CWI Syllabi

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

The CWI is a research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a nonprofit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands Organization for the Advancement of Research (N.W.O).

CWI Syllabus 24

Bewijzen in de wiskunde

Onder redactie van
P.W.H. Lemmens

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

1980 Mathematics Subject Classification: 01A99, 03A05, 03D05, 68F05.
ISBN 90 6196 373 7
NUGI-code: 811

INHOUD

VOORWOORD.

Ongeveer twee jaar geleden liet Prof. dr. A.F. Monna mij een door hem geconcipieerd manuscript lezen over historische beelden van het fenomeen "bewijzen" in de wiskunde. Het ging daarin vooral over het begrip "streng bewijs", geïllustreerd aan de hand van historische foute of onvolledige bewijzen. Het leek ons zinvol om dit toegankelijk te maken voor een breder publiek.

Erg verheugend was het, Prof. dr. N.G. de Bruijn en Prof. dr. D. van Dalen bereid te vinden om ook een bijdrage te leveren.

Speciaal voor deze uitgave heeft D. van Dalen hoofdstuk II (Bewijzen, waarom en hoe) geschreven. Op zijn verzoek breng ik hier zijn dank over aan H. Freudenthal, R.P. Nederpelt en P.G.J. Vredenduin voor hun commentaar.

Over het unieke AUTOMATH-projekt van N.G. de Bruijn zijn van zijn hand al veel publicaties verschenen in wetenschappelijke tijdschriften. Op enkele uitzonderingen na zijn deze in de Engelse taal gesteld en bovendien iets te technisch. Ik ben hem veel dank verschuldigd voor het geduld en de toewijding waarmee hij mij heeft begeleid bij het vertalen van gedeelten uit zijn werk.

Buiten het schrijven van zijn bijdrage heeft D. van Dalen zich ook verdienstelijk gemaakt met het kritisch bekijken van het oorspronkelijke manuscript van A.F. Monna. Van Dalens suggesties voor aanvullingen en nadere detailleringen hebben wezenlijk bijgedragen aan de hier gepresenteerde tekst van hoofdstuk I.

P.W.H. Lemmens, maart 1989.

HOOFDSTUK I

BEWIJZEN IN DE WISKUNDE

historische beelden

A.F. Monna

bewerkt en aangevuld door P.W.H. Lemmens

1. BEWIJZEN ALS IDEE.

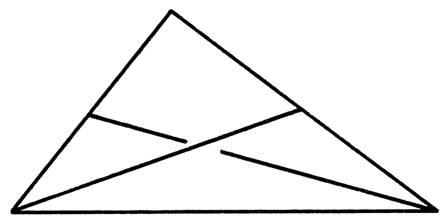
Bewijzen is één van de zeer fundamentele aktiviteiten in de wiskunde. Mathematische stellingen, beweringen, worden bewezen. Er worden bewijzen gegeven van uitspraken die in het kader van een theorie niet vanzelfsprekend zijn. Het is een wezenstrek van een mathematische theorie. De filosofische aspecten van dit "wezen" blijven hier buiten beschouwing. We zullen ons bezighouden met het begrip bewijs, met de bewijsmiddelen en met het bewijzen. Ons doel is het belichten van historische aspecten van het fenomeen "bewijzen". Dat zal gebeuren door het schetsen van de ontwikkelingen aan de hand van een aantal voorbeelden. De nadruk zal daarbij vallen op het normatieve karakter van bewijzen, en op het verloop van inzichten daarover. Aan de orde komt het veel gebruikte begrip "strengheid". Ook zal aandacht worden besteed aan de invloed die foute bewijzen gehad hebben op de ontwikkeling van de wiskunde. Uit onze behandeling zal blijken dat de begrippen "streng bewijs" en "fout bewijs" met enige voorzichtigheid moeten worden gehanteerd: ook die blijken aan ontwikkeling onderhevig te zijn.
Wellicht zijn deze beschouwingen interessant in een tijdvak waarin men vaak de klacht hoort, dat studenten niet meer weten wat stellingen met bewijs zijn als gevolg van de vergaande eliminatie van de klassieke euclidische meetkunde (zie [22]).

We laten enkele opmerkingen voorafgaan over het begrip "bewijzen" als zodanig. Beschouwen we "bewijzen" naast "het bewijs", dan lijkt het *idee* van "bewijzen" primair te zijn. Wat is eigenlijk "bewijzen"? We zullen hier niet ingaan op de vraag hoe dit begrip is ontstaan in het menselijk denken.
Het idee van bewijzen is verbonden met een waarheidsbegrip: het gaat over bewijzen als mentale aktiviteit om een bewering "waar" te maken. Het heeft ook te maken met het niet aanvaarden op gezag of op grond van aanschouwing, met daarnaast het niet uit een bijzonder geval mogen concluderen tot het algemene. In dit brede kader is het idee van bewijzen niet beperkt tot de wiskunde. In zekere mate blijkt het een universeel begrip te zijn. Zo kan men wijzen op het leveren van bewijzen in de rechtswetenschappen. Men spreekt daar van

bewijskracht en bewijslast. In de wiskunde is bewijzen niet identiek met "aannemelijk maken", zeker niet als men denkt aan een "streng" bewijs waarin wordt geredeneerd met inachtnemen van vaste regels volgens principes uit de logica. Na het idee van bewijzen volgt de vraag: wat is een bewijs en wat zijn de *middelen* die men wil gebruiken of die men bereid is te aanvaarden? Welke middelen zijn in de loop der tijden gebruikt en hoe waren de gedachten daarover? Dit voert tot het idee van strengheid in de wiskunde. Men aanvaardt vaste regels die in het bewijsproces worden toegepast op basis van definities en axioma's.

Op elk van de voornoemde punten zijn opmerkingen te maken in het licht van de historische ontwikkeling. Daarmee komen we op concreter wiskundig terrein. We zullen geen aandacht besteden aan het aspect van het niet op gezag aanvaarden, alhoewel dat eeuwenlang is gebeurd. Om een indruk te krijgen over de aanschouwing en over het generaliseren van het bijzondere geval, kan de volgende algemene stelling uit de elementaire meetkunde als voorbeeld dienen:

> De drie zwaartelijnen in een driehoek — d.w.z. in elke driehoek — snijden elkaar in één punt.



In het traditionele bewijs tekent men een figuur, en baseert de redenering daarop. Is zo'n bewijs vrij van alle aanschouwing? Is een tekening toch niet een bijzonder geval? Wordt wel eens bewezen dat twee zwaartelijnen elkaar snijden, of is dat vanzelf duidelijk? Natuurlijk zal iedere mathematicus toegeven dat deze schakel in het bewijs ontbreekt, maar waarom wordt deze leemte dan niet ingevuld? De traditionele leerboeken pretenderen een streng bewijs te geven. Er is wel eens gesuggereerd (o.a. door Jakob Steiner (1796-1863) en naar verluid (zie [43], p. 207) door de wiskundeleraar L.N.A.W. Gravelaar (1851-1913)) om de meetkunde te beoefenen zonder het tekenen van figuren, om alle gevaar van aanschouwing te weren. Bij de manier waarop de meetkunde wordt beoefend, en met name bij de keuze om wel of geen figuren te tekenen, spelen zeker ook didaktische overwegingen een rol (zie [47]). Bij het elementaire onderwijs doet zich de vraag voor of de intuïtie zoveel mogelijk uitgebannen moet worden, of dat deze op didaktische gronden juist in zekere mate moet worden geaccepteerd of zelfs aangemoedigd. Hoe dit ook zij, het streven naar strengheid schijnt in het stadium van het elementaire onderwijs een verlaten standpunt. Voor een behandeling van deze problematiek verwijzen we naar de boeken van Joh.H. Wansink [47].

In onze tijd kan ook de computer in de beschouwingen worden betrokken. We noemen bijvoorbeeld het bepalen of een getal een priemgetal is, en zo nee het berekenen van delers van dat getal. Dit is een uiterst actueel onderwerp in verband met kraak-bestendige codes. Andere voorbeelden zijn het oplossen van grote stelsels vergelijkingen, het numeriek oplossen van stelsels differentiaalvergelijkingen, het berekenen van integralen. Een zeer bekend probleem is het vier-kleurenprobleem: kan elke landkaart in het platte vlak met hoogstens vier kleuren worden gekleurd, zo dat aangrenzende landen verschillend van kleur zijn? Dit probleem (zie ook [1]), voor het eerst genoemd omstreeks 1850 door De Morgan, heeft de mathematische wereld meer dan een eeuw beziggehouden. In 1976 kondigden K. Appel en W. Haken [2] aan dat ze het in bevestigende zin hadden opgelost met intensief gebruik van computers.

Als men een probleem oplost, of denkt te kunnen oplossen, met behulp van een computer, zal die oplossingsmethode dan worden aanvaard? In het geval van het vier-kleurenprobleem twijfelt niemand meer aan de juistheid van de stelling, maar velen vinden dat het bewijs nog niet geleverd is. Alle fouten die men heeft ontdekt in de computerprogramma's zijn hersteld. Het is echter een enorme taak om streng-logisch te bewijzen dat die programma's ook inderdaad goed zijn (dat ze theoretisch doen wat de bedoeling is). En als die taak volbracht is, is er dan enige garantie dat er geen fouten zitten in de implementatie van bijvoorbeeld de gebruikte computertaal, of in de hardware? Er blijft een gevoel van het niet helemaal tot in de uiterste details kunnen controleren, zoals dat in principe wel kan bij klassieke bewijzen.
Enigszins te vergelijken met het gebruik van de computer is het oplossen van problemen van meetkundige vraagstukken met behulp van passer en lineaal. In beide gevallen hanteert de persoon de instrumenten, en gaat hij af op datgene wat die instrumenten produceren. In het ene geval zijn het de gegevens die geleverd worden door de computer, in het andere geval de verkregen figuur (de aanschouwing). Is in beide gevallen de persoon niet teveel betrokken bij het proces door de gegeven instructies ten aanzien van de te verrichten handelingen? En kan men met passer en lineaal, respectievelijk met de computer, uitstijgen boven het speciale geval en tot algemene waarheden komen?

De regel dat uit het bijzondere geval niet het algemene mag worden geconcludeerd, werd reeds gehanteerd door de Grieken. Dit is een grote mathematische stap. Maar nog in de 19e eeuw presenteerde deze problematiek zich in een concreet meetkundig gebied, met name in de meetkunde van het aantal. Hierbij gaat het om het berekenen van aantallen meetkundige figuren die aan zekere condities voldoen. Aan dit vak is naam van de wiskundige Hermann Schubert (1848-1911) verbonden, vooral door zijn beroemde boek "Kalkül der abzählenden Geometrie" (1879). Op grond van continuïteits-principes achtte hij het geoorloofd uit het bijzondere tot het algemene te mogen besluiten. We komen later nog terug op dit probleemgebied.

Zoals reeds opgemerkt, is het geven van een bewijs gebonden aan het hanteren van vaste regels die verband houden met de logica. Reeds bij de Griekse wiskunde kende men een axiomatisch systeem, en hanteerde men van daaruit principes van natuurlijke deductie. Ook aan een begrip als "vaste regels" valt te tornen. Met name kan worden gewezen op de ontwikkeling van de intuïtionistische wiskunde, in gang gezet door de nederlandse wiskundige L.E.J. Brouwer (1881-1966). Op principiële gronden werden bepaalde traditionele bewijsmethoden door hem afgewezen: hij aanvaardde slechts constructieve bewijsmethoden. Een bewijs uit het ongerijmde strandde in de ogen van Brouwer op de niet uitgesloten derde mogelijkheid naast "waar" of "onwaar", namelijk de mogelijkheid dat we (nog) niet kunnen vaststellen of een uitspraak waar danwel onwaar is. Ook zaken als het lemma van Zorn of het keuzeaxioma (we komen hierop later uitvoeriger terug) werden door hem niet erkend als bewijsmethode. De al dan niet expliciet geformuleerde formele regels waaraan bewijzen in de wiskundige praktijk zijn gebonden, kunnen zich dus wijzigen. Dat is ook soms gebeurd in de loop van de geschiedenis. Daarin ligt eigenlijk de kern van het verschijnsel dat wij bepaalde, vroeger aanvaarde bewijsmethoden nu in meer of mindere mate afkeuren. Met "bewijzen" is een objectieve handeling bedoeld, zij het dat niet alle wiskundigen daarbij dezelfde waarheidsmaat hanteren of hanteerden.

Het aantal aspecten in het begrip "bewijzen" met betrekking tot de toegelaten middelen is hiermee nog niet uitgeput. Later komen wij er nog op terug, vooral in verband met het eerder genoemde keuzeaxioma.

Tenslotte is er nog een *vormkwestie* bij het formuleren en bewijzen van mathematische uitspraken. In de historische opbouw van de ontwikkeling van nieuwe theorieën is het opmerkelijk dat de aanvankelijke resultaten niet werden geformuleerd in de vorm van geponeerde stellingen met bewijzen ervan. Dit valt in het bijzonder op bij de (zeer lange) eerste periode van de ontwikkeling van de infinitesimaalrekening in de 17e en 18e eeuw, en ook nog wel in het begin van de 19e eeuw (vóór het werk van Augustin Cauchy (1789-1857)). In deze ontwikkeling vinden we afleidingen van formules en relaties, berekeningen van integralen, expliciete oplossingen van differentiaalvergelijkingen. Op elementair niveau betreft het formules voor $\sin(a+b)$, $\cos(a+b)$ enz., op hoger niveau de diverse formules in de elementen van de theorie van gammafunkties en elliptische funkties. Het is voornamelijk het manipuleren van vergelijkingen. Cauchy doorbrak deze gang van de ontwikkeling, door meer aandacht te besteden aan de grondslagen van de analyse. Hij was ook de eerste die een existentiebewijs gaf voor een oplossing van een differentiaalvergelijking (zie [43], pag. 188-191). In vele mathematische gebieden is het aspect van afleidingen en berekeningen van formules aanwezig. In de klassieke analytische meetkunde denke men bijvoorbeeld aan de formules voor raaklijn en poollijn in de theorie van de kegelsneden. Meestal is het manipuleren van vergelijkingen en formules (wat we hier "afleidingen" noemen) een methodiek waarmee een nieuw geopend gebied systematisch wordt geëxploreerd, op zoek naar resultaten waarvan nog niet vaststaat hoe die er zullen uitzien. Pas in een latere fase kunnen dan algemene stellingen worden geformuleerd en bewezen. Zowel bij "afleidingen" als "bewijzen" gaat het om het formuleren van "ware beweringen", maar toch verstaan we onder een "bewijs" iets meer dan alleen het manipuleren met vergelijkingen en formules. Er kan naar aanleiding van dit onderscheid ook een vraag van didactische aard worden gesteld. Valt bij het gebruik van afleidingen het begrip van het geven van bewijzen volgens vaste regels niet in zekere mate weg? In de elementaire algebra en infinitesimaalrekening overheersen de afleidingen (denk bijvoorbeeld aan de afleiding van formules voor de wortels van tweede en derde graads vergelijkingen). In de elementaire meetkunde daarentegen fungeren van oudsher stellingen met bewijzen. Het terugdringen van de elementaire meetkunde in het elementaire onderwijs kan tot gevolg hebben dat het idee van "streng bewijzen" vervaagt, met de daarmee gepaard gaande nadelen bij de studie van de contemporaine wiskunde.

2. BEWIJSNORMEN EN HUN EVOLUTIE.

Lieten we in de vorige paragraaf enkele beschouwingen over het idee van "bewijzen" en de daarbij gebruikte middelen de revue passeren, in deze paragraaf zullen we aandacht besteden aan het begrip "streng" in verband met de reeds genoemde uitdrukking van "streng bewijs". Daarbij komen ook zaken aan de orde die vroeger werden aanvaard (om welke reden dan ook), maar die wij nu als niet-streng ervaren of soms zelfs als fout aanmerken. Ook komen methodische aspecten aan de orde. Wat moet onder "streng" worden verstaan? We zeggen dat een bewijs niet-streng is, en weten dan wel ongeveer wat we daarmee bedoelen. Eigenlijk zouden we moeten zeggen dat een niet-streng bewijs wiskundig gezien helemaal geen bewijs is. Het kan hoogstens als heuristiek worden getypeerd. Strengheid is verbonden met logica en grondslagen, maar daar zullen we niet erg diep op ingaan. Zoals reeds eerder gezegd, zullen we een aantal historische voorbeelden behandelen en aan de hand daarvan een beeld oproepen van het begrip "streng bewijs" en ook de betrekkelijkheid ervan (althans vanuit historisch oogpunt) illustreren.

Zijn niet-strenge bewijzen eigenlijk foute bewijzen, het kan ook gaan om slordigheden waarmee de hand wordt gelicht met de eisen van het bewijzen, terwijl men wel beter weet.

Slordigheden in bewijzen treft men nog aan in boeken van onze eeuw, ook in enkele veel gebruikte boeken. Nog in de twintiger jaren trof men de passage "zij ε een willekeurig kleine grootheid" aan, met soms als toelichting dat daarmee een grootheid werd bedoeld die tot 0 nadert. Het lijkt een vreemde toelichting. Een grootheid is toch iets dat vast, constant is? En wat is willekeurig klein? Hoe klein? Deze problematiek is natuurlijk verbonden met de oude moeilijkheden aangaande de infinitesimalen, de oneindig kleine grootheden. Hieraan heeft men pas in de hedendaagse niet-standaard analyse een solide basis kunnen geven. We

komen hierop nog terug. Het is daarom misschien beter om in het bovenstaande geval niet te spreken van een slordig taalgebruik, maar van een nog falend inzicht in de ware aard van de situatie.
Echte slordigheden, misschien beter fouten te noemen, vond men ook in sommige leerboeken, bijvoorbeeld in die van Hk. de Vries. Was hier de strengheid opgeofferd aan de didactische kwaliteit? Echter ook de zeer groten maakten zich er schuldig aan. Zo bevat ook werk van Henri Poincaré (1854-1912) slordige of schetsmatige bewijzen.
Nog in het begin van deze eeuw kon men in de elementaire meetkunde — de schoolmeetkunde — een probleem over strengheid signaleren bij het oplossen van vraagstukken. Als in de planimetrie een figuur moest worden geconstrueerd die voldoet aan zekere voorwaarden, dan behoorde die opgave uiteen te vallen in vier fasen: 1e de analyse; 2e de constructie; 3e het bewijs dat de geconstrueerde figuur aan de gestelde voorwaarden voldoet; 4e een discussie van voorwaarden waaronder er een oplosssing is. Dit waren *strengheidseisen.*
De problematiek van de strengheid komt nog tot uiting in de recente literatuur. Enkele voorbeelden mogen dit illustreren. In een aankondiging van het boek van W. Fulton, Intersection Theory (1983), vindt men over de inhoud van dit werk onder andere de volgende passage:

> "formulas from classical enumerative geometry with their first modern rigorous proof".

En uit een recent artikel over Liegroepen citeren we:

> "Firstly, Lie's Theory as is generally known, is local. (...). In order to apply to Lie's local theory the standards of precision and conceptual elegance demanded today, one can either develop the theory of local Lie groups independently of actions on a manifold and .... Or else one works within the framework of pseudo-Lie groups ... ." [21].

Het volgende citaat uit ditzelfde artikel illustreert dat het streven naar exactheid een groeiproces is:

> "Even Felix Klein, in his famed Erlangen program 1872 had tacitly assumed in defining a transformation group, that on any set a family of self-maps closed under composition had to contain the identity and inverse transformations automatically".

Vanuit de historische ontwikkeling gezien heeft het begrip strengheid verschillende aspecten. Het gaat om een *normatief begrip.* Wat men vroeger aanvaardde en als "streng" zag, aanvaarden wij thans niet zonder meer. Historisch bezien is strengheid geen absoluut begrip. Als wij bepaalde redeneringen uit het verleden als "niet-streng" betitelen, kan het zijn dat wij tot zo'n uitspraak komen omdat wij vanuit ons standpunt die redeneringen als zodanig interpreteren, soms als

ronduit fout of onvolledig moeten aanmerken. Ook "fout" moet in het licht van de historie worden bezien; misschien zag men zo'n fout niet in de ontwikkelingsfase van de wiskunde. Men bedenke dat een "fout bewijs" niet hetzelfde is als een "foute uitspraak", een "foute stelling". Het begrip "strengheid" heeft een evolutie ondergaan.
Wanneer is men gaan spreken van een "niet-streng" bewijs? Was dat in de 17e en 18e eeuw al een begrip? Wel wees men elkaar op onnauwkeurigheden, maar er is toch wel principieel verschil met wat historisch bedoeld wordt met streng of niet-streng: bij deze laatste begrippen gaat het om fundamentele kwesties.

In de wiskundige literatuur vindt men wel beschouwingen over strengheid, die dan veelal aan de hand van historische voorbeelden van niet-strenge bewijzen geïllustreerd worden. Ook wij zullen enkele voorbeelden geven; het is de bedoeling daarbij wat dieper te graven dan het louter illustratieve. Verschillende aspecten zullen aan de orde komen, zoals het ontbreken van inzichten, onjuiste inzichten, de evolutie van het idee van het "oplossen van een probleem". Het idee van "strengheid" — als we dan toch dat woord gebruiken in de context van historische ontwikkelingen — is in hoge mate gebonden aan de inzichten over het wezen van de wiskunde.

Een poging tot het analyseren van de aspecten die bij strengheid van bewijzen en bewijsmethoden in historisch verband aan de orde komen, leidt tot de volgende punten:

1. Incorrecte bewijzen die niet als zodanig werden onderkend.
2. Verkeerde of ontbrekende inzichten in de wiskunde.
3. Redeneringen die werden aanvaard — misschien onbewust — op gronden die wij thans niet meer aanvaarden. Dit betreft vaak methodologische aspecten, verbonden met principes van opbouw: algebraïsch, meetkundig enz.
4. Afwijzing van procédé's niet wegens gebrek aan inzicht, maar wegens principieel afwijkende inzichten over wat wiskunde is of moet zijn. Het gaat hierbij om kwesties van grondslagen.

Er zijn verschillende voorbeelden te geven van verschillen van inzicht op methodologisch gebied.
Zeer vermaard is een controverse tussen Réné Descartes (Cartesius, 1596-1650) en Gottfried Wilhelm von Leibniz (1646-1716) over de door Descartes in zijn in in zijn in 1637 verschenen "Géométrie" geïntroduceerde algebraïsche methoden in de meetkunde. Daarin legde hij een verbinding tussen de meetkunde en het getalbegrip; het resultaat staat bekend als de analytische meetkunde. Het bezwaar van Leibniz betrof het te automatische karakter van de methode van Descartes, waardoor het eigen meetkundig karakter van problemen niet tot zijn recht kwam. IJverig rekenen voerde tot de verlangde resultaten, waardoor de inventiviteit in het gedrang kwam. Bovendien merkte Leibniz op dat de

algebraïsche weg niet altijd de kortste was. In de tijd van Descartes schoot de algebra ook te kort wanneer het ging om transcendente krommen. Kortom, in de Cartesiaanse methodologie werd aan de algebraïsche methode een te grote waarde toegekend. Veel later heeft Poincaré soortgelijke kritiek geuit. Voor meer bijzonderheden verwijzen we naar [36].

