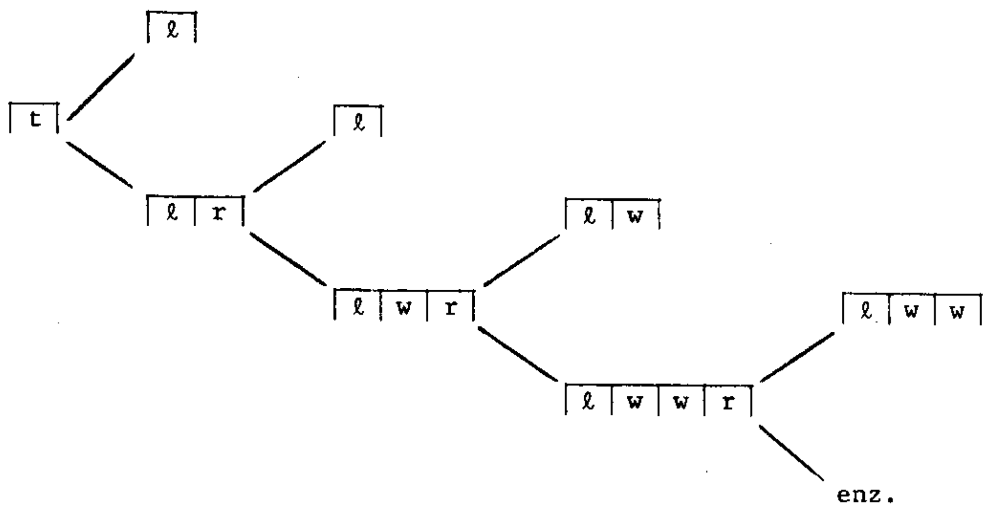
De gedachte die achter de term "eindwoord" ligt, is dat alle elementen van $A^*\backslash T^*$ locale vervanging toelaten, maar die van T^* niet. En het is de bedoeling van het stel vervangingsregels, dat we, door herhaaldelijke locale vervangingen, er een stel "eindwoorden" mee genereren.

12.5. Een voorbeeld

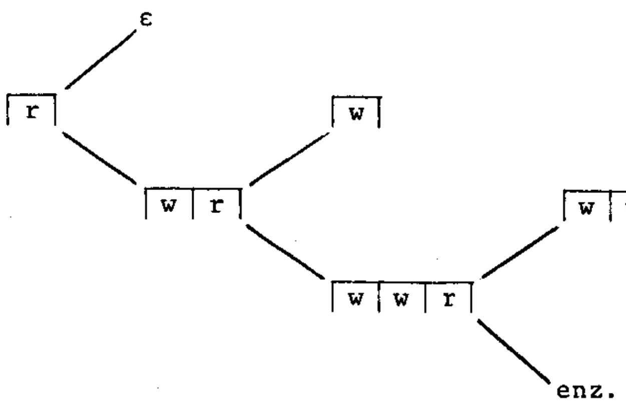
Laat het alfabet A de vier verschillende elementen t, r, ℓ, w hebben en laat W bestaan uit

$$(t, \boxed{\ell}) , \quad (t, \boxed{\ell \mid r}) , \quad (r, \varepsilon) , \quad (r, \boxed{w \mid r}) .$$

De verzameling der terminals is dus $T = \{\ell, w\}$ en die der non-terminals is $NT = \{t, r\}$. We gaan eens uit van het eenletterwoord $\boxed{t}$ en we gaan op alle mogelijke manieren series locale vervangingen uitvoeren. Het volgende schema komt tevoorschijn:



(Merk op dat $\boxed{\ell}$ twee keer wordt gegenereerd; daar is niets tegen.) Door uit te gaan van $\boxed{r}$ komt er:



Als we uitgaan van $\boxed{\ell}$ of $\boxed{w}$ dan komt er door locale vervanging in het geheel niets tevoorschijn. We stellen vast dat (met de notatie uit 12.3): als $R = \{\boxed{t}\}$, dan is

$$R_0 = \{\lceil t \rceil\},$$

$$R_1 = \{\lceil t \rceil, \lceil \ell \rceil, \lceil \ell \mid r \rceil\},$$

$$R_2 = \{\lceil t \rceil, \lceil \ell \rceil, \lceil \ell \mid r \rceil, \lceil \ell \mid w \mid r \rceil\},$$

$$R_3 = \{\lceil t \rceil, \lceil \ell \rceil, \lceil \ell \mid r \rceil, \lceil \ell \mid w \mid r \rceil, \lceil \ell \mid w \rceil, \lceil \ell \mid w \mid w \mid r \rceil\},$$

enz.

Als $R = \{\lceil r \rceil\}$, dan is

$$R_0 = \{\lceil r \rceil\},$$

$$R_1 = \{\lceil r \rceil, \varepsilon, \lceil w \mid r \rceil\},$$

$$R_2 = \{\lceil r \rceil, \varepsilon, \lceil w \mid r \rceil, \lceil w \rceil, \lceil w \mid w \mid r \rceil\},$$

$$\ldots$$

Als $R = \{\lceil \ell \rceil\}$, dan is $R_0 = R_1 = R_2 = \ldots$ en bij $R = \{\lceil w \rceil\}$ is eveneens $R_0 = R_1 = R_2 = \ldots$.

De ACG's zijn de verenigingen van de R_i's:

$$ACG(\{\lceil t \rceil\},W) = \{\lceil t \rceil, \lceil \ell \rceil, \lceil \ell \mid r \rceil, \lceil \ell \mid w \mid r \rceil, \ldots\},$$

enz. We stellen in het bijzonder belang in de "eindwoorden" uit deze verzameling. De verzameling der "eindwoorden" in $ACG(\{\lceil t \rceil\},W)$ is

$$\{\lceil \ell \rceil, \lceil \ell \mid w \rceil, \lceil \ell \mid w \mid w \rceil, \lceil \ell \mid w \mid w \mid w \rceil, \ldots\},$$

die in $ACG(\{\lceil r \rceil\},W)$ is

$$\{\varepsilon, \lceil w \rceil, \lceil w \mid w \rceil, \lceil w \mid w \mid w \rceil, \ldots\},$$

die in $ACG(\{\lceil \ell \rceil\},W)$ is $\{\lceil \ell \rceil\}$ zèlf, en die in $ACG(\{\lceil w \rceil\},W)$ is $\{\lceil w \rceil\}$ zelf.

We zullen deze verzamelingen van "eindwoorden" door V_t, V_r, V_ℓ, V_w voorstellen:

$$V_t = \{\boxed{\ell}\,,\ \boxed{\ell \mid w}\,,\ \boxed{\ell \mid w \mid w}\,,\ldots\}$$

enz.

12.6. De verzameling der "eindwoorden" gegenereerd door een "letter"

We kunnen de notatie uit 12.5 algemeen invoeren. A is een verzameling, W een deel van $A \times A^*$, en A is daardoor gesplitst in T (terminals) en NT (non-terminals). Als $x \in A$ definiëren we

$$V_x := \mathrm{ACG}(\{\boxed{x}\},W) \cap T^*$$

en dat is de verzameling van alle "eindwoorden" die we kunnen krijgen door van het eenletterwoord $\boxed{x}$ uit te gaan en herhaaldelijk locaal te vervangen met behulp van de herschrijfregels W. Het is al duidelijk gemaakt, dat $V_x = \{\boxed{x}\}$ voor alle $x \in T$.