Wellicht was Leibniz' kritiek meer gebaseerd op argumenten van utiliteit en methoden, dan op argumenten van strengheid, maar bewijsmethoden en strengheid hangen wel degelijk samen. Het volgende voorbeeld uit de complexe funktietheorie is op dit punt misschien sprekender. Er bestond een aanzienlijk verschil van inzicht tussen Karl Weierstrass (1815-1897) en Bernhard Riemann (1826-1866) over de opbouw van de complexe funktietheorie. Weierstrass gebruikte algebraïsch-analytische methoden; voor hem waren machtreeksen het fundamentele uitgangspunt. Riemann daarentegen hanteerde meer meetkundige methoden (denk aan conforme afbeeldingen, de invariantie van gebieden en aan Riemannoppervlakken). Weierstrass wantrouwde de methoden van Riemann omdat hij die, juist wegens het meetkundig karakter, in zekere zin niet streng genoeg vond. Ook heden ten dage kan men deze beide tradities in de opbouw van de complexe funktietheorie nog aantreffen: een geometrisch georiënteerde richting naast een algebraïsche richting. Wat de algebraïsche richting betreft wijzen we nog op de theorie van de algebraïsche funkties, opgezet door Richard Dedekind (1831-1916) en zijn opvolgers met methoden die ontleend zijn aan de algebra. Daarbij gaat het niet meer om wantrouwen, maar om wetenschappelijke voorkeur en interesse (zie ook [36]).

David Hilbert (1862-1943) hield in 1900 op het Internationale Mathematische Congres in Parijs een zeer indrukwekkende rede, getiteld "Mathematische Probleme". Hij somde er zijn beroemde 23 problemen op, waarvan hij verwachtte dat de bestudering ervan vooruitgang zou betekenen voor de wetenschap.
In zijn inleiding tot de lijst van problemen, maakt Hilbert ook algemene opmerkingen over het bewijzen. Zo noemt hij de eisen die aan de oplossing van een wiskundig probleem moeten worden gesteld. Allereerst moet de juistheid van het antwoord worden vastgesteld door een eindig aantal gevolgtrekkingen, op grond van een eindig aantal veronderstellingen die in de probleemstelling opgenomen zijn, en die telkens precies moeten worden geformuleerd. Hij zegt: "Diese Forderung der logischen Deduktion mittels einer endlichen Anzahl von Schlüssen ist nichts anderes als die Forderung der Strenge in der Beweisführung". Hij zegt ook dat het een vergissing is, te geloven dat strengheid en eenvoud in bewijzen niet samengaan. Talrijke voorbeelden tonen integendeel aan dat juist de strenge methode ook meteen de eenvoudigste is: "Das Streben nach Strenge zwingt uns eben zur Auffindung einfacherer Schlussweisen". Bovendien baant strengheid dikwijls de weg voor methoden die krachtiger zijn dan de oude minder strenge methoden. Hij geeft een aantal voorbeelden uit de analyse en de algebra, waarbij vooral de invloed van Weierstrass in de variatierekening veel lof toegezwaaid wordt.

Aansluitend merkt hij meteen op dat men nu niet moet denken dat alleen de analyse en de arithmetiek geschikt zijn voor uiterste strengheid. Een dergelijke houding kan uiteindelijk geen ander gevolg hebben dan dat alles wat uit de meetkunde, mechanica en natuurkunde komt wordt afgesneden van de wiskunde. Maar dit zijn nu juist belangrijke levensaders voor de wiskunde! Integendeel, zegt Hilbert, zodra in de meetkunde of in de natuurwetenschappen wiskundige begrippen opduiken heeft de wiskunde de plicht om de daaraan ten grondslag liggende principes te onderzoeken en ze door een eenvoudig en volledig systeem van axioma's zo vast te leggen dat hun scherpte en hun toepasbaarheid in deduktie in generlei opzicht onderdoen voor de oude arithmetische begrippen.
Ook maakt Hilbert nog enkele opmerkingen over de rol van *veralgemenen* en *specialiseren* bij het bedrijven van wiskunde. Hij zegt: als we een mathematisch probleem niet kunnen oplossen, dan is de oorzaak vaak te zoeken in het feit dat we het algemene gezichtspunt nog niet hebben bereikt van waaruit het specifieke probleem verschijnt als één uit een keten van verwante problemen. Na het vinden van zo'n gezichtspunt wordt het probleem vaak niet alleen meer toegankelijk voor onderzoek, maar komen we meteen in het bezit van methoden om ook de verwante problemen op te lossen. Als voorbeelden noemt hij de invoering van integratie over complexe krommen door Cauchy in de theorie van de bepaalde integralen en de introduktie door Ernst Eduard Kummer (1810-1893) van idealen in de getaltheorie.
Een nog belangrijker rol dan de veralgemening speelt volgens Hilbert de specialisering. Als we vergeefs zoeken naar het antwoord op een vraag, dan is de oorzaak van de mislukkingen meestal dat we eenvoudigere en gemakkelijkere problemen nog niet in voldoende mate opgelost hebben. Het komt er dan op aan om die gemakkelijkere problemen te zoeken en te proberen om die op te lossen met hulpmiddelen en methoden die veralgemeend kunnen worden.
Tenslotte komt het dan nog voor dat we toch niet tot een oplossing komen. Dan ontstaat de opgave om te laten zien dat het probleem onder de gegeven veronderstellingen niet is op te lossen.

Men kan Hilberts rede nalezen in [19]; een kort uittreksel is opgenomen in [43].

In de voorgaande gevallen ging het voornamelijk over verschillen van inzichten in bewijsmethoden die gekenmerkt kunnen worden als ontwikkelingen van *interne* aard: het gaat over situaties binnen de wiskunde.
Hilbert noemt echter ook uitdrukkelijk de mechanica en de natuurkunde. Inderdaad is er op het punt van kritiek op bewijsmethoden en kwesties van strengheid aanleiding om de historie in een wat breder perspectief (niet alleen binnen de wiskunde blijvend) te zien. In de 17e en 18e eeuw — en ten dele nog in de 19e eeuw — vormden onder invloed van het werk van Leibniz, Isaac Newton (1642-1727) en vele anderen de wiskunde, de mechanica en de natuurkunde nog een zekere eenheid. Er was een grote wederzijdse beïnvloeding. Hierdoor speelden *externe factoren* bij de ontwikkeling van de wiskunde een belangrijke rol, direct

of indirect. Deze fase in de ontwikkeling van de wiskunde is de *klassieke fase*, die dan ook wel *externe fase* genoemd kan worden. De onderlinge verbindingen hebben een rol gespeeld bij de gehanteerde bewijsmethoden. In de redeneringen werden overwegingen gebruikt, die ontleend waren aan de natuurwetenschappen. Uit mathematisch oogpunt aanvaarden wij zulke redeneringen thans niet langer als strenge redeneringen. Als voorbeeld noemen wij *existentiestellingen*. Existentie van zekere wiskundige objecten stond vaak vast op fysische gronden; existentie als zodanig voelde men niet als een probleem. Heel treffend is dat te zien bij de oplossing van differentiaalvergelijkingen, die veelal verband hielden met fysische problemen. De existentie van oplossingen werd ontleend aan fysische argumenten. Een concreet voorbeeld is de differentiaalvergelijking

$$\frac{dx}{dy} = f(x,y)$$

Aanvankelijk bekommerde men zich niet zo zeer om de vraag of er wel oplossingen voor dit type differentiaalvergelijkingen waren. Pas in 1814 gaf Silvestre François Lacroix (1765-1843) de oplossing in de vorm van een reeksontwikkeling voor het geval dat f analytisch is. Hij gaf echter geen bewijs dat de reeks convergeerde. Dat werd blijkbaar overbodig gevonden op natuurkundige gronden. Het ontbrekende convergentiebewijs gaf Cauchy pas in 1840, maar hij publiceerde het resultaat niet. Toch bekommerde Cauchy zich wel degelijk om strengheid.
Overwegingen van externe aard vindt men nog lange tijd in de wiskunde. Misschien kregen ze op den duur meer het karakter van heuristiek, zoals bijvoorbeeld bij Felix Klein (1849-1925) en Franz Ernst Neumann (1798-1895), gedeeltelijk ook bij Carl Neumann (1832-1925), tot laat in de 19e eeuw in de complexe funktietheorie. Fysische analogieën speelden een rol, bijvoorbeeld bij existentieproblemen van analytische funkties op Riemannoppervlakken (zie [33]).

Overigens waren er in deze externe fase ook reeds ontwikkelingen die wij thans als "niet-streng" moeten aanmerken op andere gronden dan de hantering van externe factoren. Het gaat dan om *interne factoren* die de ontwikkeling hebben beïnvloed. We geven enkele voorbeelden, en zullen daarbij wat concreter zijn dan bij de voorgaande, meer algemene, beschouwingen.

1. *Infinitesimalen.*

In de analyse, voor de grote zuivering door Weierstrass en Cauchy, riep men bij limietprocessen infinitesimalen en oneindig grote getallen te hulp. De praktijk was geen wonder van consequentheid, maar in de handen van Leibniz, Johann Bernoulli (1667-1748) en vooral Leonhard Euler (1707-1783) werden infinitesimalen juweeltjes van wiskundig vernuft. Ondanks een gevoel van onbehagen werkte men ermee. Een formulering zoals

$$\frac{\sin x}{x} \approx 1 \text{ voor infinitesimale } x$$

werkte in de praktijk. Het gebrek aan strengheid betrof hier niet een kwestie van slordigheid, maar van een nog onduidelijk inzicht in het wezen van infinitisimalen. Leibniz was echter in staat om met zijn infinitesimalen op een systematische manier resultaten te behalen, en in speciale gevallen stemden die overeen met reeds bekende resultaten waarvan de waarheid echter vaak door toeval of door grote kennis en combinatievermogen (zoals bijvoorbeeld van Christiaan Huygens (1629-1695)) waren vastgesteld. Om tot verdere voortgang te komen moest men wel werken met zo'n onduidelijk begrip, want het functioneerde.

Wat moet men exact verstaan onder een differentiaal dx, en wat onder een differentiaalquotiënt dy/dx ? Wat is het verschil tussen enerzijds $dy/dx = f(x)$ en anderzijds $dy = f(x)dx$? Is een differentiaal een oneindig kleine grootheid? Iedereen met recente ervaring in het onderwijs kent de problemen die hier worden opgeroepen. In de loop van de tijd zijn er pogingen ondernomen om een de reële getallen vervangend systeem te construeren dat ook oneindig kleine elementen ($\neq 0$) bevat. Zo'n systeem is bijvoorbeeld dat van de *duale getallen*. Dit is te beschrijven als een 2-dimensionale algebra over $\mathbf{R}$, met basis 1 en ε , waarbij $\varepsilon^2 = 0$ wordt gesteld. $\mathbf{R}\varepsilon$ is dan de deelverzameling van de infinitesimalen. Een groot probleem is echter, dat de duale getallen geen lichaam vormen. Pas in recente tijd is in de zogenaamde ***niet-standaard analyse*** een ander systeem ontwikkeld, de *hyper-reële getallen*. Het systeem van de hyper-reële getallen is een lichaam dat $\mathbf{R}$ bevat, en dat daarnaast nog oneindig kleine en oneindig grote elementen heeft. Voor een infinitesimaal ε is ε^2 nu een infinitesimaal van een hogere orde dan ε. De uitvinder van de niet-standaard analyse is Abraham Robinson (1918-1974), en inmiddels zijn er veel pogingen gedaan om zijn theorie begrijpelijker te maken. Daarbij moet zeker W.A.J. Luxemburg worden genoemd, die in [27] een interpretatie van de hyper-reële getallen heeft gegeven in de vorm van oneindig voortlopende rijtjes van reële getallen, daarbij aansluitend op werk van Schmieden en Laugwitz in [40]. Deze rijen kan men op de voor de hand liggende manier optellen en vermenigvuldigen. Er moeten echter wel equivalentieklassen worden ingevoerd om tot een lichaam te komen. Daarbij is het lemma van Zorn nodig. Dit betekent dat het model van Luxemburg niet-constructief is. Dat is echter karakteristiek voor alle modellen van de hyper-reële getallen. Ondanks dat pleit H.J. Keisler [23] er zelfs voor om in het onderwijs vanaf het begin de infinitesimaalrekening te ontwikkelen met infinitesimalen, omdat daarmee een didaktisch voordeel zou zijn te behalen. Hij kent aan de infinitesimalen een intuïtieve aanschouwelijkheid toe, en brengt de theorie zo dichter bij de oorsprong.

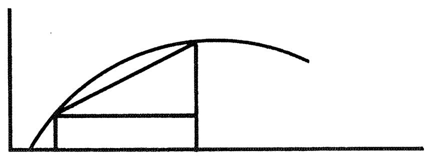
2. *Divergente reeksen.*

De praktijk van de divergente reeksen in de klassieke periode periode laat ons eveneens zien dat de mathematici van die periode met objecten manipuleerden zonder dat die objecten voldoende waren gefundeerd.
De divergente reeksen vormden nog in de tijd van Euler een niet opgehelderd

gebied. De problematiek rond convergentie en divergentie was nog niet duidelijk. Toch werkte men met divergente reeksen, en de resultaten bleken correct. In het toenmalige stadium was dit nog aanvaardbaar. Nog tegen het einde van de 19-de eeuw werkten sommigen met divergente reeksen en, zoals uit latere ontwikkelingen bleek, met succes. Een goed voorbeeld is het werk van Oliver Heaviside (1850-1926) uit ± 1887. Zonder enige rechtvaardiging te geven opereerde hij met divergente reeksen op een terrein dat wij de theorie van de operatoren noemen. Ook gebruikte hij divergente reeksen in de electrotechniek ([32]).
Ook Poincaré stuitte in zijn werk over de hemelmechanica op divergente reeksen. Poincaré kon de moeilijkheden echter overwinnen door over te gaan op asymptotische reeksen. We zullen hierop niet ingaan, maar vermelden slechts dat asymptotische reeksen te maken hebben met convergentiegedrag voor grote waarden van de variabele; het betreft een bijzondere vorm van approximatie. Overigens moet worden opgemerkt dat Emile Borel (1871-1956) tegen deze methode van Poincaré het bezwaar inbracht dat de waarde van de approximerende funktie niet exact werd gedefinieerd: met elke asymptotische reeks corresponderen oneindig veel verschillende funkties. Overigens gaf Borel wel toe dat de methode van Poincaré voor de praktijk van de hemelmechanica een bevredigende oplossing gaf. Zie [6], p. 17.

3. *De reële getallen.*

Ten aanzien van de reële getallen kan nagenoeg eenzelfde situatie als voor de divergente reeksen worden geconstateerd. Men werkte er zonder scrupules mee, lang voordat ze op strenge wijze waren ingevoerd. Dat laatste gebeurde pas in een fase die in zekere zin de moderne tijd inluidde.
Vermeldenswaard is Dedekind's boekje "Stetigkeit und irrationale Zahlen" (1872), waarvan de inhoud al stamt uit 1858. Deze tekst is nog steeds verkrijgbaar (zie [12]). In de eerste bladzijden hiervan zegt Dedekind dat hij het voornemen heeft om een echt wetenschappelijke basis te geven aan het wezen van de continuïteit der reële getallen. Hij doelt hierbij op de stelling dat iedere begrensde, monotoon stijgende rij een limiet heeft. Hier treft men dus een behoefte aan strengheid aan, omdat de toenmalige situatie onbevredigend werd gevonden. Om die onbevredigende situatie toe te lichten, moet worden opgemerkt dat men lang een zeker "fysisch" beeld van de reële getallen had in de vorm van de rechte lijn, de getallenrechte. Dat beeld wordt trouwens nog steeds gebruikt. Het is een fysische realiteit, maar is het ook een mathematische realiteit? In de beginfase van de infinitesimaalrekening geeft men nog steeds bewijzen aan de hand van figuren zoals hier getekend.



Vanzelfsprekend zijn dat geen strenge bewijzen, maar zulke tekeningen geven wel uitstekend de basisgedachten voor een streng bewijs weer. Dedekind schrijft: "Auch jetzt halte ich ein solches Heranziehen geometrischer Anschauung bei dem ersten Unterrichte in der Differentialrechnung vom didaktischen Standpunkte aus für ausserordentlich nützlich, ja unentbehrlich, wenn man nicht gar zu viel Zeit verlieren will. Aber dass diese Art der Einführung in die Differentialrechnung keinen Anspruch auf Wissenschaftlichkeit machen kann, wird wohl niemand leugnen". Dedekind vindt de oplossing van het probleem der continuïteit door de invoering van de "Dedekindse sneden", uitgaand van de rationale getallen. Georg Cantor (1845-1918) definieert de irrationale getallen met behulp van de zogenaamde fundamentaalrijen. Dit is equivalent met de sneden van Dedekind, maar ook bruikbaar voor de completering van algemene metrische ruimten. Dedekind was in zekere mate een wegbereider voor Cantor.
Over de bovengenoemde fysische aanschouwing willen we nog een opmerking maken. Dergelijke aanschouwelijke beelden zijn volstrekt onmogelijk wanneer men een analyse opbouwt over het lichaam $\mathbf{Q}_p$ van de p-adische getallen. Evenals $\mathbf{R}$ is ook $\mathbf{Q}_p$ een uitbreiding van het lichaam $\mathbf{Q}$ van de rationale getallen, maar dan ten opzichte van een andere metriek dan de gewone absolute waarde op $\mathbf{Q}$. Van $\mathbf{Q}_p$ is geen fysisch beeld zoals van $\mathbf{R}$. Bewijzen van resultaten over $\mathbf{Q}_p$ moeten dus wel puur algebraïsch-analytisch zijn. Dan is er geen gevaar dat door het hanteren van figuren het aannemen van incorrecte relaties tussen continuïteit, differentieerbaarheid en doorlopendheid binnensluipt.

4. *Complexe getallen.*

Ook met de complexe getallen werkte men lang voordat de ware aard ervan doorgrond was. Zo had Euler al de betrekking

$$e^z = e^x(\cos y + i \sin y) \text{ als } z = x + iy.$$

In deze vroege periode (eerste helft van de 18-de eeuw) was er nog geen fysisch meetkundig beeld; de weergave van de complexe getallen in een plat vlak volgde pas in een later stadium. In zekere zin werden de complexe getallen toegepast als methode. Een strenge rechtvaardiging werd pas door Carl Friedrich Gauss (1777-1855) gegeven.
In dit kader past een opmerking over het werk van Gauss aangaande de zogenaamde hoofdstelling van de algebra:

elke algebraïsche vergelijking heeft in $\mathbf{C}$ tenminste één wortel.

Gauss had kritiek op eerdere bewijzen van D'Alembert en van Lagrange. In de loop der jaren gaf Gauss vier bewijzen van deze stelling (zie [26]). Het is interessant te lezen wat F. Klein daarover schrijft in zijn boek "Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert" (Berlijn, 1926/1927). Op blz. 51 e.v. wijdt Klein historische beschouwingen aan het begrip "streng". Over het eerste bewijs van Gauss van de hoofdstelling merkt Klein op dat het

in principe juist is, echter niet volledig omdat Gauss stilzwijgend eigenschappen van algebraïsche krommen gebruikte. Eens te meer blijkt uit deze episode dat "strengheid" een begrip is dat in de historie met voorzichtigheid moet worden benaderd.
Zoals gezegd gaf Gauss vier bewijzen van de hoofdstelling van de algebra. Dat men, naast verbeteringen, verschillende bewijzen geeft voor eenzelfde stelling, is een verschijnsel dat vaker optreedt. Het kan te maken hebben met nieuwe ontwikkelingen, waardoor de betreffende stelling ook vanuit een nieuw gezichtspunt kan worden bewezen. Ook kan het zijn dat een weliswaar goed bewijs in een later stadium toch betrekkelijk omslachtig of onduidelijk blijkt. Een goed voorbeeld van zo'n stelling is de fundamentele stelling van Cauchy over de integraal van een complexe funktie over een gesloten kromme in C. We geven de formulering zoals die te vinden op p.48 van [25]:

> Als $f(z)$ regulier is in het enkelvoudig samenhangend gebied G, dan is $\int_C f(z)dz = 0$ als C een willekeurige gesloten pad aanduidt dat geheel binnen G ligt.

De moeilijkheden bij deze stelling liggen vooral op het gebied van de topologie. De eisen die aan C worden opgelegd (C is een *pad*; zie [25], p.13-14) zijn tamelijk ingewikkeld. Nog vele jaren na het bewijs van Cauchy in zijn "Mémoire sur les intégrales définies, prises entre des limites imaginaires" dat in 1825 verscheen — zelfs nadat Riemann in 1851 de complexe funktietheorie op solide basis had gezet — werd in boeken en artikelen aangekondigd dat een streng bewijs zal worden gegeven van Cauchy's stelling. Volledig bevredigende bewijzen konden pas worden gegeven nadat de topologie een zeker stadium van ontwikkeling had bereikt.

5. *De begrippen kromme en dimensie.*

In de 19-de eeuw (tenminste tot 1878) was het gebruikelijk om de dimensie van een variëteit te definiëren als het aantal benodigde parameters bij parametrisering (naar Riemann: die Ortsbestimmung in einer n-fach ausgedehnten Mannigfaltigkeit ist auf n Grössenbestimmungen zurückzuführen). In de natuurkunde is hieraan het begrip "aantal vrijheidsgraden" gekoppeld. In de definities uit die tijd werd van een n-dimensionale variëteit (eine nach n Dimensionen ausgedehnte Mannigfaltigkeit) V slechts geëist dat er een ééneénduidige beschrijving is door een systeem van n coördinaten. De gangbare formulering was:

> de elementen van V hangen af van n onderling onafhankelijke reële continue variabelen $x_1, x_2, \dots, x_n$, zo dat bij elk element van V een toelaatbaar systeem van waarden (ein zulässiges Werthsystem) $x_1, x_2, \dots, x_n$ hoort en andersom.

Impliciet werd als vanzelfsprekend aangenomen dat het verband tussen V en het coördinatensysteem een continu verband is.

G. Cantor toonde in 1878 (zie [10]) aan dat het mogelijk is om twee variëteiten van verschillende dimensie (beide ≥ 1) eeneenduidig op elkaar af te beelden. Hij liet expliciet zien dat de verzameling

$$\{(x_1, x_2, \ldots, x_n) \in \mathbf{R}^n | 0 < x_i < 1\}$$

gelijkmachtig is met het interval (0,1) in $\mathbf{R}$. Hij gaf een tamelijk ingewikkeld aandoende redenering, waarin gebruik wordt gemaakt van kettingbreuken. Het tegenwoordig meest gangbare elementaire bewijs gaat uit van het gegeven dat ieder reëel getal > 0 eenduidig is te schrijven als een oneindig voortlopende decimale breuk (0,25 schrijven we dus in de vorm 0,2499999...). Voor bijvoorbeeld $n = 2$ voegen we nu in principe aan $x = 0, a_1a_2a_3a_4\ldots$ het paar $x_1 = 0, a_1a_3a_5\ldots$ en $x_2 = 0, a_2a_4a_6\ldots$ toe. Het is de bedoeling dat aldus een afbeelding ontstaat van $(0,1]$ op $(0,1] \times (0,1]$ waarvan ook de inverse duidelijk is. Dit is nog niet helemaal correct, want voor $x = 0,11101010101\ldots$ zou $x_2 = 0,1000\ldots$ zijn, in tegenstelling met de eis van oneindig voortlopende breuken. Het is wel in orde als we voor de a_i telkens een aaneensluitend *blok* van cijfers nemen dat eindigt op het eerstvolgende cijfer $\neq 0$. Dus bij bijvoorbeeld $0,30010620073804\ldots$ is $a_1 = 3, a_2 = 001, a_3 = 06, a_4 = 2, a_5 = 007, a_6 = 3, a_7 = 8, a_8 = 04$, etc..
Cantor deed met zijn constructie een wereldschokkende ontdekking: voortaan zal men in de definitie van een n-dimensionale variëteit expliciet moeten opnemen dat de coördinatisering een continue afbeelding moet zijn. Zonder deze eis is het zinloos om te spreken van een n-dimensionale variëteit, omdat alle variëteiten van dimensie ≥ 1 onderling gelijkmachtig zijn.
Cantor, Jürgens, Lüroth, Netto en Thomae (zie bijv. [37]) haastten zich te bewijzen dat een afbeelding

$$\mathbf{R}^n \to \mathbf{R}^m \quad (n > m)$$

onmogelijk zowel eeneenduidig als continu kan zijn, want zoals Hans Freudenthal het formuleert in [15]:

> "Man kam auf die bange Frage, ob man die Räume verschiedener Dimension wenigstens im Bereich der eineindeutigen stetigen Abbildungen voneinander unterscheiden könne, dem Problem der Dimensionsinvarianz".

Ondanks verwoede pogingen daartoe, lukte het alleen voor kleine m ($m = 1, 2$, en uiteindelijk 3 (Lüroth)). Steeds weer bleek de intuïtie toch onmisbaar en misleidend.
Een waterdicht bewijs voor het algemene geval werd pas geleverd door L.E.J. Brouwer in 1911 (zie [8]). Brouwer publiceerde in 1913 tevens als eerste een nieuw, inductief geformuleerd, begrip van dimensie, waarvan bepaalde karaktertrekken reeds in het werk van eerder genoemde onderzoekers te onderkennen

zijn. Later is dit dcor P. Urysohn en K. Menger uitgewerkt tot het tegenwoordige klassieke begrip van dimensie.

Niet te scheiden van de moeilijkheden in de dimensietheorie zijn de problemen die men had bij het begrip *kromme*. In zijn "Cours d'Analyse" definieerde Camille Jordan (1838-1922) het begrip *continue kromme* in het platte vlak op de manier waarop wij het nu nog kennen: geëist wordt een continue parametrisering in één variabele t die het segment [0,1] doorloopt.
Hoe ingewikkeld de materie was, bleek in 1890 toen Giuseppe Peano (1858-1932) de tweede forse stoot uitdeelde aan de intuïtie. Hij liet aan de hand van een voorbeeld zien dat het segment $[0,1]$ continu kan worden afgebeeld *op* het vierkant $[0,1] \times [0,1]$ (zie [38]).
Peanos vondst heeft niets geheimzinnigs. Hij schrijft elk reëel getal in [0,1] in het 3-tallig stelsel, en geeft een algoritme om daaruit twee reële getallen te bepalen, laat zien dat elk paar in $[0,1] \times [0,1]$ gevormd kan worden, en dat de zo gemaakte afbeelding continu is.
Voor de nieuwsgierige lezer geven we Peanos algoritme:
Als $x = 0, a_1a_2a_3\ldots$ de 3-tallige breuk is (dus $x = \sum a_i/3^i$), dan is (eveneens in het 3-tallig stelsel) $x_1 = 0, b_1b_2b_3\ldots$ en $x_2 = 0, c_1c_2c_3\ldots$, waarbij

$b_1 = a_1$

$c_1 = a_2$ als a_1 even is, en $c_1 = 2 - a_2$ als a_1 oneven is,

en voor $n \geq 2$ geldt

$b_n = a_{2n-1}$ als $a_2 + a_4 + \ldots + a_{2n-2}$ even is,

$b_n = 2 - a_{2n-1}$ als $a_2 + a_4 + \ldots + a_{2n-2}$ oneven is,

$c_n = a_{2n}$ als $a_1 + a_3 + \ldots + a_{2n-1}$ even is,

$c_n = 2 - a_{2n}$ als $a_1 + a_3 + \ldots + a_{2n-1}$ oneven is.

Het gaat er bij de berekening van b_n uit a_{2n-1} dus steeds om of van de voorgaande cijfers a_i *met* i *even* de som even of oneven is, en analoog is bij de berekening van c_n uit a_{2n} de som van de voorgaande cijfers a_i *met* i *oneven* bepalend.
Het voorschrift houdt rekening met meerduidige schrijfwijzen. Zo levert $x = 0,120121222\ldots$ de getallen $x_1 = 0,100222\ldots$ en $x_2 = 0,011000\ldots$ op en de andere schrijfwijze $y = 0,120122000\ldots$ voor x geeft $y_1 = 0,100222\ldots$ en $y_2 = 0,010222\ldots$. Daar het 3-tallige schrijfwijzen betreft, is $x_2 = y_2$.

Het voorbeeld van Peano is overtuigend, maar het is een arithmetische constructie, en geeft geen inzicht in de meetkundige aard. Hierin werd al snel voorzien door D. Hilbert, die in hetzelfde jaar 1890 voor het Gesellschaft deutscher Naturforscher und Aerzte een voordracht hield, waarin hij een *meetkundige* constructie gaf van een kromme die het eenheidsvierkant opvult (zie [18]). Het idee bestaat uit het construeren van eenvoudige benaderende krommen, die geen van alle het vierkant vullen, maar waarvan de uniforme limiet wel "vlakvullend" is. Na Hilbert kwamen er anderen met soortgelijke constructies (we noemen E.H. Moore, H. Lebesgue, W. Sierpinski) en F. Klein gaf een dergelijke constructie voor het oorspronkelijke voorbeeld van Peano.

Het blijkt dus, dat het begrip continue kromme te algemeen is (men zal een vol vierkant geen kromme willen noemen!). Anderzijds is het ook weer te beperkt, want een figuur als

$$\{(x,y) \in \mathbf{R}^2 | 0 < x \leq 1, y = \sin(1/x)\}$$

uitgebreid met zijn limietpunten

$$\{(x,y) \in \mathbf{R}^2 | x = 0, -1 \leq y \leq 1\}$$

valt er niet onder. Desalniettemin heeft Jordans definitie alle kritiek overleefd: onder een kromme verstaat men tegenwoordig algemeen de continue kromme.

Al vóór Jordan had Cantor het begrip *continuüm* gedefinieerd. Een deelverzameling van het platte vlak kan hij dan een kromme noemen als het een continuüm is zonder inwendige punten. Vanuit analytisch standpunt is dit niet hanteerbaar. Wel is er een nauw verband tussen continua en homeomorfe beelden van segmenten en cirkels, indien men eisen stelt over het aantal punten dat uit een continuüm moet worden weggelaten om het resterende deel onsamenhangend te maken. Het homeomorfe beeld van een cirkel (we bedoelen steeds cirkel*omtrek*) staat tegenwoordig algemeen bekend onder de naam Jordankromme. Jordan heeft dat verdiend met zijn befaamde stelling dat het platte vlak door elk continu eeneenduidig beeld S van een cirkelomtrek wordt verdeeld in twee disjuncte gebieden die ieder S tot rand hebben. Deze eigenschap leidde Arthur Schoenflies (1853-1928) tot zijn definitie van *gesloten kromme*: Een deelverzameling K van het vlak heet een gesloten kromme als het complement van K bestaat uit twee gebieden, die ieder K als rand hebben.
Hierover en over aanverwante zaken verrichtte hij diepgaand onderzoek. Hoezeer ook hem de intuïtie parten speelde, bleek in 1910, toen (alweer) Brouwer (zie [7]) aan de hand van een voorbeeld een hele lijst opsomde van foute stellingen van Schoenflies. Brouwers voorbeeld behelst een kromme die het vlak verdeelt in drie (!) gebieden, en van elk van die gebieden is ze de rand! Een populaire versie (Lakes of Wada) hiervan gaat uit van een eiland met twee meren. Door het successievelijk graven van steeds smaller en langer wordende kanalen vanuit de twee meren en vanuit de zee ontstaat het voorbeeld: de kromme is het overblijvende land en de drie gebieden zijn de zee en de twee meren met hun respectievelijke kanalen (zie [20]).

Voor wie meer wil lezen over bovenstaande zaken, zijn [14], [45], [48], en de levensbeschrijving van Brouwer in [9] aanbevolen. Over de huidige stand van zaken kan in vrijwel ieder boek over topologie nadere informatie worden ingewonnen. Goed leesbaar is bijvoorbeeld [20].

6. *De meetkunde van het aantal.*

Bij de bespreking van de algemene aspecten van het fenomeen "bewijzen" zoals dat in de wiskunde fungeert, wezen we erop dat bewijzen is verbonden met het fundamentele idee dat uit het bijzondere geval niet zonder meer een conclusie kan worden getrokken met betrekking tot het algemene geval. We hebben toen het eenvoudige geval van eigenschappen in driehoeken genoemd. De meetkunde van het aantal is een voorbeeld waarbij in de historische ontwikkeling juist wel de weg van het bijzondere naar het algemene geval werd gevolgd, zij het met toepassing van een bepaald principe. In de moderne wiskunde is de meetkunde van het aantal overgegaan in het gebied van de algebraïsche meetkunde, alwaar het is voorzien van een strenge basis. Dit voorbeeld illustreert dus de overgang van een vage heuristische methode naar een strenge behandeling.

De meetkunde van het aantal is, zoals reeds eerder opgemerkt, verbonden met de naam van H. Schubert wegens zijn beroemde boek "Kalkül der abzählenden Geometrie". Het probleem is als volgt te omschrijven.

> Bepaal het aantal meetkundige figuren van een zeker type dat aan voorgeschreven condities voldoet. Hieronder vallen bijvoorbeeld raakproblemen en snijproblemen.

Een typisch voorbeeld is de vraag naar het aantal lijnen in $\mathbf{R}^3$ dat vier gegeven lijnen snijdt. Schubert kwam tot het antwoord: 2 of ∞. Hij vond dit antwoord door de vier gegeven lijnen in speciale posities te bekijken waarvoor de uitkomst evident is, en op continuïteitsgronden concludeerde hij vervolgens dat dit antwoord in het algemeen goed is. Schubert hanteerde hier het *principe van het behoud van het aantal.*
Een speciale positie van de vier gegeven lijnen in het genoemde voorbeeld is die waarbij twee van de vier gegeven lijnen elkaar snijden. Dan zijn er inderdaad twee lijnen die de vier gegeven lijnen snijden. Immers, laat de gegeven lijnen aangeduid worden door a, b, c, d, waarvan a en b elkaar snijden in punt A. Zij V het vlak door a en b. Dan hebben c en d snijpunten met V, en deze bepalen een lijn die voldoet. De andere lijn die voldoet gaat door A en het snijpunt van d met het vlak bepaald door A en c.

Schubert behandelde met dit principe gecompliceerde problemen, bijvoorbeeld de klassieke stelling van Bezout over het aantal snijpunten van algebraïsche krommen. Een ander voorbeeld is de vraag naar het aantal kwadratische oppervlakken in $\mathbf{R}^3$ dat aan 9 gegeven kwadratische oppervlakken raakt. Met dit soort problemen hield J. Steiner zich reeds bezig. Zonder bewijs poneerde deze in 1848 de foutieve stelling dat er 6^5 kegelsneden zouden zijn die raken aan 5 gegeven kegelsneden.

De geschiedenis van de meetkunde van het aantal gaat terug tot Victor Poncelet (1788-1867). Poncelet wilde de meetkunde bevrijden van de dominerende invloed van de algebraïsche methoden die geïntroduceerd waren door Descartes (vergelijk de reeds eerder genoemde kritiek van Leibniz). Poncelet gebruikte in zijn meetkundige beschouwingen het zogenaamde *continuïteitsprincipe.* Dit principe zegt ongeveer: bij continue bewegingen blijven eigenschappen behouden. Een typisch voorbeeld is het geval van raaklijnen aan een cirkel. Door een punt buiten de cirkel kunnen twee raaklijnen aan de cirkel worden getrokken. Volgens Poncelet moeten er dan door een punt binnen de cirkel ook twee raaklijnen aan de cirkel gaan, maar dat zijn dan (conform Poncelet) imaginaire raaklijnen. Hij vond het niet nodig om dat begrip "imaginair" nauwkeurig in te voeren.

Het continuïteitsprincipe heeft een algebraïsche achtergrond. Algebraïsch worden de bovenstaande vraagstellingen uitgedrukt door algebraïsche vergelijkingen. Onder variatie van de hierin optredende constanten (coëfficiënten) blijft het aantal wortels gelijk, of wordt ∞ als alle coëfficiënten 0 worden. De genoemde problemen zijn echter moeilijk algebraïsch te behandelen en daarom volgde Poncelet de zuiver meetkundige weg.

Aan Cauchy was het principe bekend. Hij verwierp het als ongefundeerd en sprak er over als "forte induction". Desondanks bleef men er mee werken. Poncelet beschouwde het continuïteitsprincipe als een soort axioma, een grondwaarheid, puur meetkundig te aanvaarden en niet tot eenvoudiger concepten terug te brengen.

Omstreeks 1870 kwam het continuïteitsprincipe onder de aandacht van Schubert. Hij gebruikte in zijn "Kalkül" het principe van het behoud van het aantal, dat met Poncelet's principe verwant is. Hoewel er aanwijzingen zijn dat Schubert een rechtvaardiging noodzakelijk achtte, hanteerde hij zijn principe zonder commentaar.

Gaandeweg groeide echter het wantrouwen tegen Schubert's en Poncelet's principes, en werden er ook fouten gevonden. In zijn reeds genoemde rede in 1900 noemde Hilbert ook de meetkunde van het aantal als bijzonder aandachtsgebied: probleem 15 is "Strenge Begründung von Schuberts Abzählungskalkül". Hilbert wilde terug naar een algebraïsche behandeling. Hij vroeg erom, de eliminatie in bijzondere gevallen zo uit te voeren dat de graad van de uiteindelijke vergelijkingen en de multipliciteit van de oplossingen ervan voorspelbaar zijn ("sich voraussehen lässt").
Het onderzoek kwam in handen van de algebraici, en leidde tot de moderne algebraïsche meetkunde. Het is een merkwaardige ontwikkeling, want Poncelet wilde juist de algebra vermijden. Hij wilde de meetkundige methode perfectioneren omdat die was achtergebleven bij de analytische meetkunde.

De huidige situatie ten aanzien van de *meetkunde* van het aantal is niet zo somber als door het bovenstaande wellicht gesuggereerd wordt. Er zijn tegenwoordig ook topologisch gerichte onderzoekingen op dit gebied, met onder andere doorsnijdingen, multipliciteiten en singulariteiten als onderwerpen (zie [16], [17], [24], [41]).

7. *Moderne bewijsproblematiek.*

De tot nu toe behandelde voorbeelden betreffen enerzijds ontwikkelingen die niet gefundeerd waren wegens nog ontbrekende inzichten in het wezen van de zaak en die we daarom als niet-streng moeten aanmerken. Anderzijds hebben we ook de zogenaamde externe methoden en overwegingen genoemd die we thans afwijzen als strenge mathematische methoden. Er zijn veel meer van dergelijke voorbeelden uit de ontwikkelingsgang van de wiskunde aan te wijzen, zoals de klassieke kwestie van het onderscheid tussen continuïteit en differentieerbaarheid van funkties, de klassieke misvattingen over de convergentie van de Fourierreeks van een continue funktie, het niet steeds onderkende onderscheid tussen supremum en maximum, het isoperimetrische probleem (deze beide laatste onderwerpen komen uitgebreid aan de orde in de volgende paragrafen). Ook vermeldenswaard zijn pogingen tot oplossing van problemen, waarvan pas later kon worden vastgesteld dat ze tot mislukking gedoemd waren. Voorbeelden hiervan zijn de trisectie van de hoek, de kwadratuur van de cirkel, het oplossen van de algemene vergelijking van de 5-de graad vóór Niels Henrik Abel (1802-1829) en Evariste Galois (1811-1832).

Rond de eeuwwisseling van de 19-de naar de 20-ste eeuw begonnen zich ontwikkelingen voor te doen waarbij *verschil van inzicht* in het wezen van de wiskunde aanleiding was tot het ter discussie stellen van theorieën, methoden en resultaten. Dat had niet zozeer te maken met kwesties van strengheid in bewijzen, maar met kwesties van principe. Hierdoor werd de problematiek op een breder plan gebracht. We zullen deze problemen niet in volle algemeenheid behandelen, maar ons beperken tot enkele saillante opmerkingen.

Vroeger (ruwweg vóór 1900) was er betreffende de bewijsproblematiek nog een zekere mate van objectiviteit, afhankelijk van het ontwikkelingsstadium. Met Cantor en zijn theorie van de verzamelingen doen meer subjectieve elementen hun intrede in de aanvaarde bewijsmethoden. Die subjectiviteit komt voort uit wisselende inzichten in het wezen van de wiskunde voor zover het de noodzakelijk geachte fundering van theorieën betreft. Het is geen subjectiviteit in die zin dat ieder er zijn eigen idee over geoorloofde maatstaven van strengheid op na kan houden. Er blijft theorievorming, maar er kunnen verschillende theorieën ontstaan door de verschillen in inzicht over de fundering van theorieën. Daardoor ontstaan ook discussies over de aanvaardbaarheid van mathematische concepties.

Een voorbeeld is de ontwikkeling van het *funktiebegrip*. De ontwikkeling van het begrip funktie als analytische uitdrukking — ver voor Cantor — met begrippen als continuïteit en doorlopendheid, naar het begrip afbeelding is van lange duur geweest. Het was Peter Gustav Lejeune Dirichlet (1805-1859) die als eerste de analytische uitdrukking van het eerste plan verdreef. Maar er is wel een en ander gebeurd voordat men bij het algemene begrip van een afbeelding bij Bourbaki is gekomen. Rond de eeuwwisseling was er een fundamentele discussie, onder andere tussen René Baire (1874-1932), E. Borel en Henri Lebesgue (1875-1941), over de vraag welke funkties nog aanvaardbaar zijn. De hier genoemde wiskundigen worden semi-intuïtionisten genoemd (eerst L.E.J. Brouwer zou het intuïtionisme funderen) en aanvaardden in principe alleen constructieve

concepten. De discussie ging over de kwestie van *definitie* versus *existentie*: bestaat alles wat wordt gedefinieerd?
Men moet hierbij denken aan definities die van het normale patroon afwijken, bijvoorbeeld aan definities die samenhangen met de decimale ontwikkeling van π : het al of niet voorkomen van een gegeven eindige rij van cijfers daarin. Het betreft definities die afhangen van een enigma, d.w.z. een (nog) onopgelost probleem. Een ander curieus voorbeeld is een definitie waarin het aantal Fransen voorkomt dat is gesneuveld in de slag bij Waterloo. Is zo'n definitie toelaatbaar in de wiskunde? Is dit een "strenge" definitie? Is het überhaupt een mathematische definitie? Voor meer details verwijzen we naar [31].

In essentie gaat het hier om *effectiviteit* en *constructiviteit*. Wil men die als strengheidseisen zien, dan moet het begrip "streng" wat ruimer worden opgevat dan in "streng bewijs". Hier zijn meer wezenlijke zaken in de wiskunde aan de orde.

Met Cantor begint een nieuwe periode. *Externe* motiveringen en rechtvaardigingen — voor zover nog aanwezig in de laatste decennia van de 19-de eeuw — worden vervangen door *interne* overwegingen en daarmee gepaard gaan andere strengheidscondities, die beginnen te raken aan het wezen van de wiskunde.

We willen nog enkele opmerkingen maken over een belangrijke bewijsprincipe uit de moderne periode: het *keuze-axioma*. Dit luidt als volgt:

> Zij W een niet-lege familie van niet-lege verzamelingen. Dan bestaat er een funktie f die aan elke $V \in W$ een element $f(V) \in V$ toevoegt.

Het keuze-axioma werd voor het eerst geformuleerd door Ernst Zermelo (1871-1953) in 1904 en was een onderwerp van fundamentele discussie. Uiteraard ging het daarbij om effectiviteit: kan zo'n f steeds effectief worden aangegeven? Een goed voorbeeld is de verzameling W van de equivalentieklassen in $\mathbf{R}$ onder de equivalentierelatie $x \sim y \quad \leftrightarrow \quad x - y \in \mathbf{Q}$. Voor elke equivalentieklasse moeten we dan een element van die equivalentieklasse kunnen aanwijzen. Anders geformuleerd: construeer een deelverzameling A van $\mathbf{R}$ zodat A van elke equivalentieklasse precies één punt bevat. Niemand is er nog in geslaagd een dergelijke A expliciet aan te geven. Het keuze-axioma is een niet-constructief apparaat. Er bestaan enkele veel gebruikte equivalenten van dit axioma, o.a. het lemma van Zorn (Max Zorn), dat handelt over de existentie van maximale elementen in partieel geordende verzamelingen (zie [36]).

We illustreren de bewijsproblematiek rond het keuze-axioma nog aan een ander voorbeeld. Reeds Cauchy beschouwde de funktionaalvergelijking

$$f(x+y) = f(x) + f(y), \qquad (x, y \in \mathbf{R},\ f : \mathbf{R} \to \mathbf{R})$$

Onder de conditie dat f continu is, is het eenvoudig aan te tonen dat een oplossing f een lineaire funktie is (dat kan trouwens onder veel zwakkere condities worden bewezen). Dan ontstaat de vraag: bestaan er niet-lineaire (dus discontinue) oplossingen? Met het lemma van Zorn kan men bewijzen dat dit het geval is. Deze methode van bewijzen is echter niet-constructief, en men kan (nog) geen enkele discontinue oplossing effectief aangeven. In [36] heb ik de uitdrukking "zwakke existentie" gebruikt voor resultaten waarvan alleen niet-constructieve bewijzen bekend zijn, in tegenstelling tot "sterke existentie" (constructieve existentie).

Het probleem is, of men zwak existentiële resultaten wil aanvaarden. De intuïtionisten wijzen ze op principiële gronden af. Is het vraagstuk over de existentie van niet-continue oplossingen van de bovenstaande funktionaalvergelijking nu wel of niet opgelost, streng opgelost? Wat is het "oplossen van een probleem"? Het hangt er van af wat men meent te kunnen aanvaarden. Het gaat niet om "strengheid" in de oude traditionele betekenis, maar om een pricipiële zaak. Maar ging het daar ook vroeger niet om, toen men externe (fysische) overwegingen aanvaardbaar vond, althans als heuristiek? Een groot verschil lijkt te zijn, dat men vroeger de externe overwegingen als vanzelfsprekend aannam, terwijl het gebruik van principes zoals het keuze-axioma expliciet wordt vermeld. Pas wanneer zwak existentiële resultaten of methoden worden gebruikt zonder dat te onderkennen (door slordigheid: het keuze-axioma lijkt een evident ware uitspraak), kan daarop het begrip "niet-streng" van toepassing zijn. In die zin kunnen we zeggen:

> "Strengheid" kan een kwestie van nauwkeurigheid zijn, maar ook een kwestie van principiële aard, verbonden met inzichten over het wezen van de wiskunde.