We kijken weer eens naar het voorbeeld van 12.5. De vervangingsmogelijkheden voor t zijn

$$\boxed{\ell} \quad \text{en} \quad \boxed{\ell \mid r}\,.$$

Wat is nu $\mathrm{ACG}(\{\boxed{t}\},W)$? We krijgen dat door aan $\{\boxed{t}\}$ alles toe te voegen wat door locale vervanging ontstaat. Maar elke rij van locale vervangingen, die bij t begint, komt langs $\boxed{\ell}$ of langs $\boxed{\ell \mid r}$, nl. al bij de eerste stap. En alles wat door een rij locale vervangingen uit $\boxed{\ell}$ of $\boxed{\ell \mid r}$ ontstaat,

ontstaat ook door een rij locale vervangingen uit $\lceil t \rceil$. Dus

$$ACG(\{\lceil t \rceil\},W) = \{\lceil t \rceil\} \cup ACG(\{\lceil \ell \rceil\},W) \cup ACG(\{\lceil \ell \mid r \rceil\},W)$$

en analoog

$$ACG(\{\lceil r \rceil\},W) = \{\lceil r \rceil\} \cup \{\varepsilon\} \cup ACG(\{\lceil w \mid r \rceil\},W) .$$

Als U_1, U_2, U_3 deelverzamelingen van A^* zijn, dan is

$$ACG(\boxed{U_1 \mid U_2 \mid U_3},W) = \boxed{ACG(U_1,W) \mid ACG(U_2,W) \mid ACG(U_3,W)} .$$

(Bedenk, dat $\boxed{U_1 \mid U_2 \mid U_3}$ betekent $CONCAT(U_1,U_2,U_3)$.) Verder bedenken we dat

$$\boxed{U_1 \mid U_2 \mid U_3} \cap T^* = \boxed{U_1 \cap T^* \mid U_2 \cap T^* \mid U_3 \cap T^*}$$

(want de concatenatie van "woorden" α, β, γ is een "eindwoord" wanneer en alleen wanneer α, β, γ zelf "eindwoorden" zijn) en dat $\{\lceil \ell \mid r \rceil\} = \boxed{\{\lceil \ell \rceil\} \mid \{\lceil r \rceil\}}$.

Door alleen naar de "eindwoorden" te kijken, komen we nu tot

$$V_t = V_\ell \cup \boxed{V_\ell \mid V_r} , \qquad (1)$$

en analoog

$$V_r = \{\varepsilon\} \cup \boxed{V_w \mid V_r} . \qquad (2)$$

We wisten al, dat

$$V_\ell = \{\lceil \ell \rceil\} \quad , \quad V_w = \{\lceil w \rceil\} .$$

We kunnen de betrekkingen (1) en (2) opvatten als "vergelijkingen", waaruit de "onbekende" verzamelingen V_t en V_r kunnen worden opgelost. Men kan ook nog laten zien dat onze V_t en V_r in zekere zin de minimale oplossingen van dit stel vergelijkingen vormen, maar we gaan daar nu niet op in.

We zijn begonnen met de herschrijfregels W en hebben daaruit de vergelijkingen (1) en (2) afgeleid. Men kan ook omgekeerd te werk gaan: uitgaan van de vergelijkingen en dan tot de herschrijfregels komen. Ook dit laten we hier onbesproken.

We laten de betrekking tussen W en het stel verzamelingsvergelijkingen nog even zien aan een iets groter voorbeeld, dat ook in 12.7 dienst zal doen. Laat $A = \{a,b,p,q,r\}$, waarbij a, b, p, q, r twee aan twee verschillen. Laat W bestaan uit

$$(p, \lceil a \mid q \rceil) \quad , \quad (p, \varepsilon) \; ,$$

$$(q, \lceil b \mid p \mid a \rceil) \quad , \quad (q, \lceil r \mid p \rceil) \; ,$$

$$(r, \lceil r \mid b \rceil) \; .$$

De non-terminals zijn p, q, r en de verzamelingsvergelijkingen worden

$$V_p = \boxed{\{\lceil a \rceil\} \mid V_q} \cup \boxed{\{\varepsilon\}}$$

$$V_q = \boxed{\{\lceil b \rceil\} \mid V_p \mid \{\lceil a \rceil\}} \cup \boxed{V_r \mid V_p}$$

$$V_r = \boxed{V_r \mid \{\lceil b \rceil\}} \; .$$

Die $\boxed{\{\lceil b \rceil\} \mid V_p \mid \{\lceil a \rceil\}}$ ziet er wat afschrikwekkend uit, maar kan eenvoudig beschreven worden als de collectie van alle "woorden" van de vorm $\mathrm{concat}(\lceil b \rceil, \varphi, \lceil a \rceil)$ met $\varphi \in V_p$. En natuurlijk is $\boxed{\{\varepsilon\}}$ hetzelfde als $\{\varepsilon\}$.