We besluiten deze paragraaf met enkele opmerkingen van fundamentele aard. De voorbeelden geven aanleiding de vraag de stellen wat de rol is geweest van befaamde historische fouten in de wiskunde. Beziet men de ontwikkelingsgang, dan kan worden vastgesteld dat misvattingen en fouten soms een scheppende rol hebben vervuld bij de opbouw van de wiskunde. Dat gebeurde dan meestal onbewust, zodat men misschien beter kan spreken van conclusies achteraf. Het is een zaak van vallen en opstaan geweest. Het in paragraaf 4 te bespreken probleem van de isoperimetrie is in dit opzicht bijzonder illustratief. Is het te gewaagd om te veronderstellen dat misvattingen ook heden ten dage nog een scheppende rol kunnen vervullen? Aan dit ontwikkelingsaspect wordt weinig aandacht besteed. Deze facetten van de gang van de ontwikkelingen zijn behalve vanuit historisch oogpunt ook interessant vanuit didaktisch standpunt. Het zou nuttig zijn om er eens oude boeken op na te slaan.

In de volgende paragrafen staat het zogenaamde isoperimetrische probleem in het centrum van de beschouwingen, een klassiek probleem uit de meetkunde. Het voor de oplossing van dit probleem door Steiner gegeven onjuiste, of op zijn minst onvolledige, bewijs hangt samen met het daarbij door hem niet onderkende onderscheid tussen maximum en supremum. Wij groeperen de beschouwingen rond dit incorrecte bewijs. Ter inleiding laten wij een bespreking van enkele extremaalproblemen uit de elementaire meetkunde voorafgaan, waarbij het onderscheid tussen maximum en supremum eveneens een rol speelt. Wij doen dit mede om er nog eens de aandacht op te vestigen dat de elementaire meetkunde, de niet gealgebraïzeerde meetkunde, nog steeds de mogelijkheid biedt om interessante onderwerpen daaruit aan de orde te stellen. Zij kunnen een aanloop zijn tot diepere zaken zoals hier het isoperimetrische probleem en de theorie van convexe lichamen. We hopen dat de behandeling hier een pleidooi zal zijn om nog eens oudere boeken te raadplegen. Het gaat dan weliswaar vaak om oudere zaken, maar hoevelen kennen ze nog en realizeren zich de betekenis ervan?

Het onjuiste bewijs van Steiner kan in een breder perspectief worden geplaatst, waarbij het eveneens gaat om het ontbrekend inzicht in maximum en supremum. In de analyse, in het bijzonder in de potentiaaltheorie en de complexe funktietheorie, zijn er in dit verband zeer ingrijpende analoge ontwikkelingen geweest. Daaraan zijn verbonden de namen van Dirichlet en Riemann. Het is niet onze bedoeling om ook daarop uitvoerig in te gaan, zodat we met enkele korte indicaties daarover volstaan. Overigens is juist dat bredere perspectief aanleiding om het isoperimetrische probleem wat meer in detail te behandelen. Wie er meer over wil lezen zij verwezen naar [3], [4], [5].

3. MAXIMA EN MINIMA.

"Maxima en minima" valt bij de schoolwiskunde onder het onderwerp differentiaalrekening. Meestal geven de problemen aanleiding tot een zekere funktie waarvan de afgeleide gelijk aan 0 wordt gesteld. Hoe gemakkelijk wordt daarbij niet vergeten dat dit slechts een noodzakelijke voorwaarde is? Het is het eenvoudigste geval van de problemen uit de klassieke variatierekening: het onderzoek naar extrema van veel algemenere funkties, funkties gerepresenteerd door integralen. De klassieke methode herleidt een dergelijk probleem tot een differentiaalvergelijking (de vergelijking van Euler-Lagrange), waarbij zich dan de problematiek van nodige en voldoende voorwaarden voordoet. Later is voor dergelijke problemen de zogenaamde *directe methode* ontwikkeld, waarbij rijen van passende objecten (funkties, krommen) worden geconstrueerd die door convergentiebeschouwingen rechtstreeks tot het extremale object voeren. In het nu volgende gaat het over deze directe methode.

We behandelen enkele extremaalproblemen uit de Euclidische meetkunde in het platte vlak. J. Steiner heeft vele van dergelijke problemen geformuleerd en met elementaire meetkundige middelen behandeld (zie [42]). We noemen er enkele:

a. Van alle driehoeken met gegeven basis en omtrek heeft de gelijkbenige de grootste oppervlakte.

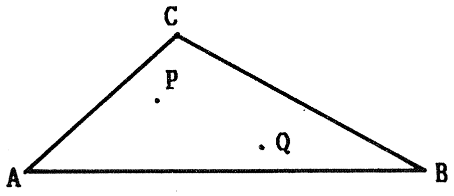
b. Van alle driehoeken met gegeven basis en gelijke oppervlakte heeft de gelijkbenige de kleinste omtrek.

c. Van alle driehoeken met gelijke tophoek en gelijke som van de opstaande zijden heeft de gelijkbenige de grootste oppervlakte en de kleinste basis.

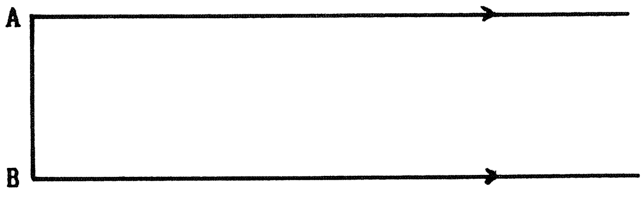
Steiner behandelde ook vraagstukken over de cirkel en over algemenere convexe figuren.

De volgende problemen dienen ter inleiding van het isoperimetrische probleem.

(i) Gegeven een gesloten diehoek ABC. Gevraagd punten P en Q in deze driehoek met maximale afstand.



Redenering. Stel van twee punten P en Q ligt P in het inwendige. Dan is $|PQ|$ zeker niet de maximale afstand, want voor een passend punt P_1 in een passende omgeving van P is $|P_1Q|$ groter. Liggen P en Q op de rand, maar niet beide in een hoekpunt, dan geldt een analoge redenering.
Conclusie: de grootste afstand krijgt men voor een zijde van de driehoek en dan uiteraard de grootste zijde.
Vraag: is dit betoog correct?



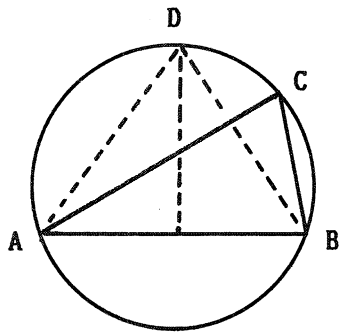
Voor de bovenstaande figuur stelt men hetzelfde probleem (i). Dan kan dezelfde redenering worden gehouden. Als het lijnstuk PQ niet het lijnstuk AB is, is er altijd een puntenpaar P_1, Q_1 met grotere afstand. De conclusie zou dan zijn: A, B is het paar met de grootste afstand, hetgeen absurd is.
We moeten dus concluderen dat ook het betoog in het eerste geval niet juist is. In het tweede geval is de verzameling niet begrensd. Men zou dus kunnen vragen of de redenering wel goed is voor begrensde figuren. Het antwoord is ontkennend, hetgeen blijkt door een driehoek te nemen waarvan de basis AB de langste is van de drie zijden, terwijl AB (inclusief A en B) *niet tot de driehoek wordt gerekend.* De verzameling van de afstanden van de puntenparen in de

driehoek is dan naar boven begrensd, maar het "bewijs" voldoet niet, want er is geen maximale afstand.

Wat in het betoog ontbreekt is het bewijs van de *existentie* van een puntenpaar P, Q als gevraagd.

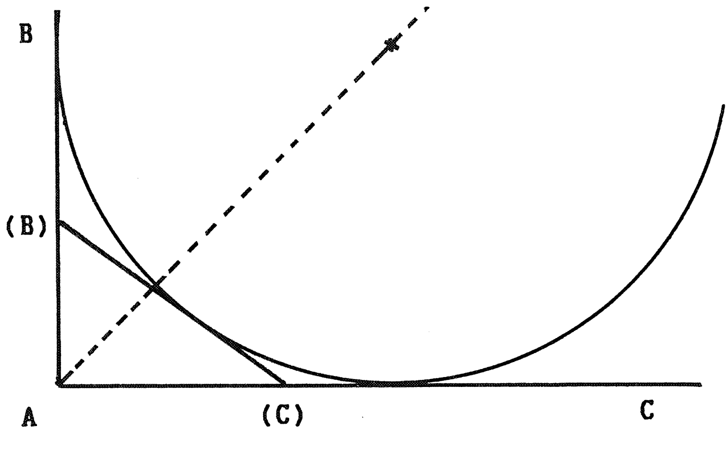
(ii) Dezelfde lacune zit in het "bewijs" van de volgende bewering.

Bewering: van alle ingeschreven driehoeken van een gegeven cirkel heeft de gelijkzijdige de grootste oppervlakte.



Redenering. Stel dat de driehoek ABC niet gelijkzijdig is, bijvoorbeeld $|AC| \neq |BC|$. Construeer dan op AB een gelijkbenige driehoek; deze heeft een grotere oppervlakte. Dus: de gelijkzijdige driehoek heeft de grootste oppervlakte.

(iii) Het volgende voorbeeld geeft aanleiding tot uitvoeriger beschouwingen. Het is een aanloop tot het isoperimetrische probleem.



Gegeven een rechte hoek BAC. Gevraagd wordt een driehoek ABC af te snijden met gegeven omtrek L en zo groot mogelijke oppervlakte S. Vooraf een opmerking. Men kan analytisch te werk gaan. Stellen we $|AB| = x$, $|AC| = y$, dan is

$$L = x + y + (x^2 + y^2)^{1/2}$$

$$S = \frac{1}{2}xy$$

en het probleem is S te maximaliseren bij gegeven L.
Een meetkundige, directe oplossing kan als volgt worden gegeven. Zij ABC een driehoek met omtrek L. Beschouw de aangeschreven cirkel aan de zijde BC. De straal hiervan is $L/2$ en die cirkel kan dus worden geconstrueerd. De zijde BC van de gevraagde driehoek moet daaraan raken. Bonnesen — aan wie ik dit voorbeeld ontleen — zegt dan: de meetkundige intuïtie zegt dan dat de maximale oppervlakte wordt bereikt voor de gelijkbenige driehoek.

Deze methode van concluderen roept vragen op. Wat is intuïtie? Is er een maximum of een minimum? De intuïtie berust kennelijk op overwegingen van symmetrie, op het hanteren van spiegelingen. Dit soort vage redeneringen treffen we wel meer aan in de meetkunde. Strikt genomen betreffen ze echter slechts de helft van het bewijs. Bij dit soort redeneringen staat de spiegelingsmeetkunde op de achtergrond.

We kunnen berekenen dat de maximale waarde van de oppervlakte gelijk is aan αL^2 met $\alpha = (3 - 2\sqrt{2})/4$.
Voor elke rechthoekige driehoek met omtrek L en oppervlakte S geldt dus

$$\alpha L^2 - S \geq 0.$$

Dit is een eenvoudig geval van de zogenaamde *isoperimetrische ongelijkheid*.
Deze ongelijkheid kan worden verscherpt. Zij r de straal van de ingeschreven cirkel van een rechthoekige driehoek met omtrek L. Volgens de elementaire meetkunde is $rL = 2S$, anders geschreven

$$rL - S = S.$$

Beschouw nu *alle* rechthoekige driehoeken die een vaste cirkel met straal r als ingeschreven cirkel hebben. Daarbij is er één met minimale oppervlakte (minimumprobleem). De oppervlakte daarvan is $(r^2)/(4\alpha)$, met α als boven. Derhalve geldt $rL - S \geq (r^2)/(4\alpha)$ of

$$\alpha L^2 - S \geq \alpha(L - \frac{r}{2\alpha})^2.$$

Ook dit resultaat is niet scherp. Bonnesen gebruikt voor een exact bewijs speciale convergentieprocédé's betreffende driehoeken en komt dan tot de ongelijkheid

$$\alpha L^2 - S \geq \frac{1}{16\alpha}(R - r)^2,$$

waarin R de straal is van een bepaalde in het betoog ingevoerde cirkel. Voor de gelijkbenige driehoek geldt $R = r$, zodat in dat geval het gelijkteken geldt.

4. HET ISOPERIMETRISCHE PROBLEEM.

Het eigenlijke isoperimetrische probleem heeft betrekking op kromlijnige figuren. Het probleem luidt als volgt:

> Gevraagd wordt onder alle enkelvoudig gesloten krommen in $\mathbf{R}^2$ met gelijke lengte die kromme te bepalen waarvan de daardoor ingesloten verzameling de grootste oppervlakte heeft.

Bij de formulering van de probleemstelling doet zich uiteraard de vraag voor naar een definitie van de begrippen lengte en oppervlakte. We gaan daaraan voorbij — het is niet essentieel in deze beschouwingen — en veronderstellen dat de kromme aan passende voorwaarden voldoet.

Naast dit probleem kan men vragen om onder alle krommen waarvan de ingesloten verzameling dezelfde oppervlakte heeft, de kromme te bepalen met de kleinste omtrek. Dit is het duale van het isoperimetrische probleem. Met een passend gekozen gelijkvormigheidstransformatie is eenvoudig te bewijzen dat beide equivalent zijn. Voor beide problemen wordt de oplossing gegeven door de cirkel.

Het isoperimetrische probleem gaat terug tot de klassieke oudheid (zie [46]). Steiner gaf een ingenieus meetkundig bewijs, dat later een fout bleek te bevatten of althans, zo men wil, niet volledig bleek te zijn. Deze fout is het beginpunt geweest van vele ontwikkelingen.

Het bewijs van Steiner loopt langs de volgende grote lijnen. Eerst wordt aangetoond dat het voldoende is zich te beperken tot *convexe* gesloten figuren. Daartoe gaat men over op het convexe omhulsel — de doorsnede van alle convexe verzamelingen die de kromme, en dus ook de daardoor ingesloten verzameling, bevatten — waardoor de omtrek kleiner en de oppervlakte groter wordt, en past dan een gelijkvormigheidstransformatie toe. De leidende gedachte in het bewijs van Steiner is: maak bij elke kromme die geen cirkel is een nieuwe kromme met gelijke lengte en grotere ingesloten oppervlakte. Daartoe verzon Steiner een ingenieuze methode. Door een soort mechanisch (maar wel intern mathematisch gedefinieerd) procédé, het "Viergelenkverfahren" (zie ook [28]) toe te passen op een kromme die geen cirkel is, kon hij zo'n nieuwe kromme construeren. Steiners conclusie luidde vervolgens: de oplossing is dus een cirkel.
Dit "bewijs" vertoont dezelfde leemte als de hiervoor besproken elementaire voorbeelden. Wat ontbreekt is het bewijs van de *existentie* van een oplossing. Steiner bewees in feite slechts: *als* er een oplossing is, dan is dat de cirkel. In zijn conclusie maakte Steiner dus een denkfout tegen de regels van de logica.
Er is echter ook een mathematische achtergrond. Zij $V \subset \mathbf{R}$ de verzameling van de oppervlakten S van de door gesloten krommen met lengte L omsloten

verzamelingen. Dan is V naar boven begrensd: er geldt bijvoorbeeld $S < L^2$, omdat de afstand tussen twee punten uit de omsloten verzameling niet groter dan $L/2$ kan zijn, en de omsloten verzameling ligt dus in een cirkel met straal $L/2$. De verzameling V heeft daarom een supremum en er moet worden bewezen dat dit supremum een maximum is, dus dat het supremum van V in V zit. Hier zit de lacune: het niet in acht nemen door Steiner van het onderscheid tussen de begrippen supremum en maximum. Deze zelfde fout is te bespeuren in meer ontwikkelingen in de wiskunde, in de analyse en ook in de algebra. Pogingen om die fouten te elimineren zijn bronnen geweest voor nieuwe theorieën. Wij zullen er later met korte aanduidingen op terugkomen.

Na Steiner heeft men zich intensief met dit existentieprobleem bezig gehouden. Er is een uitgebreide literatuur en een correcte behandeling is bepaald niet eenvoudig. We zullen er slechts enkele opmerkingen over maken en voor het overige verwijzen naar de genoemde boeken.

Wilhelm J.E. Blaschke (1885-1962) bestudeerde het probleem door eerst met elementaire middelen de stelling te bewijzen voor veelhoeken — waarbij de oplossing wordt gevonden in de klasse van de regelmatige veelhoeken — en daarna gebruik te maken van approximaties door veelhoeken. Hij generaliseerde in dit verband de klassieke stelling van Bolzano-Weierstrass (existentie van convergente deelrijen van een begrensde rij; lokale compactheid) voor rijen van convexe verzamelingen.

Constantin Carathéodory (1873-1950) paste het "mechanische" procédé van Steiner oneindig vaak toe op een gesloten kromme, en bewees dat dit proces naar een cirkel convergeert. Ook Eduard Study (1862-1930) ging op soortgelijke wijze te werk.

De onderzoekingen hebben geleid tot de isoperimetrische ongelijkheid waarvan we reeds een variant hebben gezien:

Voor elke enkelvoudig gesloten kromme die aan passende condities voldoet geldt tussen de lengte L en de oppervlakte S van de ingesloten verzameling de betrekking

$$L^2 - 4\pi S \geq 0.$$

Slechts voor de cirkel geldt het gelijkteken.

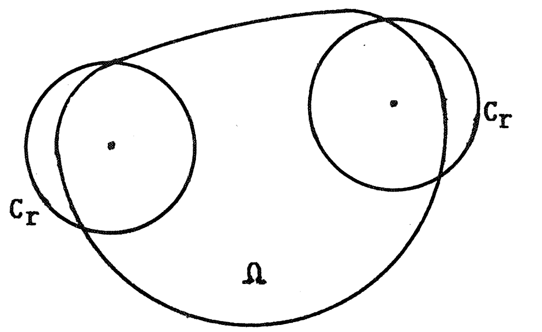
Vermeldenswaard is dat Adolf Hurwitz (1859-1919) een strikt analytisch bewijs gaf van deze ongelijkheid voor het geval van gladde krommen. Hij gebruikte daarbij de zogenaamde volledigheidsbetrekking uit de theorie van de Fourierreeksen: $\sum(c_n)^2 = \int f^2 dx$, waarin de c_n de Fouriercoëfficiënten van f zijn (zie [11], p. 43).

De uitdrukking $L^2 - 4\pi S$ staat bekend als het *defecit* van de kromme; er kan een meetkundige betekenis aan worden toegekend. Nadere studies voeren tot een verscherping van de isoperimetrische ongelijkheid. In deze studies spelen de begrippen ingeschreven en omgeschreven cirkel van een convexe verzameling een rol. We komen op die begrippen terug, maar vermelden eerst de verscherpte ongelijkheid. Deze luidt

$$L^2 - 4\pi S \geq \pi^2 (R - r)^2,$$

waarin R de straal is van de omgeschreven cirkel en r die van de ingeschreven cirkel. Het gelijkteken geldt slechts als $R = r$, dus voor de cirkel. Vergelijk hiermee de ongelijkheden in paragraaf 3 voor een driehoek.

Waar komt de uitdrukking $L^2 - 4\pi S$ vandaan? Deze blijkt de discriminant te zijn van een kwadratische vorm die voortkomt uit operaties op convexe figuren.



Zij Ω een convexe verzameling en Ω_1 de vereniging van de cirkels C_r met straal r en middelpunt in Ω. Noem L respectievelijk S de omtrek en de oppervlakte behorend bij Ω en evenzo L_1 en S_1 die behorend bij Ω_1. Dan geldt

$$L_1 = L + 2\pi r,$$

$$S_1 = S + rL + \pi r^2.$$

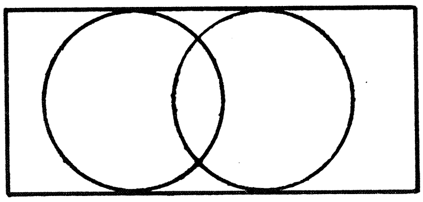
Men bewijst deze betrekkingen eerst voor polygonen en daarna door limietovergang voor algemene convexe figuren. Het rechterlid van de tweede betrekking geeft aanleiding tot een kwadratische vorm

$$\pi x^2 + xL + S$$

waarvan $\Delta = L^2 - 4\pi S$ de discriminant is. Meetkundige beschouwingen waarin de in- en omgeschreven cirkel een rol spelen leren dat $\Delta \geq 0$ is, en voeren uiteindelijk tot de verscherpte isoperimetrische ongelijkheid.

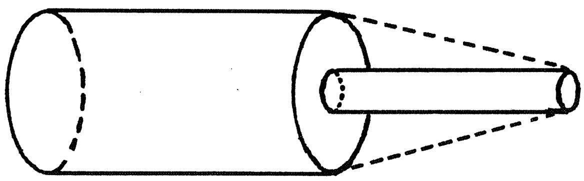
Ingeschreven en omgeschreven cirkels behoren traditioneel tot de planimetrie, de euclidische meetkunde in $\mathbf{R}^2$. Zoals zovele onderwerpen uit de klassieke wiskunde laat ook dit onderwerp zich in een bredere context plaatsen, namelijk in de context van de meetkunde van convexe figuren. We maken nog enkele

opmerkingen over in- en omgeschreven cirkels. Deze opmerkingen zijn ten dele ook van didaktische aard.
Zij Ω een convexe figuur. Onder de omgeschreven cirkel van Ω verstaan we de kleinste cirkel waarin Ω is bevat. Een ingeschreven cirkel is een grootste cirkel die bevat is in Ω. Waar hier sprake is van "kleinste cirkel" en "grootste cirkel", wordt "cirkel met kleinste straal" respectievelijk "cirkel met grootste straal" bedoeld. Men kan bewijzen dat de omgeschreven cirkel bestaat en eenduidig bepaald is. Van de ingeschreven cirkel is de straal eveneens eenduidig bepaald, maar de ligging daarentegen niet (zie de tekening voor de ingeschreven cirkels in een rechthoek).



De bovenstaande definities van in- en omgeschreven cirkel wijken af van de traditionele definities voor driehoeken in de planimetrie, waar "raken aan de zijden" respectievelijk "gaan door de hoekpunten" het gestelde criterium is. Wegens de grotere algemeenheid verdienen de hier gegeven definities de voorkeur. Dan moet wel worden aangetoond dat van een driehoek de ingeschreven cirkel aan de zijden raakt en de omgeschreven cirkel door de hoekpunten gaat.

Enige informatie over het analogon van het isoperimetrische probleem in $\mathbf{R}^3$ mag niet achterwege blijven. Dit is het zogenaamde *isepiphane probleem.* Hier wordt gevraagd om onder alle lichamen met een gegeven oppervlakte het lichaam met de grootste inhoud te bepalen. Het gaat dus om karakteriseringen van de bol. Dit probleem in $\mathbf{R}^3$ is aanzienlijker moeilijker gebleken dan het probleem in $\mathbf{R}^2$; er doen zich complicaties voor.
In $\mathbf{R}^2$ konden we ons beperken tot convexe figuren, zonder de algemeenheid te schaden. Dat gebeurde door overgang op het convexe omhulsel, een operatie waarbij de lengte niet groter wordt. In $\mathbf{R}^3$ moeten we daar voorzichtiger mee zijn. Er bestaan namelijk voorbeelden waarbij de oppervlakte groter wordt bij overgang naar het convexe omhulsel. We ontlenen het volgende voorbeeld aan Bonnesen.

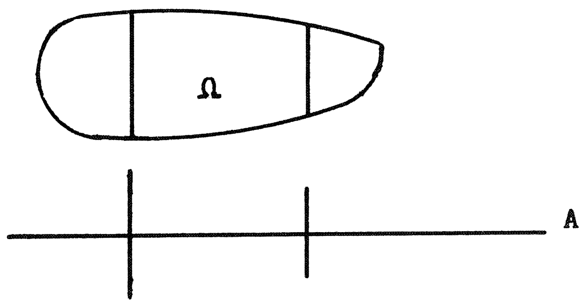


Het niet-convexe lichaam is de vereniging van twee cylinders met straal R, respectievelijk r, zodat $R > r$. Een eenvoudige berekening toont aan dat het convexe omhulsel voor voldoend kleine r een grotere oppervlakte heeft dan het lichaam zelf.

In $\mathbf{R}^3$ is het daarom in eerste instantie noodzakelijk om het isepiphane probleem te beperken tot convexe lichamen.
Het eerder genoemde "mechanische" procédé van Steiner in $\mathbf{R}^2$ werkt niet in $\mathbf{R}^3$. Voor $\mathbf{R}^3$ heeft Steiner het later naar hem genoemde *symmetriseringsprocédé* bedacht. Daarin spelen stellingen over symmetrie een rol. Bijvoorbeeld geldt de volgende stelling.

> *Zij C een begrensd convex lichaam met de eigenschap dat bij elk vlak een daarmee evenwijdig symmetrievlak van C bestaat. Dan is C een bol.*

Het symmetriseringsprocédé werkt nu als volgt. Zij Ω een convex lichaam en zij A een vlak, niet evenwijdig aan een symmetrievlak van Ω. We veronderstellen dus dat Ω geen bol is.



We gaan nu symmetriseren ten opzichte van A. Beschouw alle lijnen loodrecht op A. Als zo'n lijn Ω snijdt, verschuif het snijsegment dan in de lijn zodanig dat het midden ervan op A komt te liggen (zie de tekening). Aldus ontstaat uit Ω een nieuw lichaam Ω_1 waarvan A een symmetrievlak is. Men kan bewijzen dat Ω_1 weer een begrensd convex lichaam is. Volgens de stelling van Bonaventura Cavalieri (1598-1647) heeft Ω_1 dezelfde inhoud als Ω. Steiner geeft aan dat de oppervlakte van Ω_1 kleiner is dan die van Ω. Hier zitten echter complicaties waar we niet op ingaan. De conclusie is duidelijk: een convex lichaam dat geen bol is kan worden vervangen door een convex lichaam met gelijke inhoud en kleinere oppervlakte. Steiner gaat dan over op het duale probleem (het isepiphane probleem) en concludeert dat de oplossing een bol is. Ook hier ontbreekt echter, net als bij het isoperimetrische probleem, het bewijs van de existentie van een convex lichaam met minimale inhoud bij gegeven oppervlakte.

Later zijn correcte bewijzen gegeven, onder andere door toepassing van oneindig veel symmetrizeringen. Het onderzoek heeft zich ook uitgestrekt tot ongelijkheden analoog aan de iosoperimetrische ongelijkheid. Aldus kan een op het eerste gezicht eenvoudige uitspraak een aanleiding zijn voor verstrekkende onderzoekingen.

5. WIJDER PERSPECTIEF.

De fouten in de incorrecte bewijzen die we in de vorige paragraaf geschetst hebben, werden veroorzaakt door het niet voldoende inachtnemen van het onderscheid tussen de begrippen supremum en maximum. Dit aspect kan in een wijder perspectief worden geplaatst. Het is merkwaardig dat dezelfde foutieve gedachtengang kan worden aangewezen in fundamentele ontwikkelingen die in andere gebieden van de wiskunde in nagenoeg dezelfde periode plaatsvonden. Dit is te meer merkwaardig omdat sommige mathematici werk van anderen op dit punt critizeerden, terwijl zij in eigen werk op een ander gebied dezelfde fout begingen. Blijkbaar was het onderscheid tussen de begrippen supremum en maximum in die periode nog moeilijk. Zelfs heden ten dage kan men nog regelmatig in boeken en artikelen bewijzen tegenkomen waarin dezelfde fout wordt gemaakt. We zijn dan geneigd om aan te nemen dat de schrijver het evident heeft gevonden (meestal voldoet inderdaad een simpel compactheidsargument) dat het supremum wordt aangenomen binnen de beschouwde verzameling. Maar is dat wel zo, of is het toch gewoon slordigheid?

In [33] worden de boven bedoelde ontwikkelingen uitvoerig uiteengezet, en we volstaan er daarom mee ze hier slechts kort aan te duiden.
In paragraaf 2 noemden we reeds de bewijzen die Gauss gaf van de hoofdstelling van de algebra. Hij had kritiek op het eerder gegeven bewijs van D'Alembert, onder andere omdat deze de existentie van van een zeker minimum zonder bewijs had aangenomen. In zijn eigen werk op een heel ander gebied beging Gauss zelf echter ook deze fout. In zijn onderzoekingen over de potentiaaltheorie stuitte Gauss op het probleem om een zekere integraal te minimaliseren waarvan de integrand afhangt van een funktie φ uit een bepaalde klasse van funkties. Uit het feit dat die integraal voor alle φ uit die klasse een positief infimum heeft, besloot hij dat de integraal voor een zekere φ_0 in die klasse een minimum waarde aanneemt. Fysische overwegingen zullen daarbij zeker van invloed zijn geweest.

De geschiedenis heeft zich herhaald bij Dirichlet, die eveneens belangrijk werk in de potentiaaltheorie heeft verricht. Voor een open verzameling Ω in $\mathbf{R}^3$ en een familie van funkties u gedefinieerd op Ω, beschouwde hij voor alle u de integraal

$$I = \int_\Omega ((\frac{\partial u}{\partial x})^2 + (\frac{\partial u}{\partial y})^2 + (\frac{\partial u}{\partial z})^2)\,dt.$$

Uit het feit dat altijd $I \geq 0$ geldt, concludeerde Dirichlet dat I een minimum waarde aanneemt voor een zekere funktie u_0 uit de familie van funkties. Ook Dirichlet verwarde hier de existentie van een infimum met de existentie van een minimum. Naar later bleek, is de uitspraak van het bestaan van een minimum in het algemeen (behoudens in triviale gevallen) onjuist. Het is dan wel merkwaardig dat Dirichlet het bewijs van Steiner voor het isoperimetrische probleem bekritiseerde op het niet onderscheiden van supremum en maximum.

De historie vervolgend, kan men Riemann noemen. Bij diens fundering van de theorie van de complex analytische funkties beschouwde hij een integraal analoog aan die van Dirichlet, maar dan in twee dimensies. In het minimalizeringsprocédé maakte ook Riemann dezelfde fout als Dirichlet. Dit was een ernstige leemte, want het door Riemann verlangde resultaat was fundamenteel voor een verdere ontwikkeling van de complexe funktietheorie.

Het was Weierstrass die aan een concreet voorbeeld van een familie van integralen het onderscheid tussen de begrippen supremum en maximum expliciet aan het licht bracht. Overigens was deze kritiek van Weierstrass van een geheel andere orde dan diens wantrouwen in de meetkundige methoden van Riemann (zie paragraaf 2). De onjuiste — of zo men wil onvolledige — bewijzen van Dirichlet en Riemann betroffen zuiver mathematische kwesties, ongeacht verschillen van inzicht in de gebruikte methoden.

Wat betreft de consequenties van de in deze paragraaf genoemde fouten zij nog opgemerkt dat de funktietheorie deze moeilijkheden langs haar eigen weg heeft geëlimineerd. Voor de potentiaaltheorie echter heeft de gesignaleerde onjuistheid grote gevolgen gehad: pogingen om de fout te herstellen hebben geleid tot het inzicht dat het "probleem van Dirichlet" niet altijd een oplossing heeft. De gehele moderne potentiaaltheorie is historisch verbonden met het onderzoek naar de consequenties hiervan. Voor meer bijzonderheden verwijzen we naar [33].

Tenslotte nog een vraag. Als wij constateren dat Steiner, Dirichlet, en Riemann analoge fouten maakten zonder dit van zichzelf te beseffen, hoe staat het dan met ons? Zijn wij zo zeker? Hoe zal men over 100 jaren onze verrichtingen beoordelen? Hebben wij de echte, absolute, waarheid? En verder: lettend op de historische ontwikkeling, die ondanks vallen en verkeerde uitgangspunten toch is voortgegaan, zou men wel eens tot het standpunt kunnen komen dat met het stellen van strengheidseisen enige voorzichtigheid moet worden betracht. Uit aanvankelijke fouten zijn vaak goede zaken voortgekomen.

6. MEETKUNDE VAN CONVEXE LICHAMEN.

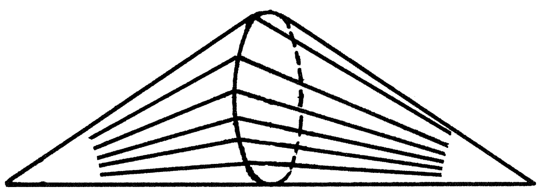
Bij de onderzoekingen over het isoperimetrische en het isepiphane probleem sluiten onderzoekingen aan over de meetkunde van convexe lichamen. Verschillende belangrijke begrippen uit de theorie van de convexe verzamelingen gaan terug tot Hermann Minkowski (1864-1909) (zie [29]). Enerzijds hebben zij betrekking op numerieke toevoegingen (zoals inhoud en oppervlakte). Anderzijds gaat het om onderzoekingen van puur meetkundige aard, bijvoorbeeld over

meetkundige objecten die in verbinding kunnen worden gebracht met convexe lichamen (zoals de in- en omgeschreven cirkel respectievelijk bol). Er zijn ook meetkundige onderzoekingen die meer intrinsiek van karakter zijn. We noemen in het bijzonder het begrip *extremaalpunt.* We zullen niet in algemene zin ingaan op deze onderzoekingen, omdat zij niet strikt het fenomeen "bewijzen" betreffen. Voor het begrip "extremaalpunt" maken we echter een uitzondering wegens de daarbij optredende existentievraag, waarbij methodologische aspecten een rol spelen.
Eerst geven we een paar definities. We formuleren deze definities in $\mathbf{R}^n$, maar ze zijn zonder enige verandering ook geldig voor oneindig-dimensionale ruimten over $\mathbf{R}$.

> Een deelverzameling A van $\mathbf{R}^n$ heet *convex* indien voor alle punten x en y in A en voor alle reële getallen λ met $0 \leq \lambda \leq 1$ geldt dat ook $\lambda x + (1 - \lambda)y$ een punt van A is. Korter gezegd: als van een lijnstuk de eindpunten in A liggen, dan ligt het lijnstuk geheel in A.
>
> Zij A een convexe deelverzameling van $\mathbf{R}^n$. Een punt x van A heet *extremaalpunt* van A indien er geen open lijnstuk (zonder eindpunten) in A is dat x bevat. Een andere definitie is: $x \in A$ is een extremaalpunt van A indien $A - \{x\}$ convex is.

We geven enkele voorbeelden.

> (i) Een driehoek zonder rand heeft geen extremaalpunten; de extremaalpunten van een gesloten driehoek zijn precies de hoekpunten.
>
> (ii) Van een gesloten cirkelschijf zijn alle punten van de cirkelomtrek extremaalpunten.
>
> (iii)



> Van bovenstaand lichaam zijn R, Q, en alle punten van de cirkel behalve P extremaalpunten. Dit betekent dat van een compacte convexe verzameling in $\mathbf{R}^3$ de verzameling van de extremaalpunten niet gesloten hoeft te zijn. In $\mathbf{R}^2$ kan zich dit niet voordoen; daar

geldt dat van een compacte convexe verzameling de verzameling van de extremaalpunten gesloten is.

(iv) Van de bol in $\mathbf{R}^n$ bepaald door $\sum_{i=1}^n x_i^2 \leq 1$ zijn de punten waarvoor $\sum x_i^2 = 1$ de extremaalpunten. Voor $n = 2$ en $n = 3$ is dit een aanschouwelijk evidente uitspraak. Voor $n > 3$ is dat stellig niet meer het geval en moet een analytisch bewijs worden geleverd. Trouwens ook voor $n = 2$ en $n = 3$ moet men dit strikt genomen verlangen. Maar doet men dat ooit, en heeft men dan toch geen scrupules? Wat is meetkundige "aanschouwelijkheid" en "evidentie"?

(v) In de Hilbertruimte van de rijen $(x_1, x_2, \ldots)$ met $\sum(x_i)^2 < \infty$ is de deelverzameling H van de rijen met $\sum(2^i x_i)^2 \leq 1$ convex, en de verzameling van de extremaalpunten van H ligt overal dicht in H.

(vi) Een oneindig lange cylinder in $\mathbf{R}^3$ heeft geen extremaalpunten.

Er doet zich blijkbaar een existentieprobleem voor.

Men kan bewijzen dat elke niet-lege, convexe, compacte verzameling A in $\mathbf{R}^n$ extremaalpunten heeft (existentie van extremaalpunten), en dat A de afsluiting is van het convexe omhulsel van de verzameling van zijn extremaalpunten (de stelling van Krein-Milman). Deze stellingen gelden ook voor oneindig-dimensionale ruimten over $\mathbf{R}$ die lokaal convex en separabel zijn. Juist in oneindig-dimensionale gevallen vindt de stelling van Krein-Milman toepassing in de analyse. We noemen een integraal-representatie van een zekere klasse van funkties. Het is curieus dat een bewijs daarvan langs de weg van de stelling van Krein-Milman licht doet schijnen op een, om zo te zeggen, "extern" aspect van deze integraal-representatie. Dit bewijs demonstreert het verband met een begrip van externe aard, namelijk het begrip zwaartepunt, zij het dat het daarbij misschien meer gaat om een terminologisch dan om een extern methodologisch aspect (vergelijk paragraaf 2 over externe factoren). Het zou buiten het kader vallen om op het bewijs van de genoemde toepassing in te gaan. We bepalen ons tot een opmerking over de algemene stelling van Krein-Milman, met nadruk op de bewijsvoering.
De bewijzen van de existentie van extremaalpunten en van de stelling van Krein-Milman (zie [13], [30], [44]) zijn niet gecompliceerd, maar ook niet elementair. Er wordt gebruik gemaakt van het lemma van Zorn. Dit betekent dat de bewijzen niet-constructief zijn. Voor het bewijs van de existentie van extremaalpunten in de eindig dimensionale $\mathbf{R}^n$ kan men gebruik maken van volledige inductie naar de dimensie (in $\mathbf{R}^1$ is de existentie triviaal), maar met name in $\mathbf{R}^3$ zou men graag een expliciet constructief bewijs willen.
De vraag naar een constructief bewijs is niet ingegeven door eisen van strengheid: de resultaten zijn naar onze normen streng bewezen. Maar naast strengheid spelen bij de wiskunde zoals wij die opbouwen nog andere factoren een rol. Men

spreekt in de wiskunde van mooie bewijzen, van elegante bewijzen, van duidelijke bewijzen, etc.. Ook al is een resultaat reeds streng bewezen, de wiskundige streeft naar verbeteringen en naar methoden die beter passen bij de aard van het probleem of van de theorie. Naast normen van strengheid is dit ook een aspect van de ontwikkeling van de wiskunde (zie [49]. Overigens moet gezegd worden dat bewijzen met behulp van het lemma van Zorn of het keuze-axioma in het algemeen veel eleganter zijn dan bewijzen die daar geen gebruik van maken.

De veranderingen in de mathematische cultuur manifesteren zich in de introductie en de hantering van mathematische begrippen en methoden. De plaats van en de ontwikkelingen rond het begrip "existentie" zijn daarvan een illustratie. In de klassieke periode trad existentie als zodanig, expliciet geformuleerd en in zijn betekenis ter discussie gesteld, nauwelijks op. Existentie, in verband met het oplossen van problemen, had betrekking op expliciete oplossingen, oplossingen in concrete zin. Een oplossing was een mathematisch object dat zich — zeer schetsmatig gezegd en misschien niet steeds toepasbaar — leende tot verificatie van de verlangde eigenschappen, zo te zeggen tot controle. Aanvankelijk verzette de wiskundige gemeenschap zich tegen zuiver existentiële bewijzen. Toen Paul Gordan (1837-1912) Hilberts niet-effectieve bewijs van het "basis-probleem" in de invariantentheorie zag, moet hij hebben uitgeroepen: Dit is geen wiskunde, het is theologie! (zie [50], p. 429).
Het begrip "existentie" is thans een primair en zeer op de voorgrond tredend begrip geworden, zeker in de analyse. Het vindt zijn uitdrukking in formuleringen als "Er bestaat ..." en "Voor alle ... is er ...". Het begrip heeft een andere klank gekregen, het gaat om zogenoemde pure existentie, een begrip met een ander filosofisch karakter, niet gekoppeld aan constructie. Het begrip als zodanig is, naar het lijkt, zo vanzelfsprekend en zo probleemloos geworden dat het nauwelijks meer wordt ondervonden als een evolutie in de mathematische cultuur. Is er nog wel — behoudens uiteraard in filosofische kringen — een bewust inzicht in de principiële, voor de wiskunde essentiële problematiek van de existentie? Hoe ondervinden onze studenten dit? Het gevaar bestaat dat zij het begrip existentie probleemloos aanvaarden en de resultaten dienaangaande op zich als vanzelfsprekend beschouwen, omdat er nu eenmaal bewijzen voor worden geleverd met behulp van algemeen aanvaarde bewijsmethodieken. Als de achtergronden verloren gaan, lijkt dat een verarming. Het onderwerp existentie verdient zeker ook aandacht vanuit didaktisch oogpunt (vergelijk verder de bijdrage van Van Dalen).

7. NABESCHOUWING.

Het voorgaande overziende, zal men opmerken dat de verschillende onderwerpen besproken zijn met inachtneming van een zekere systematiek. We hebben getracht een struktuur aan te brengen in de volgorde. Deze volgorde sluit — voor zover mogelijk — aan bij de ontwikkeling van de wiskunde in een eeuwenlang proces. In dat proces was er een voortdurend stijgend niveau en een groeiende samenhang tussen de diverse disciplines. Als leidraad hebben we de wisselende en groeiende bewijsmethodiek en bewijsproblematiek gekozen. Bewijsmethodiek is nauw verbonden met de materie waarop die methodiek wordt toepast. Uit het voorgaande komt dit verband ook naar voren. De methode van Descartes — die meetkunde in verbinding bracht met algebra — voerde tot nieuwe gebieden. Evenzo voerde het gebruik van infinitesimalen door Leibniz tot de infinitesimaalrekening en verder. In een recentere periode kan worden gewezen op het werk van Cantor dat leidde tot de theorie van oneindige verzamelingen, waarin later het keuze-axioma een fundamentele plaats kon innemen.

De vraag dringt zich op hoe en met welke middelen de wiskunde in een nog steeds voortdurend proces is en wordt opgebouwd. Dit probleem overstijgt het kader van deze bijdrage.

In een poging om te komen tot een synthese van het hiervoor behandelde kan men zeggen dat voortgang in de wiskunde ontstaat uit een samenspel van twee nauw verweven facetten:

1. Voortgang in onderwerpen, de schepping en bewerking van nieuwe concepten en ideeën.
2. Voortgang in bewijsmiddelen en bewijzen waarmee nieuwe concepten worden uitgewerkt in theorieën.

Deze beide facetten hebben, in nauwe relatie tot elkaar, een evolutie ondergaan. In beide facetten kan een aspect worden aangewezen waaraan de essentiële grensverleggende voortgang is toe te schrijven. Dat aspect is de *discontinuïteit in het denkproces*. In de continue stroom van de voortgang zijn ontwikkelingen aan te wijzen van een discontinu type. Juist die discontinuïteiten hebben het niveau verhoogd, hebben althans hogere niveaux toegevoegd. Descartes, Leibniz, Cantor en anderen markeerden met hun volstrekt nieuwe werk essentiële overgangen naar nieuwe fasen. Voor een nadere uiteenzetting van het discontinuïteitsidee verwijzen we naar [34] en [35]. Ook in de ontwikkelingsgang van andere wetenschappen kan het discontinuïteitsidee worden opgemerkt. We denken dan bijvoorbeeld aan het wijsgerige werk van Descartes, aan Copernicus en zijn inzichten over het planetenstelsel, aan Darwin en de evolutietheorie, aan Lorentz en Einstein en de relativiteitstheorie, aan Bohr, aan Planck, ... Wellicht kan men zelfs denken aan inzichten in de taalwetenschap (Chomski) (zie [51]). Kan men stellen dat het discontinuïteitsidee essentieel is voor de creatie en de intrede van werkelijk nieuwe concepten, inzichten en gebieden? Het is hier uiteraard niet de plaats om dit probleem te analyzeren en het ligt bovendien buiten de competentie van de schrijver.

8. LITERATUUR

[1] J.M.Aarts: *Het vierkleurenprobleem.* In P.W.H.Lemmens (ed.): *Discrete wiskunde: tellen, grafen, spelen en codes.* CWI Syllabus 11. Centrum voor Wiskunde en Informatica, Amsterdam, 1986.

[2] K.Appel, W.Haken: *The solution of the Four-Color-Map Problem.* Scientific American, oct. 1977, 108-121.

[3] W.Blaschke: *Kreis und Kugel.* Leipzig 1916.

[4] T.Bonnesen: *Les problèmes des isopérimètres et des isépiphanes.* Paris 1929.

[5] T.Bonnesen und W.Fenchel: *Theorie der konvexen Körper.* Berlin 1934.

[6] E.Borel: *Leçons sur les séries divergentes.* Paris 1901.

[7] L.E.J. Brouwer: *Zur Analysis Situs.* Math. Annalen 68 (1910), 422-434.

[8] L.E.J. Brouwer: *Beweis der Invarianz der Dimensionenzahl.* Math. Annalen 70 (1911), 161-165.

Dit artikel is ook opgenomen in E.M.J.Bertin et al.: *Two Decades of Mathematics in The Netherlands.* Math. Centre, Amsterdam 1978.

[9] L.E.J. Brouwer: *Collected Works*, Vol 2. (Ed. H. Freudenthal). Amsterdam etc., 1976.

[10] G.Cantor: *Ein Beitrag zur Mannigfaltigkeitlehre.* J. f. d. reine und angewandte Math. 84 (1878), 242-258.

[11] R.Courant, D.Hilbert: *Methoden der Mathematischen Physik I.* Berlin 1968.