12.7. Backus-Naur Form (BNF)

De met BNF aangeduide notatie is een manier om de verzameling W der herschrijfregels te noteren. We laten dat zien aan het voorbeeld van het slot van 12.6. We schrijven W op in een lijst, waarbij aan elke non-terminal een regel is gewijd en we gebruiken daarbij het symbool ::= als volgt:

$$p \ ::= \ \{\boxed{a \mid q}\ , \varepsilon\}$$

$$q \ ::= \ \{\boxed{b \mid p \mid a}\ , \boxed{r \mid p}\}$$

$$r \ ::= \ \{\boxed{r \mid b}\}\ .$$

Dit is nog niet precies BNF. We schrijven eerst nog de verzamelingen rechts zonder accoladen en met vertikale strepen als scheidingstekens (i.p.v. komma's):

$$p \ ::= \ \boxed{a \mid q} \ \Big| \ \varepsilon$$

$$q \ ::= \ \boxed{b \mid p \mid a} \ \Big| \ \boxed{r \mid p}$$

$$r \ ::= \ \boxed{r \mid b}\ .$$

Vervolgens heeft men de gewoonte om "string" gewoon door achterelkaarplaatsing te noteren: a b c i.p.v. $\boxed{a \mid b \mid c}$. (Dit wordt overigens ook wel voor concat gedaan: concat(φ,ψ) wordt als $\varphi\,\psi$ geschreven. Soms komt het gemengd voor: a $\varphi\,\psi$ i.p.v. concat(string(a) , φ , ψ), zodat bijv. uit de keuze van lettertype moet blijken welke opvatting men dient te huldigen.) Men schrijft dus

$$p \ ::= \ a\,q \ \Big| \ \varepsilon$$

$$q \ ::= \ b\,p\,a \ \Big| \ r\,p$$

$$r \ ::= \ r\,b\ .$$

Men gaat nog verder, want de consequentie is, dat men het "lege woord" ε noteert door eenvoudig niets op te schrijven. In het algemeen is de moeilijkheid daarbij, dat het zo lastig is vast te stellen wáár er niets opgeschrevan is, maar hier redt men zich met de overweging dat wanneer er tussen twee vertikale strepen of vóór de eerste, of ná de laatste niets staat, er een ε bedoeld moet zijn. Dus voor de eerste regel komt er

$$p \ ::= \ aq \mid \quad .$$

Nog steeds is dit niet de echte BNF. Het wordt pas echt wanneer men als namen voor de non-terminals geen losse letters gebruikt of samengestelde formules (als f een afbeelding van T in NT is, zal bijv. ook f(a) een non-terminal voorstellen), maar alleen speciale symbolen in de vorm $<\ldots>$, waarbij meestal op de plaats van de stippeltjes een zelfstandig naamwoord wordt geschreven. Men gebruikt dus namen als <natuurlijk getal>, <cijferreeks>. Laten we om misverstanden te vermijden afzien van het kiezen van speciale woorden in ons voorbeeld, en p, q, r vervangen door $<\pi_1>$, $<\pi_2>$, $<\pi_3>$. Er komt nu

$$\begin{aligned} <\pi_1> \ &::= \ a<\pi_2> \mid \\ <\pi_2> \ &::= \ b<\pi_1>a \mid <\pi_3><\pi_1> \\ <\pi_3> \ &::= \ <\pi_3>b \ . \end{aligned}$$