[12] R.Dedekind: *Stetigkeit und Irrationale Zahlen*, 7e Auflage. Braunschweig 1969.

[13] H.G.Eggleston: *Convexity.* Cambridge 1963.

[14] H. Freudenthal: *Wiskunde in wetenschap en dagelijks leven.* De Haan / Meulenhoff, 1967.

[15] H. Freudenthal: *Die Topologie in historischen Durchblicken.* In D.Laugwitz, *Überblicke Mathematik* (1971), Band 4. Zürich 1972

[16] J.C.H.Gerretsen: *Inleiding tot een topologische behandeling van de meetkunde van het aantal.* Groningen 1939.

[17] J.C.H.Gerretsen: *Der Kalkül der abzählenden Geometrie.* Nieuw Archief voor Wiskunde (3), XXVI (1978), 142-160.

[18] D. Hilbert: *Ueber die stetige Abbildung einer Linie auf ein Flächenstück.* Math. Annalen 38 (1890), 459-460.

[19] D.Hilbert: *Gesammelte Abhandlungen*, Band 3, pp.290-329. Berlin etc., 1935.

[20] J.G. Hocking, G.S. Young: *Topology.* Reading etc., 1961.

[21] K.H.Hofmann and J.D.Lawson: *On Sophus Lie's Fundamental Theorems I.* Proc. Kon. Ned. Akad. v. Wetensch. Serie A, Vol. 96, no. 4 = Indag. Math. 45, fasc. 4 (1983), 453-454.

[22] Ramesh Kapadia: *Bring back Geometry.* The Math. Intelligencer Vol. 7, nr 2 (1985).

[23] H.J.Keisler: *Elementary Calculus.* University of Wisconsin 1976.
H.J.Keisler: *Foundations of Infinitesimal Calculus.* Idem.

[24] St.L.Kleinman: *Problem 15. Rigorous Foundation of Schubert's enumerative Calculus.* In: *Mathematical developments arising from Hilbert's Problems.* Proc. of Symposia in pure mathematics. Vol XXVII, Part 2. Am. Math. Soc. 1976

[25] K.Knopp: *Theory of Functions*, part I. New York 1945.

[26] R.Kooistra: *Gauss en de hoofdstelling van de algebra.* Nieuw Tijdschrift voor Wiskunde, 64 (1977), 173-175.

[27] W.A.J.Luxemburg: *Non-standard Analysis.* Pasadena 1962.

[28] H.Meschkowski und I.Ahrens: *Theorie der Punktmengen.* Zürich 1974.

[29] H.Minkowski: *Geometrie der Zahlen.* Leipzig 1910.

[30] A.F.Monna: *Zwaartepunten en convexe verzamelingen.* Euclides 43 (1968), 305-312.

[31] A.F.Monna: *The Concept of Function in the 19th and 20th Centuries, in Particular with Respect to the Discussions between Baire, Borel and Lebesgue.* Archive for History of Exact Sciences, Vol. 9, no. 1, 57-84 (1972).

[32] A.F.Monna: *Functional Analysis in historical perspective.* Utrecht/New York 1973.

[33] A.F.Monna: *Dirichlet's principle, a mathematical comedy of errors and its influence on analysis.* Utrecht 1975.

[34] A.F.Monna: *Where does the development of mathematics lead to?* Nieuw Archief voor wiskunde (4), 1 (1983), 33-56.

[35] A.F.Monna: *The way of mathematics and mathematicians; a historical-philosophical study.* Communications of the Mathematical Institute Rijks Universiteit, 17, Utrecht 1984.

[36] A.F.Monna: *Methods, concepts and ideas in mathematics: aspects of an evolution.* CWI Tract 23, Amsterdam 1986.

[37] E. Netto: *Beitrag zur Mannigfaltigkeitslehre.* J. f. d. reine und angewandte Math. 86 (1879), 263-268.

[38] G. Peano: *Sur une courbe, qui remplit toute une aire plane.* Math. Annalen 36 (1890), 157-160.

[39] A.Robinson: *Non-standard Analysis.* Amsterdam 1966.

[40] C.Schmieden, D.Laugwitz: *Eine Erweiterung der Infinitesimalrechnung.* Math. Zeitschrift 69 (1958), 1-39.

[41] F.Severi: *Grundlagen der abzählenden Geometrie.* Hannover 1948.

[42] J.Steiner: *Gesammelte Werke II* (Hrsg. K. Weierstrass). Berlin 1881.

[43] D.J.Struik: *Geschiedenis van de wiskunde.* Utrecht 1965.

[44] F.A.Valentine: *Convex sets.* New York 1964.

[45] Hk. de Vries: *Leerboek der Integraal en Differentiaalrekening, en van de Theorie der Differentiaalvergelijkingen.* Groningen, 1920.

[46] B.L. van der Waerden: *Science Awakening.* Groningen 1961.

[47] Joh.H.Wansink: *Didactische oriëntatie voor wiskundeleraren.* 3 delen, Groningen 1967-1971.

[48] R.L. Wilder: *The Origin and Growth of Mathematical Concepts.* Bulletin American Math. Soc. 59 (1953), 423-448.

[49] R.L.Wilder: *Mathematics as a Cultural System.* Oxford etc. 1981.

[50] E.T.Bell: *The Development of Mathematics.* New York 1940.

[51] J.Kaldewaij: *Structuralisme en transformationeel generatieve grammatica. Continuïteiten en discontinuïteiten in de twintigste eeuwse taalkunde.* Dissertatie, Utrecht 1986.

HOOFDSTUK II

BEWIJZEN, WAAROM EN HOE.

D. van Dalen

Was beweisbar ist , soll in der Wissenschaft nicht ohne Beweis geglaubt werden.

R. Dedekind

1. WAAROM.

Niet zo heel lang geleden werd een collega na een van zijn analysecolleges door een eerstejaars student met enige verontwaardiging aangesproken: "Steeds als u een bewering doet bewijst u hem ook nog, is dat niet erg ouderwets?" Hoe vreemd zo'n opmerking ook mag klinken in de oren van beroepswiskundigen, of van de oudere generatie in het algemeen, hij illustreert dat zo langzamerhand het nut en doel van bewijzen aan een grote groep van studenten en (waarschijnlijk) docenten ontgaat.

Het kan dan ook geen kwaad om de pro's en contra's van 'bewijzen' nog eens op een rijtje te zetten. Waarom zouden we wèl bewijzen dat de diagonalen van een rechthoek gelijk ("even lang") zijn en niet dat water kookt bij 100° C? Het antwoord heeft te maken met de mate van zekerheid die we aan beide uitspraken verbinden. "Zekerheid" is een in hoge mate theoretisch begrip, maar het is heel goed aan een eenvoudig voorbeeld te demonstreren; laten we zo'n simpel voorbeeld bekijken: er is een spelletje waarbij twee spelers beurtelings van een stapeltje lucifers tenminste 1 en ten hoogste 3 lucifers afpakken. Wie de laatste lucifer pakt verliest.

Voor zo'n spel is er een eenvoudige strategie, en u verkeert in de gelukkige omstandigheid dat hij aan u wordt meegedeeld door een oom die hem weer van zijn zwager heeft, die hem weer weet van een geleerde uit Zuid-Patagonieë. De strategie is : neem zoveel lucifers weg dat er een viervoud plus een overblijft. Wanneer er om te beginnen , zeg, 17 lucifers liggen , dan kunt u alleen maar hopen dat Uw tegenstander de strategie nog niet gehoord heeft. De vraag is nu, zal een doorsnee lezer op grond van deze mededeling bereid zijn te spelen om zeer grote inzetten ? Daarvoor moet hij toch wel heel zeker van de correctheid van de strategie zijn. Een mededeling alleen lijkt daarvoor niet voldoende, stel dat bij het doorgeven van de strategie onderweg een vergissing ingeslopen is, of erger nog, dat hij opzettelijk voor de gek gehouden wordt! De enige manier om achter de juistheid van de strategie te komen, en dus de gevraagde zekerheid te krijgen, is een overtuigend, sluitend argument ervoor te leveren. Zo'n argument kan er als volgt uitzien:

Noem de spelers I en II ; I is het eerst aan zet.Het stapeltje bevat n lucifers. Als n = 1 dan verliest I, maar als n = 2, 3, 4 dan kan I winnen door resp. 1, 2, 3 lucifers weg te nemen. Is echter n = 5, dan blijven er na de zet van I 4, 3 of 2 lucifers over en dan wint II (als hij slim is). Bij 1 en 5 kan II derhalve winnen, hij heeft een (winnende) strategie. Men ziet gemakkelijk dat voor n = 6, 7, 8 I weer kan winnen doordat hij II op 5 kan zetten. Zo generaliserend komen we op de volgende conclusie: I heeft een winnende strategie als n geen viervoud plus 1 is.

Vraag: is hiermee *bewezen* dat het bovenstaande correct is? In zekere zin wel, we hebben een betoog in elkaar gezet dat onszelf en vrienden en kennissen overtuigt. Overtuigt het ook een robot of Sherlock Holmes? Daar is waarschijnlijk meer voor nodig, zij zullen geen genoegen nemen met "men ziet gemakkelijk dat" en "zo generaliserend".Sherlock Holmes, met zijn superieure intelligentie, zal waarschijnlijk ons "bewijs" niet nodig hebben; hij heeft aan een paar woorden genoeg om zelf een correct bewijs te leveren, maar als sceptisch toehoorder zal hij ongetwijfeld onze redenering als ondeugdelijk verwerpen. Machines en Pietjes Precies eisen een puntgaaf bewijs, zonder beroep op de welwillendheid van de lezer. Zo'n bewijs leveren we in dit geval met het *principe van volledige inductie* . Alvorens dat bewijs te geven zullen we trachten nog wat onheil te stichten met behulp van dit bewijsprincipe.

We geven eerst een bewijs van een veel spectaculairdere bewering: Alle mensen zijn mannelijk òf alle mensen zijn vrouwelijk.

Eerst een bewijs dat zich niet bekommert om formele details: beschouw een groep van n mensen, zeg $a_1,...,a_n$.We herleiden het probleem als volgt tot een kleinere groep: laat a_1 weg, dan blijven $a_2,...,a_n$ over.Als we al wisten dat groepen van n-1 mensen van hetzelfde geslacht waren dan bestaan $a_1,...,a_n$ uit uitsluitend mannen of vrouwen.Wanneer we inplaats van a_1 persoon a_n weggelaten hadden, waren we tot de conclusie gekomen dat $a_1,...,a_{n-1}$ allen van het zelfde geslacht zijn. Ergo; iedereen is van hetzelfde geslacht. Nu wijst de weg zichzelf, in eindig veel stappen komen we bij een groep bestaande uit één persoon, en voor dat geval is de bewering onmiddellijk duidelijk!

De bovenstaande redenering is misschien wel wat erg nonchalant, vandaar de dwaze conclusie. Laten we dus overgaan tot een exact bewijs met behulp van het principe van volledige inductie; de stilzwijgende aanname is dat er slechts eindig veel (thans levende of reeds overleden) mensen zijn. Wij kunnen met inductie "naar het aantal mensen" aantonen dat "voor elke n geldt dat iedere verzameling van n mensen bestaat uit personen van het zelfde geslacht" Voor n = 1 is de uitspraak evident: een verzameling van één mens bestaat uit louter vrouwen of mannen.

Beschouw nu een verzameling van n + 1 mensen $a_1,....,a_n, a_{n+1}$. De inductiehypothese zegt dat alle groepen van n mensen uit mannen òf uit vrouwen bestaan. De verzameling $\{a_1, ..., a_n\}$ is derhalve, zeg, een collectie vrouwen. Maar de verzameling $\{a_2, ... a_{n+1}\}$ is eveneens een verzameling vrouwen (want a_2 was al een vrouw en $a_2, ..., a_{n+1}$ zijn allen van hetzelfde geslacht), nu is echter a_{n+1} een vrouw en dus zijn $a_1, ..., a_{n+1}$ allen van hetzelfde geslacht. Een toepassing van het inductie- principe leert ons dat alle eindige verzamelingen van mensen van hetzelfde geslacht zijn, en dus ook de collectie van *alle* mensen.

We zitten nu met een levensgroot probleem: we hebben een evident onware uitspraak bewezen. De ervaring leert dat studenten die met dit bewijs geconfronteerd worden in grote verwarring raken. De meest geliefde conclusie is dat het principe van volledige inductie *dus* niet juist is. Nu, dat is het wèl, en daarom loont het de fout in het bewijs op te sporen. De lezer die de fout niet gezien heeft doet er goed aan het boek nu even te sluiten en zelf de fout op te sporen.

De kneep zit hem in de juiste formulering van het inductieprincipe[1]:

$[A(1) \wedge \forall n(A(n) \rightarrow A\ (n+1))] \rightarrow \forall n A(n)$.

(Merk op dat we de natuurlijke getallen hier laten beginnen met 1; er is niets op,tegen om 0 bij de natuurlijke getallen te rekenen, in dat geval moeten we het principe aanpassen: $[A(0) \wedge \forall n(A(n) \rightarrow A(n+1)) \rightarrow \forall n A(n)]$. De keuze tussen beginpunt 0 of 1 wordt meestal op zuiver opportunistische gronden gemaakt; de vraag of 0 nu wel of niet een natuurlijk getal is staat hier helemaal buiten!)

We hebben het verifiëren van de premisse wat te snel gedaan; voor n = 1 geldt de bewering A(n) "iedere verzameling van n mensen is van hetzelfde geslacht", daar zit geen probleem. Nu het volgende onderdeel, voor iedere n moet gelden $A(n) \rightarrow A\ (n+1)$.

In ons bewijs hebben we stilzwijgend aangenomen dat er een persoon a_2 zowel in $\{a_1, ...,a_n\}$ als $\{a_2, ..., a_{n+1}\}$ zit, maar dit veronderstelt dat n > 2. Er behoort dus een apart bewijs gegeven te worden voor $A(1) \rightarrow A(2)$. Aangezien A(1) al correct was moeten we met blote handen (d.w.z. zonder steun van de inductiehypothese, die immers geen extra informatie geeft) A(2) bewijzen. Welnu, de verzameling {Adam, Eva} is een tegenvoorbeeld. Ergo, $A(n) \rightarrow A(n+1)$ geldt niet voor alle n.

Wat is nu de moraal van deze excursie naar een fout bewijs? In de eerste plaats een waarschuwing dat overtuigd worden door een goed ogend betoog niet zoveel waarde heeft; in het maatschappelijke verkeer is iedereen zich terdege bewust van de macht van de drogreden (of erger), maar in het wetenschappelijk bedrijf is men zozeer opgegroeid met 'ons vertrouwt ons', dat met opzettelijke misleiding nooit gerekend wordt (dat is een van de redenen waarom goochelaars beter dan geleerden in staat zijn paranormale claims te ontmaskeren). Toevallig was de bovenstaande redenering inderdaad een geval van opzettelijke misleiding, althans een poging daartoe, maar hoe licht kan men niet te goeder trouw een fout bewijs produceren! In de tweede plaats demonstreert het bovenstaande dat de "proof of the pudding", te weten het nauwkeurig napluizen van de redenering tot een verklaring van het raadsel leidt; hiervoor is het vaak noodzakelijk om de hele bewijsmethodiek grondig overhoop te halen, deze gang van zaken is in de geschiedenis van de wetenschap volstrekt niet uitzonderlijk.

Terug nu naar het spelletje met de lucifers. Om helemaal zeker te zijn dat $\forall n W(n)$ juist is, met W(n) := "I heeft een winnende strategie als $n \neq 1 \pmod 4$" geven we een bewijs met behulp van volledige inductie.

We veranderen de bewering een beetje (maar niet wezenlijk):

W'(k) := " I heeft een winnende strategie als er 4k+2, 4k+3 of 4k+4 lucifers zijn."

---

[1] Ter vereenvoudiging van ons betoog zullen we gebruik maken van de notaties van de symbolische logica. Hieronder volgt een lijstje van notaties:

$\wedge$	-	en, conjunctie
$\vee$	-	of, disjunctie
$\rightarrow$	-	als....dan, implicatie
$\neg$	-	niet (non), negatie
$\leftrightarrow$	-	dan en slechts dan als, bi-implicatie
$\forall$	-	voor alle, alquantor
$\exists$	-	er is, existentiequantor

(1) W'(0) zegt dat er een winnende strategie voor I is bij 2, 3 of 4 lucifers. Inderdaad, I neemt in die gevallen 1, 2 of 3 lucifers weg; W'(0) is dus correct.

(2) Neem nu W'(k) aan. W'(k+1) luidt dat er bij 4k + 6, 4k +7 of 4k +8 lucifers een winnende strategie is. Neem dus aan dat er 4k+6,4k+7 of 4k+8 lucifers zijn. I neemt nu respectievelijk 1, 2 of 3 lucifers weg, zodat II van een stapel van 4k +5 moet nemen. Hij reduceert de stapel tot 4k+4, 4k+3 of 4k+2, maar nu kan I, op grond van de inductiehypothese, het spel winnen met een winnende strategie. De winnende strategie voor W'(k+1) bestaat dus uit het volgende voorschrift: kies zoveel lucifers dat er 4k + 5 overblijven, wacht tot II gekozen heeft en pas verder de reeds gegeven winnende strategie van W'(k) toe. Het principe van volledige inductie zegt nu dat $\forall k W'(k)$ en dus $\forall n W(n)$. Merk op dat de uitspraak alleen de *existentie* van een strategie verzekert, de inductiestap is echter zo eenvoudig dat een expliciete strategie ogenblikkelijk af te lezen valt.

Men zou over het bovenstaande bewijs kunnen zeggen 'veel geschreeuw maar weinig wol', immers de allereerste, wat luchtige redenering overtuigt ook al. Dat is misschien waar, niettemin zal het "mannen-vrouwen" voorbeeld menige lezer voorzichtig gemaakt hebben en hem ingeprent hebben dat beweringen bewijzen nodig hebben. Wanneer uw oom een winnende strategie voor een of ander spel verklapt, dan wilt u toch wel een bewijs hebben dat de methode werkt voordat u er grote sommen geld aan gaat wagen!

Bewijzen vervullen in het algemeen de rol van 'zekerheid verschaffers'. Iemand die zelf knutselt aan zijn electrische installatie zal een schema maken van de schakelingen en, uitgaande van de natuurkundige wetten, beredeneren (d.w.z. *bewijzen*) dat de installatie functioneert. Weliswaar zal hij zich indekken tegen risico's door eerst de stoppen te verwijderen, en daarna als een proef op de som de stroom in te schakelen, maar dat is een normale en prijzenswaardige voorzichtigheid die de melkboer ook toepast wanneer hij een rekening voor alle zekerheid twee keer optelt (althans wanneer hij geen rekenmachientje bij zich heeft).

Het zekerheidsargument heeft in realistische situaties een beperkte waarde omdat de te behandelen problematiek in de regel behept is met onnauwkeurigheden van materiele aard, bij voorbeeld nauwkeurigheidsgrenzen van metingen. Voorts zijn er in het algemeen theoretische vooronderstellingen die niet altijd volledig overeenstemmen met de werkelijkheid. De wiskundige wast in zo'n geval zijn handen in onschuld en zegt dat zijn uitspraak zeker is ten opzichte van de theoretische en experimentele gegevens. Wat er ook afgedongen kan worden op de mate van zekerheid die de wiskunde verschaft, het is duidelijk dat er zonder wiskunde (inclusief zijn bewijstechniek, d.w.z. logica) in het geheel geen zekerheid verkregen kan worden.

2. WAARHEID OF BEWIJSBAARHEID

"Op mijn bureau staat een flesje Tipp-Ex", ziehier een uitspraak waarvan de waarheid gemakkelijk vast te stellen is. Op het moment dat ik dit schrijf overzie ik mijn bureau en constateer dat er zo'n flesje staat, het is wit, van plastic gemaakt, en ik heb zojuist gecontroleerd dat er nog Tipp-Ex vloeistof inzit. Strikt genomen moet ik de uitspraak wat aanvullen om hem een blijvende waarheid te verschaffen; ik moet bijvoorbeeld het tijdstip toevoegen en vertellen welke van mijn vele bureau's het flesje draagt en wie ik ben. Maar die toevoegingen zijn voor mijzelf voor het constateren van de waarheid niet zo belangrijk; waar het om gaat is dat ik de waarheid eenvoudigweg *constateer*, de waarheid van eenvoudige uitspraken stelt men eenvoudigweg vast door inspectie. Hier is natuurlijk sprake van een fikse idealisatie, het constateren van ervaringsdata is een gecompliceerde materie; van deze problematiek zien we hier opzettelijk af. De waarheid van gecompliceerde uitspraken levert meer moeilijkheden, evenals de waarheid over abstracte, denkbeeldige zaken. Omdat wiskunde zich bezighoudt met denkbeeldige zaken - zoals getallen, bollen, functieruimten, afgeleiden - loont het om even stil te staan bij het begrip 'waarheid' in de context van de wiskunde. Aangezien de mens zijn eigen wiskundige objecten maakt - in Brouwer's terminologie spreekt men van mentale constructies - zijn zelfs eenvoudige uitspraken als '2 + 2 = 4' en '5 > 3' geen direct verifieerbare of constateerbare uitspraken, maar uitspraken waarvan men de waarheid aan de hand van een redenering, uitgaande van de definitie van 'optelling' of 'groter dan', inziet.

Het waarheidsbegrip zoals dat in de logica en de wiskunde wordt gehanteerd is een idealisatie van de gangbare praktijk. Men neemt aan dat een bepaalde wiskundige structuur (bij voorbeeld de gehele getallen met de ring operaties en met de ordening) in haar geheel te overzien is, precies zoals men de afrekening van het groot winkelbedrijf, of de kinderen in een klas, overziet. Men leest dan direct de waarheid af van '7.2 = 14' af; sterker nog, men leest direct de waarheid af van

$$\forall x \exists y\ (y>x\ \wedge\ \forall z_1 \forall z_2\ (z_1.z_2 = y \rightarrow z_1 =1 \vee z_2 =1 \vee z_1 =-1 \vee z_2 =-1))$$

(d.w.z. "er zijn oneindig veel priemgetallen").

Onder het gezichtspunt van de "waarheid" kan men dus oneindige verzamelingen en hun eigenschappen overzien zoals men de tafel van 7 overziet.

Het is duidelijk dat we niet zoveel aan het waarheidsgezichtspunt hebben; zolang er geen groot boek is waar alle waarheden in staan - en dat voor ons toegankelijk is - helpt 'waarheid' ons niet verder. Het vermoeden van Fermat is waar of onwaar, maar zolang we niet weten welke van de twee mogelijkheden het geval is helpt ons zo'n algemene uitspraak niet veel. Het zou al een stuk helpen als we een bewijs van "Fermat" of van zijn negatie hadden, immers, een bewijs heeft het grote voordeel boven 'waarheid' dat bewijzen voor ons mensen toegankelijk zijn. Waarheid is iets dat voorbehouden is aan geïdealiseerde wezens die een ongelimiteerd kenvermogen hebben (de alwetendheid). Er is dus alle reden voor ons stervelingen om het in de eerste plaats maar bij bewijsbaarheid te houden.