Meestal wordt deze notatie gebruikt met een bepaalde interpretatie van de terminals. We hebben bijv. de fysisch reproduceerbare symbolen Δ, $\square$ en we interpreteren a als Δ, b als $\square$. Nu komt er

$$\begin{aligned} <\pi_1> \ &::= \ \Delta<\pi_2> \mid \\ <\pi_2> \ &::= \ \square<\pi_1>\Delta \mid <\pi_3><\pi_1> \\ <\pi_3> \ &::= \ <\pi_3>\square \end{aligned}$$

en dit is nu wat men gewoonlijk BNF noemt. In zo'n BNF-lijst is de volgorde van de regels irrelevant en ook de volgorde van de stukken tussen de verticale strepen rechts. Het gaat er immers alleen om dat we W beschrijven! En dat gaat even goed met bijv.

$$\begin{aligned}
\langle\pi_3\rangle &::= \langle\pi_3\rangle\square \\
\langle\pi_1\rangle &::= \;\mid \Delta\langle\pi_2\rangle \\
\langle\pi_2\rangle &::= \langle\pi_3\rangle\langle\pi_1\rangle \mid \square\langle\pi_1\rangle\Delta \;.
\end{aligned}$$

Wat we deden met fysisch reproduceerbare symbolen, wordt ook vaak gedaan met symbolen die de ons vertrouwde vorm van letters of cijfers hebben. Dit heeft als bezwaar, dat we al letters gebruiken in onze wiskundige taal, en dat de cijfers daar zelfs een geheel vaste betekenis hebben. Als we veilig willen praten, doen we misschien verstandiger om voor die fysisch reproduceerbare letters en cijfers geheel nieuwe symbolen te kiezen, zoals $k_a, k_b, \ldots, k_z, k_0, \ldots, k_9$ (die men bijv. zou kunnen zien als namen van de toetsen op een schrijfmachine).

Op zichzelf zou het geen bezwaar hebben om wiskundige objecten te nemen i.p.v. toetsen, maar, als men de gewoonte wil handhaven om concatenatie door aaneenschrijven te noteren, is dit erg verwarrend. Denk bijv. aan de vrijheid die we hebben om wiskundige objecten voor te stellen. Als we het over het 12-tallige stelsel hebben, werken we met

$$\langle\text{cijfer}\rangle ::= 0 \mid 1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9 \mid 10 \mid 11$$

en dan moet 11 niet als concatenatie van twee enen worden gezien, maar als naam voor een natuurlijk getal, nl. het getal dat een andere keer misschien als 8 + 3 geschreven wordt. Bij de opvatting dat 0,...,11 wiskundige objecten voorstellen en geen krabbels op papier, past ook de opmerking dat bovengenoemde regel hetzelfde betekent als

<cijfer> ::= $0 \mid 1 \mid 2 \mid 1+2 \mid 2^3/2 \mid 5 \mid 6 \mid 4+3 \mid 9-1 \mid 3^2 \mid 2\times 5 \mid 11$.

De voornaamste bron van misverstanden zit in het aaneenschrijven: 1 1 0 zou zowel $\boxed{11}\boxed{0}$ als $\boxed{1}\boxed{1}\boxed{0}$ als $\boxed{1}\boxed{10}$ kunnen betekenen.

Eindconclusie: BNF is geschikt in gevallen, waarin de symbolen "fysisch" zijn geïnterpreteerd. In andere gevallen is het misschien een handig kortschrift, maar dan moet men goed weten wâár het de afkorting van is. Het is een manier om W te beschrijven, en daardoor tegelijk de "verzamelingsvergelijkingen". Uit dat laatste komt de gewoonte voort om de non-terminals te noteren in de vorm <...> waar op de stippeltjes een substantief staat. Kijk maar eens naar de grammatica van 12.5, die in BNF kan zijn:

<trein> ::= ℓ | ℓ<rij wagens>
<rij wagens> ::= | w<rij wagens>

en men leest zoiets als: "een trein is ℓ (locomotief) of ℓ gevolgd door een rij wagens" en "een rij wagens is leeg of het is w gevolgd door een rij wagens".