3. BEWIJZEN - CONVENTIES OF NATUURLIJKE METHODEN?

Een bewijs is, in eerste opzet, een redenering die ons overtuigt. Moet men hierbij denken aan een soort gevoelsproces waarbij men op een bepaald moment de drempel van de twijfel achter zich laat en zegt "Ja, nu neem ik het wel aan", of is er meer? In de rechtszaal bij Perry Mason gaat het er om de jury "beyond reasonable doubt" te overtuigen, maar in de wiskunde gaat het om overtuigen "beyond any doubt". Het is natuurlijk maar de vraag of dat kan. Soms wel en soms niet.

In bepaalde gevallen schrijft de vorm van de bewering voor waar een bewijs uit moet bestaan. Wanneer men wil bewijzen dat "f is continu en positief definiet", bewijst men gewoon twee dingen: "f is continu" en "f is positief definiet". Schematisch: $A \wedge B$ (d.w.z. A *en* B) bewijst men door A te bewijzen en B te bewijzen.

Een implicatie als "in een gelijkbenige driehoek zijn de hoeken tegenover de gelijke zijden gelijk" bewijst men door aan te nemen dat twee zijden gelijk zijn en daaruit te bewijzen dat de tegenoverliggende hoeken gelijk zijn.Schematisch: $A \rightarrow B$ bewijst men door A aan te nemen en B te bewijzen.

In het algemeen geeft de logische vorm van de uitspraak aan wat er bewezen moet worden. Wij geven hieronder in telegramstijl weer hoe logisch samengestelde uitspraken bewezen moeten worden.

Men bewijst: $A \wedge B$ door A te bewijzen en B te bewijzen
$A \to B$ door A aan te nemen en B te bewijzen.
$\forall x A(x)$ door $A(a)$ te bewijzen voor een "willekeurige" a.

Voor de negatie hoeven we geen aparte afspraak te maken omdat de negatie gedefinieerd wordt uit de implicatie en een onwaarheid (contradictie): $\neg A$ betekent $A \to \perp$, waar $\perp$ een contradictie (onware uitspraak) is, zoiets als $0 = 1$. Om $\neg A$ te bewijzen nemen we dus A aan en bewijzen een contradictie.

In de jaren dertig heeft G. Gentzen een logisch systeem bedacht dat nauw aansluit bij onze bewijspraktijk, het systeem van de *natuurlijke deductie;* dit systeem bootst getrouw de stappen na die hierboven aangegeven zijn. De notatie van de natuurlijke deductie is wellicht wat verrassend voor de lezer die het voor de eerste maal ziet; bewijzen worden namelijk als bomen geschreven. Dat is niet erg wezenlijk omdat iedere wiskundige weet hoe hij bomen moet platslaan. Ter illustratie laten we hieronder enkele karakteristieke voorbeelden van natuurlijke deductiestappen zien:

$$\frac{A \quad B}{A \wedge B} \qquad \frac{A \wedge B}{A} \qquad \frac{A \quad A \to B}{B} \qquad \frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \to B}$$

De laatste deductiestap eist enige toelichting, men moet de regel lezen als: wanneer een bewijs van B uit A gegeven is, dan verkrijgt men in één stap hieruit een bewijs van $A \Leftarrow B$ door de hypothese A weg te laten. Dit weglaten is aangegeven door het tussen haakjes zetten van A. Natuurlijk komt de hypothese A in de totale redenering nog voor, maar hij is niet meer nodig om $A \to B$ te rechtvaardigen. Merk op dat deze deductie stap verschilt van de voorafgaande doordat hier in een stap het hele bewijs betrokken wordt. De andere deductiestappen zijn *locaal*, maar deze zg. $\to$-introductie niet!

We hebben twee samenstellingen weggelaten: $A \vee B$ en $\exists x A(x)$. Er is een goede reden voor deze terughoudendheid, men kan namelijk van mening verschillen over de betekenis van "of" en "er is een ......". De constructieve interpretatie van $\exists x A(x)$ is "we kunnen een object a en een bewijs van A(a) aangeven", de gebruikelijke niet-constructieve opvatting van "er is een x zodat A(x)" is "het is niet waar dat $\neg A(x)$ voor alle x geldt". In symbolen $\exists x A(x) := \neg \forall x \neg A(x)$. Hetzelfde geldt voor de disjunctie, de constructivist zal $A \vee B$ alleen aanvaarden als hij een van beide bewezen heeft, de niet-constructieve wiskundige zal daarentegen al tevreden zijn als hij kan aantonen dat $\neg A$ en $\neg B$ niet beide waar kunnen zijn. In symbolen $A \vee B := \neg(\neg A \wedge \neg B)$.

De natuurlijke deductiestappen voor de disjunctie en de existentie-quantor zien er wat onaantrekkelijker uit dan de bovenstaande stappen, bijvoorbeeld

$$\dfrac{A \vee B \qquad \begin{array}{c}[A]\\ \mathcal{D}\\ C\end{array} \qquad \begin{array}{c}[B]\\ \mathcal{D}'\\ C\end{array}}{C}$$

Dit is niet de plaats om in te gaan op de deugden of ondeugden van het constructivisme. Het moge volstaan om te zeggen dat er inderdaad gevallen zijn van existentie-uitspraken in de wiskunde die wel *non-constructief* maar niet *constructief* aangetoond zijn. In de folklore spreekt men van "zuivere existentiebewijzen", er was een tijd dat wiskundigen zelfs trots waren op dit soort bewijzen, als een soort super goocheltruc (zie ook hfdst. I).

De vraag is nu of al het bewijzen van zuiver logische aard is; anders gezegd: zijn alle bewijzen en bewijsmethoden puur logisch en "subject-onafhankelijk"? De logistici (de school van Frege en Russell) waren inderdaad die mening toegedaan.

Er zijn echter gevallen waarin de wiskundige structuur de bewijsmethode voorschrijft. Het voorbeeld bij uitstek is de structuur van de natuurlijke getallen.

De natuurlijke getallen worden gegenereerd door het simpele proces van het herhaald toevoegen van eenheden.[2]

Hier is het recept:- 1 is een natuurlijk getal ($1 \in \mathbb{N}$)
- als n een natuurlijk getal is, dan is n+1 ook een natuurlijk getal ($n \in \mathbb{N} \rightarrow n+1 \in \mathbb{N}$)

Bij deze manier van genereren hoort een bewijsmethode:

$[A(1) \wedge \forall n \in \mathbb{N}\ (A(n) \rightarrow A(n+1))] \rightarrow \forall n \in \mathbb{N}\ A(n)$

Deze methode (de volledige (of mathematische) inductie) wordt gedicteerd door de inductieve manier van voortbrenging van de natuurlijke getallen.

Hier is een argument ter ondersteuning van het bewijs met volledige inductie:

Gevraagd wordt een methode die voor iedere willekeurige n een bewijs van A(n) levert. Zo'n n wordt verkregen door achtereenvolgens 1, 2, 3, ..., n-1, n te genereren. We hebben een bewijs van A(1) en een bewijs van $\forall n \in \mathbb{N}\ (A(n) \rightarrow A(n+1))$, hieruit volgt dat we een bewijs van $A(1) \rightarrow A(2)$ hebben. We combineren de bewijzen van A(1) en $A(1) \rightarrow A(2)$ en krijgen een bewijs van A(2). Nu gaan we op dezelfde manier voort, iedere keer dat het volgende getal k gegenereerd wordt leveren we er een bewijs van A(k) bij. Conclusie: ieder getal n dat gegenereerd wordt heeft een bijbehorend bewijs van A(n).

Het voorbeeld van de natuurlijke getallen is typisch voor z.g. *inductief gedefinieerde verzamelingen.* Andere voorbeelden van inductief gedefinieerde verzamelingen zijn eindige bomen,formules in een formeel systeem, expressies (programma's) in een programmeertaal. Die verzamelingen hebben elk hun eigen karakteristieke bewijsmethoden.

---

2 Bij het opbouwen van de natuurlijke getallen uit eenheden moet men wel met 1 beginnen; de toevoeging van 0 (met zijn eigenschappen) kan louter als een handige truc gezien worden, maar er zijn ook diepzinnige beschouwingen die de invoering van 0 rechtvaardigen. Bezien vanuit het standpunt van de geordende verzamelingen is er natuurlijk geen verschil tussen natuurlijke getallen met of zonder 0 - de verzamelingen zijn isomorf.

De moraal is dat er wel degelijk essentieel *wiskundige* bewijsmethoden bestaan.

4. BEWIJZEN VAN PARADOXALE RESULTATEN.

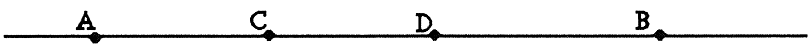
Bewijzen leren ons "wat het geval is". Een bewijs overtuigt ons ervan dat ieder natuurlijk getal op eenduidige wijze te factorizeren is in priemfactoren; in zekere zin is dat een "proef op de som" - we dachten al lang dat het zo was. Zo'n bewijs verschaft ons een absolute zekerheid waar wij al de correctheid geloofden, maar misschien nog dat extra stukje zekerheid nodig hadden om te zien dat er geen addertjes onder het gras scholen. Het gaat wat verder om in te zien dat ieder natuurlijk getal de som is van vier kwadraten (Lagrange), hier is het bewijs geen extraatje, maar juist het wezenlijke inzicht gevende. Zonder dat bewijs zouden we hoogstens een vermoeden kunnen hebben, maar geen zekerheid. Er bestaan ook zelfs stellingen die in eerste aanleg geen zekerheid, maar alleen verwarring scheppen; hier zijn enkele voorbeelden: (a) het segment [0,1] kan continu op het eenheidsvierkant afgebeeld worden (Peano); (b)Een bol kan in een eindig aantal stukken verdeeld worden die zo aan elkaar geplakt kunnen worden dat twee bollen van dezelfde grootte als de oorspronkelijke bol ontstaan (Banach - Tarski), [J].

Ofschoon we deze bewijzen stap voor stap kunnen volgen zijn de resultaten in conflict met onze aanschouwing. Wie voor het eerst zo'n stelling tegenkomt zal als regel het bewijs voor onjuist verslijten.

Deze z.g. paradoxale stellingen (in de zin dat ze in strijd lijken met onze weloverwogen verwachtingen) staan als waarschuwingsborden langs het pad van de wiskunde, ze leren ons dat onze (vooral ruimtelijke) intuïtie niet het laatste woord heeft en dat in ieder stadium van de wiskunde bepaalde anti-intuïtieve feiten aangetoond worden, die na verloop van tijd de basis van een aangepaste intuïtie gaan vormen.

Zo beschouwde men aanvankelijk het optreden van discontinue functies als een soort van pathologie, waar de intuïtie zich overigens al snel bij aanpaste. Veel later werden verschijnselen als 'continu, nergens differentieerbare functies' ontdekt, en nu verbaast niemand zich daar meer over.

Een voorbeeld ter illustratie van zo'n verschuiving van de intuïtie: een van de axioma's van Euclides luidt "het geheel is groter dan zijn deel". In de meetkunde van Euclides is dit een evident feit. Het lijnstuk CD is een deel van AB en het is onmiddellijk duidelijk dat AB groter is dan CD.



Het enige wat ons zou kunnen hinderen in Euclides' axioma is het feit dat "groter dan" niet gedefinieerd is; het begrip komt wel eerder voor (een stompe hoek is dat wat groter is dan een rechte hoek), maar het is niet omschreven. We kunnen het axioma ook lezen als een bepaling van "groter dan", en inderdaad laat zich de meetkunde van Euclides met deze notie van "groter dan" uitstekend behandelen.

Het bovenstaande axioma van Euclides had zo'n grote aanschouwelijk evidentie dat men het zonder verdere kritische analyse tot een algemene waarheid verhief. In 1638 merkte Galilei op dat in bepaalde omstandigheden het axioma tot ongerijmdheden leidde. Galilei beschouwde binnen de verzameling $\mathbb{N}$ der natuurlijke getallen de verzameling K der kwadraten; hij merkte op dat hoewel K een echt deel van $\mathbb{N}$ is, toch K en $\mathbb{N}$ 'even groot' zijn. En wel als volgt: hij voegde aan ieder getal n zijn kwadraat n^2 toe en merkte op dat deze toevoeging een-eenduidig was (in de huidige terminologie, $\mathbb{N}$ en K zijn gelijkmachtig). In de zin van Euclides zijn $\mathbb{N}$ en K met recht als 'gelijk' aan te merken, ze "passen op elkaar".

Het resultaat is de paradox van Galilei: de verzameling der kwadraten is zowel "kleiner dan" als "gelijk aan" de verzameling der natuurlijke getallen.

Aan het eind van de negentiende eeuw werden beschouwingen van deze soort weer opgenomen (o.a. door Bolzano en Cantor;) en nader geanalyseerd. De wiskundige aanschouwing paste zich snel aan de feiten aan, en sindsdien is het gemeengoed om "groter", "kleiner" en "gelijk" los van Euclides' axioma te beschouwen. Uiteindelijk leiden paradoxale verschijnselen altijd tot een verdieping van inzicht - dat is de wetenschappelijke manier om zwaarden tot ploegscharen om te smeden. Een toepassing van de verbeterde inzichten over "kleiner" en "gelijk" is Cantors bewijs van het bestaan van transcendente getallen.

De les van deze voorbeelden is dat bewijzen nuttig en noodzakelijk zijn als corrigerend medium voor onze vaak onvolmaakte aanschouwing.

5. BESTAAT ZEKERHEID WEL?

Zolang als filosofen bestaan hebben, zolang zijn er verdedigers geweest van het standpunt dat zekerheid niet bestaat. Een argument voor dat standpunt berust op de observatie dat door voortdurend verscherpen der criteria van exactheid veel stellingen mettertijd als 'onjuist' of 'onbewezen' hun status van juistheid verloren hebben. Lakatos heeft een buitengemeen boeiend verslag van de lotgevallen van de stelling van Euler betreffend het verband tussen de aantallen vlakken, ribben en hoekpunten van polyhedra geschreven [L]. Men heeft hier wel de boodschap aan verbonden dat "absolute zekerheid niet bestaat". Zo'n interpretatie van de wiskundige ervaring is echter wel wat hardvochtig en overtrokken. Laten wij een voorbeeld beschouwen: de middelwaardestelling van de reële analyse wordt als regel bewezen door een iteratie van intervalkeuzen. Precies beschouwd komt zo'n bewijs neer op een toepassing van het keuzeaxioma. Was het bewijs juist toen het keuzeaxioma nog niet ontdekt was? Een mogelijk antwoord is: nee, want er werd gebruik gemaakt van een niet bewezen resultaat; een ander antwoord luidt: toch wel, want een nadere analyse van het bewijs laat ons zien dat het keuze-axioma stilzwijgend toegepast werd, m.a.w. de auteur nam aan dat een keuzeproces, als gebruikt in het bewijs, toegestaan was.

De verdwenen exactheid kan derhalve gerehabiliteerd worden door het bewijs als primair te beschouwen en pas daarna de stelling correct te formuleren. In zekere zin bedrijft men dan een soort wiskundige archeologie: er is een bewijsachtige tekst gegeven die men stap voor stap nagaat op correctheid en gebruikte principes. Het resultaat is dan een korte samenvatting van het bewijs, in de vorm van "als zo en zo en zo, dan zus". Natuurlijk leent ook deze uitleg zich tot een parodie. Zo kan een student beweren dat hij een goede oplossing gegeven heeft onder de aanname dat 27 een priemgetal is. Daar is misschien alleen tegen in te brengen dat de waarde van een correct bewijs met teveel hypothesen (i.h.b. incorrecte) niet zo erg hoog is.

Andere argumenten tegen de exactheidspretenties van de wiskunde komen uit de koker van Wittgenstein en gaan in feite al terug op Mannoury. Zij hebben betrekking op de problemen die verbonden zijn aan het toepassen van regels. Men kent de populaire spelletjes van "noem het volgende getal". Wat volgt op 2, 4, 6, 8, 10? Wie zal het zeggen, er zijn genoeg regels die om te beginnen 2, 4, 6, 8, 10 opleveren. De moeilijkheid wordt opgelost door een regel te geven: begin met 2 daarna wordt ieder getal verkregen door 2 bij de voorafgaande op te tellen. Nu brengt de scepticus het volgende bezwaar naar voren: hoe weet ik wat deze regel betekent. Misschien ben ik gewend om de regel $a_1 = 2$, $a_{n+1} = a_n + 2$ op te vatten als $a_1 = 2$, $a_{n+1} = a_n \oplus 2$, waar "$x \oplus 2$" betekent "tel 2 op zolang $x \leq 500$ en vermenigvuldig met 2 als $x > 500$". Er zit niet veel anders op dan ons te beperken tot situaties waarin regels correct toegepast worden [K].

Ook binnen de wiskunde zelf is er niet te negeren kritiek op het zekerheidsideaal uitgeoefend. Allereerst zal het niemand ontgaan zijn dat allerlei handige maar twijfelachtige principes na verloop van tijd ontmaskerd zijn, men denke aan het "permanentieprincipe;" (Hankel (1867): formele wetten blijven behouden bij overgang naar nieuwe systemen). Het "principe van behoud van aantal" (vergl. Hfdst. I) valt ook onder dit hoofd.

Er is echter ook kritiek op korrekte bewijzen binnen een bepaald gegeven kader. Zo verwierp Brouwer het principe van de uitgesloten derde($A \vee \neg A$), als geldig bewijsmiddel en in de relevantielogica verwerpt men bewijzen waarbij stappen toegelaten zijn die geen "verband" leggen tussen premisse en conclusie; een bewering als "als de maan een Edammer kaas is dan is π irrationaal" wordt in de relevantielogica verworpen.

Een analyse en oplossing voor problemen van deze soort is als volgt te geven: de te gebruiken logische (en wiskundige) principes worden bepaald door het (filosofische) kader waarin men werkt. Zo gebruikt men in de constructieve wiskunde de intuïtionistische logica, en in de inconstructieve, ontologische wiskunde de klassieke logica, enz.

Het primaat van de logica vervalt hiermee; logica is niet langer autonoom en context-onafhankelijk, maar daar valt mee te leven.

Niettemin blijft enige knagende, en helaas niet op te heffen twijfel over: wanneer de bewijsmethoden van onze voorvaderen ten offer zijn gevallen aan steeds voortschrijdende exactheid en daarmee gepaard gaande verfijning van kritiek, kunnen wij ons dan veilig wanen? In absolute zin kunnen wij ons niet indekken tegen latere kritiek maar een troost is er toch: uitgaande van *onze* beginselen is er een exactheidscriterium waarvan we de huidige wiskundige productie kunnen meten. Na ons de zondvloed!

6. FORMALISMEN VOOR BEWIJZEN.

Zolang als de mensheid wiskunde bedreven heeft zijn er bewijzen geleverd, en al betrekkelijk vroeg is men tot het inzicht gekomen dat bewijzen volgens een regelmatig patroon verlopen (men denke aan de syllogismen van Aristoteles). Dit inzicht heeft op den duur geleid tot een formalisering van de logica en van het bewijzen. In een formeel systeem zijn bewijzen bepaalde configuraties van formules, waarbij de kleinste stappen (toepassingen van afleidingsregels) direct inzichtelijk zijn op grond van de betekenis van de voegtekens. Deze formele bewijzen zijn voor de gangbare praktijk van de wiskunde voldoende en adequaat, in de zin dat bewijsbaarheid in de z.g. predicatenlogica overeenstemt met waarheid (de volledigheidsstelling van Gödel, 1930).

Er zijn belangrijke voordelen verbonden aan deze formele bewijzen. In de eerste plaats is in een formele context precies vast te stellen wat een bewijs is. Om met Leibniz te spreken, de juistheid van een bewering kunnen we vaststellen door rekenen; dubbelzinnigheid is er niet meer! Bovendien leent een formeel systeem zich voor machinale verificatie (vgl. het hoofdstuk III). Er is nog een extra bonus, men kan de structuur van bewijzen bestuderen en door transformaties speciale, overzichtelijke vormen verkrijgen die extra inzicht verschaffen. De praktijk van het machinaal bewijzen (*automated theorem proving*) berust voor een groot deel op de studie van bewijzen als objecten met een eigen bestaansrecht.

Formaliseringen hebben overigens ook hun begrenzingen, met name wanneer men de theorie van een speciaal stuk wiskunde wil behandelen. Zo kan men zich afvragen of er een formele theorie bestaat die precies alle ware uitspraken van de rekenkunde (preciezer uitgedrukt, alle uitspraken die waar zijn in het standaard model van de natuurlijke getallen) bewijst. Gödels onvolledigheidsstelling (1931) leert ons dat iedere enigermate fatsoenlijke theorie (d.w.z. waarvan we de axioma's systematisch kunnen opschrijven) te kort schiet; dat wil zeggen dat er altijd een ware uitspraak is die binnen zo'n theorie niet te bewijzen is.

Of men de stelling van Gödel nu aangenaam vindt of niet, het is een van de "facts of life" en hij leert ons enige bescheidenheid.

Het formalisme als doctrine is aan scherpe kritiek onderworpen; het idee dat wiskunde een formeel spel is waaraan we geen betekenis hechten is een handige fictie, maar bij nadere beschouwing nauwelijks te verdedigen. Niettemin zijn de vruchten van formalisering aanzienlijk.

Er zijn tal van formalismen voor bewijzen in omloop, er zijn zelfs diverse formalismen voor de beschrijving van de wiskunde. Sommige verschillen alleen in kleine details, andere hebben berusten op hetzelfde principe maar bezitten een totaal verschillende notatie. Tenslotte zijn er verschillen in systemen die van principiële aard zijn. In de praktijk kan men meestal op een systematische manier van het ene formalisme overstappen op het andere. Hetzelfde geldt voor de bewijs-formalismen, er zijn tal van formaliseringen van de notie 'afleidbaar', die ieder hun verdiensten hebben (en meestal ook hun ondeugden).

In grote lijnen zijn er twee klassen van systemen: (1) systemen met veel axioma's, maar met weinig aandacht voor de afleidingsregels, (2) systemen met weinig (het liefst geen) axioma's en veel afleidingsregels.

De eerste soort is van oudsher in de wiskunde gebruikt. Euclides had alleen axioma's (postulaten) en in het geheel geen afleidingsregels. Dat laatste is niet verwonderlijk omdat in het stadium van naieve formaliseringen verfijnde verschillen, zoals tussen 'afleidingsregel' en 'axioma' nog niet gemaakt werd en nauwelijks gemaakt worden kunnen.

De euclidische formalisering was het prototype van formalisering voor de wiskunde, en in zekere zin is hij dat nog steeds. In de negentiende eeuw ontstonden de eerste formaliseringen van de logica, de bekendste - die van Frege - was naar euclidisch patroon ontworpen. Frege gaf de logische basiswetten in de vorm van axioma's en voegde twee afleidingsregels toe om tenminste vanuit de axioma's stapsgewijs bij stellingen uit te kunnen komen.

Hilbert nam deze methode over in zijn publicaties en sindsdien spreekt men van "Hilbert-type systemen", het zou juister zijn om van "Frege-Hilbert-type systemen" te spreken.