Terzijde maken we de opmerking dat we in de eerste regel ook hadden kunnen schrijven <trein> ::= ℓ<rij wagens>. Dat had dezelfde collectie "eindwoorden" opgeleverd.

HOOFDSTUK 13. FORMELE BESCHRIJVING VAN BOMEN

13.1. Inleiding

Er zijn verschillende soorten van structuren waarbij men de term "boom" gebruikt. Wij beschrijven er twee, die we hier "ongeordende boom" en "geordende boom" noemen. De laatstgenoemde kennen we al, doordat we daar in Hoofdstuk 1 formules mee voorstelden.

13.2. Ongeordende bomen

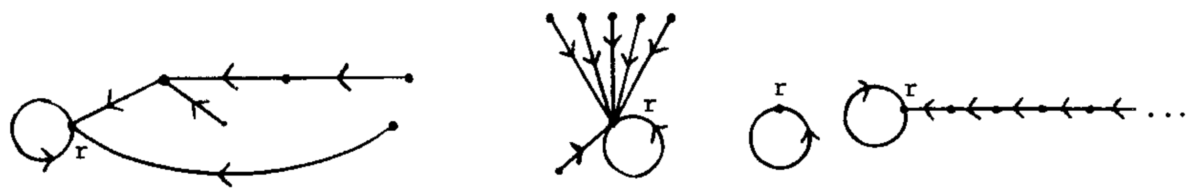
Een ongeordende boom is een tripel (S,r,f), waarin S een verzameling is, r een element van S (r wordt de wortel van de boom genoemd) en f een afbeelding van S in S, met de volgende eigenschappen:

(i) $f(r) = r$.

(ii) Als voor $n \in \mathbb{N}$, $n \geq 1$, de n-de geïtereerde van f door f^n wordt voorgesteld (dus bijv. $f^3(x) = f(f(f(x)))$), dan geldt

$$\forall_{x \in S} \exists_{n \in \mathbb{N} \setminus \{0\}} (f^n(x) = r) .$$

Voorbeelden.



Het laatste voorbeeld kan in formule worden gegeven als het tripel $(\mathbb{N},0,f)$ met $f(0) = 0$ en $f(n+1) = n$ voor alle $n \in \mathbb{N}$.

Daar $r \in S$, komt het geval $S = \emptyset$ niet voor.

Elementen y van S waarbij geen x bestaat met $x \neq r$, $f(x) = y$, heten <u>eindpunten</u> van de boom.

Als $y = f(x)$ en $x \neq r$, zegt men wel dat y de <u>vader</u> van x is. Als $x \in S$ zegt men dat de verzameling $f^{vo}(\{x\})\backslash\{r\}$ de <u>kinderschaar</u> is van x. Eindpunten zijn dus punten met lege kinderschaar, en omgekeerd. En de verzameling van alle eindpunten is $S\backslash f^{bd}(S)$, als $S \neq \{r\}$.

<u>Voorbeeld</u>. In de boom $(S,r,\lambda_{x\in S}\, r)$ is elk punt $\neq r$ een eindpunt. De kinderschaar van r is $S\backslash\{r\}$.

13.3. <u>Geordende bomen</u>

Voordat we zeggen wat een <u>geordende boom</u> is, noemen we even het begrip <u>totale ordening</u> (ook wel lineaire ordening genoemd). Een binaire relatie $<$ (infix genoteerd) op een verzameling K heet een totale ordening als

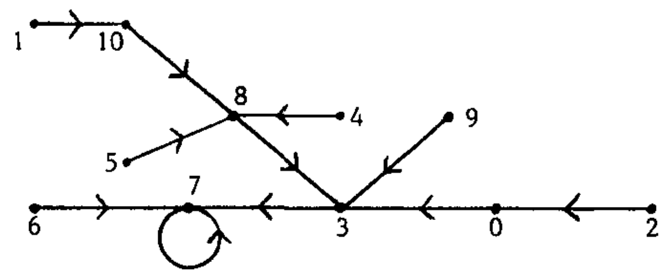
(i) Voor elk paar x,y uit K geldt precies één van de proposities $x < y$, $x = y$, $y < x$ ("trichotomie").

(ii) Als $x \in K$, $y \in K$, $z \in K$, $x < y$, $y < z$, dan ook $x < z$ ("transitiviteit").

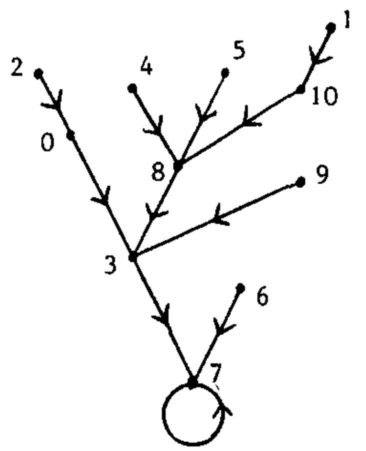
Nu zeggen we: een <u>geordende boom</u> is een ongeordende boom (S,f,r) waarbij voor elke $x \in S$ een totale ordening $<$ in de kinderschaar van x gegeven is.

We kunnen een geordende boom (althans als S eindig is) op papier steeds zo tekenen dat de wortel r onderaan ligt, dat bij elke x de kinderschaar boven x ligt, en dat in die kinderschaar elk punt u steeds links ligt van alle punten v met $u < v$.

Als voorbeeld gaan we uit van een totale ordening op S. Deze induceert in elke kinderschaar weer een totale ordening (eenvoudig door te zeggen dat als $K \subset S$, en $u \in K$, $v \in K$, $u < v$ bij de ordening in S, dan ook $u < v$ bij de ordening in K). De ordening is aangeduid door rangnummers 0,...,10. De boom



kan nu worden getekend als

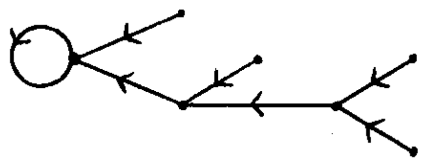


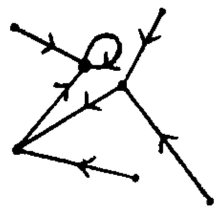
Men kan in deze boom <u>niveau's</u> aangeven: 7 (de wortel) ligt op niveau 0; 3 en 6 op niveau 1; 0, 8, 9 op niveau 2; 2, 4, 5, 10 op niveau 3 en tenslotte 1 op niveau 4. Het niveau kan beschreven worden als het aantal iteratiestappen dat met f gedaan moet worden om bij de wortel te komen. Bij een ongeordende boom kan dit natuurlijk net zo goed.

Men kan de punten van een eindige ongeordende boom steeds zó van nummers voorzien (bij verschillende punten verschillende nummers), dat de vader-pijlen steeds van hoog naar laag nummer lopen (en de wortel dus het laagste nummer heeft). Bij geordende bomen kan men bovendien bereiken, dat binnen iedere kinderschaar de rangorde van de nummers overeenstemt met de ordening binnen die kinderschaar.

Twee ongeordende bomen (S_1, r_1, f_1) en (S_2, r_2, f_2) heten <u>isomorf</u> als er een bijectie $g : S_1 \to S_2$ is met $g(r_1) = r_2$ en $g \circ f_1 = f_2$ (d.w.z. $g(f_1(x)) = f_2(x)$ voor alle $x \in S_1$).

<u>Voorbeeld</u>.





We gaan <u>niet</u> zover dat we zeggen dat hier twee keer dezelfde boom staat. Wie zoiets wèl zegt, bedoelt met "boom" niet hetzelfde als wij, maar "equivalentieklasse van ongeordende bomen".

Wanneer men zegt dat twee geordende bomen isomorf zijn, bedoelt men dat die bijectie g ook de ordeningen in de kinderscharen intact laat. Het komt erop neer dat voor alle x, y, z met $x \in S_1$, y en z in de kinderschaar van x, met $y < z$ ook geldt $g(y) < g(z)$ in de kinderschaar van $g(x)$.