In de jaren dertig introduceerde Gentzen twee systemen waarin juist aan de afleidingsregels aandacht geschonken werd, en waarin het aantal axioma's geminimaliseerd werd. Het hierboven genoemde systeem van *natuurlijke deductie* is er een van; het andere systeem, de z.g. *sequenten calculus* heeft een ingebouwd "geheugen"; bij elke stap wordt bijgehouden welke premissen er zijn.

Het systeem van Gentzen heeft het voordeel dat alle voegtekens in isolatie behandeld worden. Men hoeft om de regels (eigenschappen) van $\wedge$ (conjunctie) te geven niet te weten wat met $\rightarrow$ gebeurt.

In de regels

$$\frac{A \quad B}{A \wedge B} \qquad \frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B}$$

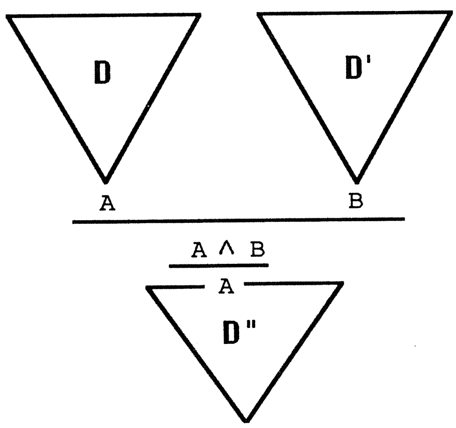
komt alleen $\wedge$ essentieel voor, terwijl in een Frege-Hilbert systeem de overeenkomstige axioma's luiden

$A \rightarrow (B \rightarrow (A \wedge B))$, $(A \wedge B) \rightarrow A$, $(A \wedge B) \rightarrow B$.

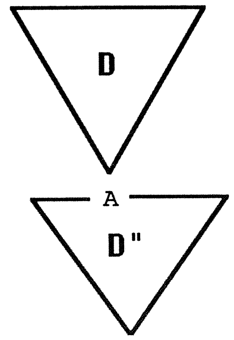
Een oppervlakkige lezer met holistische tendensen mag de axioma's misschien prefereren omdat ze de "samenhang van alles" benadrukken, men bedenke echter dat in de wetenschap het holisme suboptimaal is. Wie een verschijnsel in isolatie kan bestuderen zal zich wel twee maal bedenken complicerende factoren te introduceren.

Het natuurlijke deductie systeem heeft het voordeel van natuurlijkheid en eenvoud, bovendien hebben bewijzen in dit systeem de belangrijke eigenschap *normaliseerbaar* te zijn. Ieder bewijs kan op een normaalvorm gebracht worden. Het zou hier te ver voeren om een preciese behandeling te geven. We zullen aan een simpel voorbeeld demonstreren wat "normaliseren" (vereenvoudigen) inhoudt.

Hieronder is een bewijs schematisch aangegeven.



Het is duidelijk dat dit bewijs niet erg handig is; eerst wordt $A \wedge B$ geïntroduceerd en vervolgens geëlimineerd. Bij de eliminatie komt iets te voorschijn dat al verondersteld werd bij de introductie. Door de introductiestap "weg te gooien" en het bewijs in elkaar te schuiven verkrijgen we een eenvoudiger bewijs.



Normalisatiestappen bestaan uit het verwijderen van (overbodige!) introducties gevolgd door eliminaties. De resulterende bewijzen zijn in een bepaalde zin zo eenvoudig mogelijk, ze gebruiken geen omwegen en geen overbodige begrippen. Normalisatie is een belangrijk hulpmiddel bij theoretische onderzoekingen van de logica en de wiskunde, Gentzen gebruikte deze systemen bij zijn consistentiebewijs van de rekenkunde [G]. Vanzelfsprekend zijn normale bewijzen ook van belang voor de automatizering van bewijzen, [C], en normalisatie is in tal van vormen ingeburgerd in de informatica. Meer informatie vindt men in [D2], [Pr], [TD II, ch.10], [S1], [S2]

7. DE ROL VAN AXIOMA'S.

'Axioma' is afgeleid van 'eisen' of 'vorderen'; letterlijk genomen is een axioma een uitspraak die men aanvaardt zonder bijzondere motieven te geven. De betekenis die men bij Euclides vindt is echter die van 'evidente waarheid'. Die betekenis heeft axioma een lange tijd gehouden, Pascal [P] zegt uitdrukkelijk dat alleen evidente dingen als axioma's opgevoerd mogen worden. Sinds Hilberts *Grundlagen der Geometrie* zijn axioma's gereduceerd tot uitspraken die men (als onbewezen) aan het begin van een theorie zet.

Een andere benaming voor "het vereiste" is *postulaat*, afgeleid van postulare - eisen. In de loop der tijden hebben 'axioma' en 'postulaat' verschillende functies gehad, maar thans beschouwt men in de wiskunde de termen als verwisselbaar. Axioma's in de zin van "onbetwijfelbare waarheid" vindt men nog steeds, bv. in de logica of rekenkunde:

$[A \to (B \to C)] \to [B \to (A \to C)]$ en $\forall x\, [x + 1 \neq 0]$.

Voorbeelden van axioma's in de zin van "handig uitgangspunt" zijn er te over, in feite kan men een willekeurige formule kiezen. Om wat realistischer te blijven, beschouw de axioma's van de projectieve meetkunde plus "er zijn meer dan 7 punten". Het laatste axioma kan men moeilijk als een onbetwistbare waarheid opvatten omdat het soms niet en meestal wel geldt. Zo'n soort axioma vervult niet de rol van "weergave van een (min of meer) unieke werkelijkheid", maar van een extra voorwaarde die een klasse van modellen aangeeft (in het bovenstaande geval, alle projectieve vlakken behalve het 7-punts vlak).

Axioma's van een theorie zijn volgens het formele gezichtspunt eenvoudigweg bepaalde uitspraken waar alle stellingen van de theorie uit volgen.

Van oudsher stelt men zekere eisen aan axioma's:

1. *Onherleidbaarheid.* Deze eis is alleen te motiveren in het geval van inhoudelijke axioma's; hij komt er op neer dat een axioma niet uit een nog eenvoudiger evidente waarheid af te leiden is. Het axioma moet een echt 'onherleidbaar' beginpunt zijn.

Bij formele axioma's is de onherleidbaarheid hoogstens een pragmatische eis van elegantie en gemak. Zo kan men elke eindige axioma verzameling $A_1, \ldots, A_n$ vervangen door één axioma $A_1 \wedge \ldots \wedge A_n$, maar wezenlijk is deze kunstgreep niet; weliswaar zou omgekeerd het reduceren van de samengestelde uitspraak tot zijn onderdelen een vereenvoudiging inhouden, maar soms is het ook wat waard om slechts één axioma te hebben.

2. *Consistentie of niet-strijdigheid.* Wij eisen normalerwijze dat uit de axioma's geen contradictie volgt. Deze eis spreekt bijna voor zichzelf, immers een inconsistente verzameling axioma's heeft geen modellen, slaat nergens op.

De eis van consistentie is niet altijd makkelijk te vervullen, er zijn theorieën waarvan de consistentie slechts een kwestie van overtuiging is zonder dat er een bewijs voor is; men denke aan de verzamelingsleer. Er zijn ook theorieën geweest die pas na enige tijd als inconsistent herkend werden, het pijnlijkste geval is Freges logica [F], vgl.[D1,blz.81].

De consistentie eis is zwaarwegend, wie wil tenslotte het risico lopen over *niets* te theoretiseren!

3. *Onafhankelijkheid.* Hier is weer sprake van een elegantie-criterium: wij willen geen overbodige axioma's, dus eisen we dat geen axioma uit de overige axioma's afleidbaar is. Vroeger nam men de onafhankelijkheid hoog op, en menig artikel werd geschreven over de afhankelijkheid van een axiomastelsel. Tegenwoordig is men wat makkelijker geworden; als we weten dat B met grote inspanning en vele bladzijden hard werk uit A_1, A_2, A_3 afleidbaar is, dan is men licht geneigd B als axioma op te nemen om werk te sparen, terwijl de afhankelijkheid in een voetnoot vermeld wordt.

8. HET NUT VAN DE AXIOMATISCHE METHODE.

Hoewel de axiomatische methode door de eeuwen heen het waarmerk van de meetkunde van Euclides geweest is, werd zij pas echt populair in de twintigste eeuw toen men oog kreeg voor de vele wiskundige structuren die in de wiskundige praktijk ontdekt of zelfs verzonnen, werden. Men denke aan de diverse algebraïsche structuren die als het ware klaar lagen om herkend te worden; groepen (matrices, substituties, getalsystemen, transformaties), partieel geordende verzamelingen (deelbaarheid, ordeningen, deelverzamelingen),modulen (vectoren,matrices, functieruimten).

Deze structuren waren eenvoudig te axiomatiseren en konden derhalve onder één gezichtspunt behandeld worden. Door een stelling in de groepentheorie te bewijzen krijgt men een bewering die waar is voor *alle* groepen. Dit inzicht is nu zo stevig verankerd in onze praktijk dat het grenst aan een platitude, niettemin kan het iedereen overkomen dat hij in een ogenblik van onoplettendheid een bewering aantoont voor, zeg, matrices met behulp van veel rekenwerk (*going back to basic principles*) en pas daarna opmerkt dat het eigenlijk een zaak van eenvoudige groepentheorie was. Kortom het inzicht is gemeengoed, maar men moet wel een open oog voor de toepassingen houden.

9. WISKUNDIGEN EN HUN BEWIJZEN.

In de wiskundige gemeenschap spelen bewijzen een rol die afwijkt van het hiervoor geschetste ideaal van onaantastbaarheid en narekenbaarheid. De sociale component van het wiskundebedrijf houdt er een andere praktijk op na dan de logische component. Bewijzen worden door mensen gemaakt (althans tot voor kort) en door mensen al of niet begrepen. De normale gang van zaken is dat X een stelling bewijst en aan een aantal collegas ter kennis brengt (al of niet via een tijdschrift), vervolgens controleren een aantal mensen het bewijs, verbeteren onderdelen en vullen omissies aan. Het artikel wordt gerefereerd, van commentaar voorzien, een tweede versie wordt geschreven enz. Wanneer de stelling voldoende belangstelling trekt worden alternatieve bewijzen gegeven, lemma's geïsoleerd, generalisaties gegeven, tegenvoorbeelden tegen versies in andere contexten, enz. In de loop van zo'n langdurig proces wordt de stelling uiteindelijk opgenomen in het levende deel van de wiskunde en geniet hij het algemene vertrouwen. Het zojuist beschreven proces valt slechts een klein deel van de wiskundige productie ten deel, de gigantische hoeveelheid wiskunde die in tijdschriften, rapporten, preprints, etc. over de mensheid verspreid wordt maakt het onwaarschijnlijk dat alles als waardevol behouden zal worden. Het is zelfs onwaarschijnlijk dat het merendeel op waarde of zelfs waarheid getoetst zal worden.

Het sociale mechanisme van de wiskunde fungeert als een soort zeef die bepaalt wat tot het erkende deel van de wiskunde zal gaan behoren. Hoe gebrekkig zo'n mechanisme ook mag zijn (met name duiken er van tijd tot tijd verwaarloosde stellingen op die niet tijdig herkend waren), het is het normale middel om de vorm en inhoud van een wetenschap te bepalen.

Sinds enige tijd is er een nieuw aspect toegevoegd aan de wiskundige folklore; de computer heeft zijn medewerking verleend aan het bewijzen van stellingen. Als regel komt de computerbijdrage neer op het verrichten van bovenmenselijke hoeveelheden van verificaties en berekeningen. Het bekendste voorbeeld van zo'n computerbewijs is dat van het vierkleurenprobleem. Het verschil met de gangbare bewijzen 'met de hand' bestaat hieruit dat de computerbewijzen zich grotendeels aan de sociale controle onttrekken. De hele machinerie van lemma's, alternatieve bewijzen, generalisaties, enz. werkt hier niet (althans nog niet), de situatie is eerder te vergelijken met de fysica; het vervaardigen van een nieuw programma voor het bewijs kan vergeleken worden met het herhalen van een experiment. Ondanks alle lippendienst aan het wetenschappelijk ideaal is het herhalen van experimenten en het schrijven van nieuwe programma's eerder uitzondering dan regel. Maar zelfs al zou op ruime schaal software voor het herbewijzen van stellingen vervaardigd worden, de betrouwbaarheid van dergelijke programma's wordt niet altijd even hoog aangeslagen, bugs (fouten in het programma) blijven een voortdurende zorg.

Misschien is het echter zo dat computerbewijzen (van aanzienlijke omvang en complexiteit) nooit helemaal zullen overtuigen. Het is nu eenmaal een feit dat het begrijpen van bewijzen en stellingen eerder een kwestie is van inzicht in structuur van bewijzen, dan van de controle van hun lokale correctheid van bewijzen. Een kort bewijs m.b.v. de compactheidsstelling overtuigt nu eenmaal meer dan een bladzijdenlange exercitie met epsilons en deltas. Een computerbewijs staat en valt voorlopig met de vorm van de software; wanneer bewijzen door computers gegeven kunnen worden in een 'high-level' taal, vergelijkbaar met de gangbare taal van de wiskunde, dan is er enige kans dat men computerbewijzen op dezelfde voet zal accepteren als menselijke bewijzen, hoewel - men moet dan de inmiddels onzichtbaar geworden subniveaus met huid en haar slikken. Vooralsnog ziet het er naar uit dat de computerbewijzen tamelijk ver verwijderd zullen blijven van het hart van de wiskunde, men plaatst ze eerder aan de rand, in de buurt van de informatica en de experimentele wiskunde.

10. DE PRIJS IS HET BEWIJS.

Er zijn wiskundigen die een lage dunk hebben van een winkelketen die de hierboven staande slogan uitgevonden heeft; immers , hoe kan een prijs een bewijs zijn, en als het dan al een bewijs is, waar is het dan een bewijs van? De verontwaardiging is wel begrijpelijk, wij zijn gewend alleen redeneringen als bewijzen te aanvaarden. Toch ligt de zaak niet zo eenvoudig, er zijn bewijzen waarin nauwelijks een redenering te ontdekken valt. Iedereen kent de 'bewijzen' uit de goniometrie of differentiaal- en integraalrekening, waarin met grote volharding en slimheid integralen of goniometrische identiteiten door herleidingen uitgerekend worden. De informatica heeft het belang van dit soort procedures al enige tijd onderkend; er is een aparte studie van *herschrijfregels*. In de logica bestonden deze herschrijf praktijken allang, bijvoorbeeld in *equation calculi* of substitutie systemen.

Het redeneren in zijn traditionele vorm is bij zulke herleidingen vrijwel afwezig, kan men dan toch nog van 'bewijzen' spreken? Voor een deel is de beantwoording van deze vraag een kwestie van conventie, maar bij enig nadenken moet men constateren dat er geen inhoudelijke argumenten zijn om dit soort bewijzen niet als echt te erkennen. Aldus hebben wij hier een voorbeeld van 'bewijzen' die niet expliciet uit redeneringen bestaan. Het is nu nog maar een kleine stap om ook andere soorten 'bewijzen' te aanvaarden. Om een voorbeeld te noemen, het bewijs van de uitspraak "er zijn oneindig veel priemgetallen" kan een redenering zijn, maar het kan net zo goed een constructie zijn die bij ieder natuurlijk getal n een priemgetal bepaalt dat groter is dan n. Zo'n constructie kan zeer wel als bewijs van de gegeven uitspraak opgevat worden; sterker nog, in bepaalde stromingen binnen de wiskunde worden juist constructies beschouwd als de bewijzen bij uitstek! Nu is het een kleine stap om uit te komen bij de titel van deze paragraaf uit te komen. Immers als constructies als bewijzen aanvaard worden, dan ontkomt men er niet aan om ook ingewikkelder constructies toe te laten, bijvoorbeeld constructies die op constructies werken.Maar dan moet men ook constructies in beschouwing nemen die helemaal niets doen (constante constructies, denk aan functies) en die kan men gevoegelijk opvatten als - of zelfs identificeren met - getallen.

Nu blijft nog de vraag wat de prijs eigenlijk bewijst. Wel, de normale gang van zaken is dat men uit een bewijs automatisch kan aflezen wat er bewezen wordt, meestal is de bewezen stelling de laatste regel van het bewijs. In het geval van "De prijs is het bewijs" ontbreekt kennelijk iets, er moet wat informatie bij. Wanneer, zoals tegenwoordig gebruikelijk is, de kassabon de code van het artikel bevat, dan weten we al veel meer; het geordende paar van de prijs en de code van het artikel levert ons de informatie die we nodig hebben om in te zien dat sprake is van 'een goede koop'. Wie bezwaren heeft tegen de bovenstaande excursie bedenke dat ook beroepswiskundigen uitspraken doen die enige welwillendheid van de toehoorder vragen: "het nulpunt is het bewijs", "de differentieerbaarheid is het bewijs".

Het bovenstaande is niet zomaar een uitstapje naar het rijk der fantasie, S.C. Kleene heeft al lang geleden een begrip geïntroduceerd dat getallen de rol laat spelen van bewijzen, de zg. *realizeerbaarheid* [TD].

De belangrijkste moraal is dat bewijzen vele gedaanten kunnen hebben - zij het dat de gangbare opvatting, "bewijzen = redeneren", in de praktijk de grootste rol speelt.

11. DIDACTIEK EN PRAKTIJK.

In het onderwijs bestaat geen apart vak "Bewijzen", er is zelfs geen speciaal hoofdstuk in de gangbare wiskundeboeken dat zich bezighoudt met het bewijzen. Er bestaan weliswaar allerlei boeken die de basisbegrippen van de wiskunde invoeren, met verlokkende titels in de trant van "The number system" of "Mathematical structures" en die als eerste hoofdstuk 'logica en verzamelingen' bevatten, maar daar wordt logica als een wiskundige discipline behandeld, die in feite al een vertrouwdheid met het bewijzen veronderstelt. Grootse ondernemingen als de *Elements* van Bourbaki beginnen met een eerste deel over logica en verzamelingen (en komen er vervolgens nooit meer op terug).

Er zijn enkele bezwaren tegen deze praktijk. In de eerste plaats komt een inleidend hoofdstuk "Logica" neer op het spannen van een paard voor een reeds rijdende auto; de student weet allang (of, hoort allang te weten) *hoe* je bewijst en van zo'n hoofdstuk leert hij niet "het bewijzen", zoals hij een nieuw vak als bv. topologie leert. In de tweede plaats is de suggestie die van zo'n hoofdstuk uitgaat, nl. dat van nu af aan de schrijver, en dus de lezer, zijn bewijzen zal opschrijven als waren het logische afleidingen onrealistisch . De techniek en de kneepjes, en bovenal de zinvolheid en noodzaak van het bewijzen leert men in de wiskunde zelf. Nu is het in de loop der jaren het niet gemakkelijker geworden om in het secundaire onderwijs de bewijspraktijk te oefenen. De verschuiving van de wiskundige mode van de meetkunde naar de algebra/analyse, laten we zeggen van het meetkundige naar het numerieke, heeft een bijbehorende verschuiving van propositielogica naar predicatenlogica veroorzaakt.

Wie de oudere leerboeken over de meetkunde bekijkt, de oude planimetrie, zal zien dat quantoren nauwelijks een rol spelen. Men moet wel van tijd tot tijd een hulplijn trekken ("er is minstens één lijn die....") en men bewijst dat alle punten op de bisectrix even ver van beide benen liggen, maar daar blijft het bij. Meestal komt men wel toe met de keuze van een willekeurig punt of een willekeurige lijn. De voornaamste bewijstechnieken in de elementaire meetkunde komen uit de propositie logica. Het conscientieus behandelen van een stuk elementaire meetkunde levert als uitermate nuttig bijprodukt een bruikbare praktische vaardigheid in het bewijzen in vereenvoudigde, schematische situaties. Misschien hangt de langdurige succesvolle carrière van de Aristotelische logica wel samen met de dominerende positie die de Euclidische meetkunde in het onderwijs bleef innemen, lang nadat de analyse en algebra volwassen geworden waren.

De beoefening van de analyse, differentiaal- en integraalrekening, eist een ingewikkelder logisch apparaat. Definities als die van "differentieerbaarheid", "convergentie", "uniforme convergentie" confronteren ons met quantorenwisselingen en -combinaties die in de meetkunde niet van nature optreden. Ook hier geldt een vuistregel die bij de meetkunde van toepassing was: oefen en demonstreer het gebruik van quantoren en hun regels in realistische situaties. Met name is het van belang om het gebruik van quantoren zo natuurlijk mogelijk te doen verlopen; er is niets tegen het gebruik van "een willekeurig positief getal a" of "een willekeurige differentieerbare functie", de analyse van zulke begrippen kan men rustig aan de logica overlaten, maar de motivatie komt uit de praktijk van de wiskunde!

Gezien de moeilijkheden die verbonden zijn met het juist hanteren van quantoren en hun combinaties (denk aan de ontstaansgeschiedenis van het begrip uniforme convergentie), kan men zich afvragen hoe zo'n esoterisch vak als analyse ooit van de grond gekomen is. Misschien is dat wel te verklaren door de techniek van de infinitesimalen, die - zoals bekend - het quantorgebruik vereenvoudigt, en voor een deel zelfs overbodig maakt. Hoe dat ook zijn moge, onze taak is het om 'de quantor te geven wat des quantors is'.

Is het voorafgaande nu een pleidooi om maar helemaal van de logica als funderende-hygiënische discipline af te zien? In het geheel niet! Logica, logische technieken, bewijsmethoden hebben een terechte plaats in het wiskunde onderwijs en in de wiskundepraktijk, maar : alles op zijn tijd.

De meest wenselijke volgorde van het opbouwen van een 'bewijs attitude' is de volgende

(1) *Het aanleren van bewijzen in de wiskundige praktijk.* Hierbij kan men met vrucht het logische symbolenapparaat invoeren, zij het dan louter als handige notatie. Dit stadium is nog geheel informeel; de nadruk ligt op het leren "aanvoelen" van de bewijstechnieken.

(2) *Een analyse van de reeds verworven bewijstechnieken.* In dit stadium is een zekere mate van formalisering noodzakelijk, al was het alleen maar omdat een zinvolle analyse reeds moet plaatsvinden op een hoog niveau van precisie. Men moet echter nauw voeling houden met de wiskunde zelf, veel voorbeelden en vooral tegenvoorbeelden. In het boek "De taal van de wiskunde" van R.P. Nederpelt is een exemplarische uitwerking van zo'n analyse gegeven, compleet met verfijningen die bepaalde vereenvoudigingen van het redeneren leveren (bv. descriptie, λ-operator,typering, context).

Na stadium (2) is er een splitsing, men kan afzien van verdere toepassing van het logisch arsenaal, of men kan de logica - hetzij met het oog op toepassingen, hetzij als zelfstandige discipline, hetzij als grondslag van de wiskunde - verder bestuderen.

(3a) *Genoeg is genoeg.* Wie de logische methodologie in de zin van (2) onder de knie heeft kan voorlopig uit de voeten. In de praktijk zal men zelden (semi) formele redeneringen opzetten à la "De taal van de wiskunde", maar het is van belang dat men althans zijn argumentatie met een redelijke precisie kan presenteren wanneer men ter verantwoording geroepen wordt. De wiskundige praktijk bestaat nu eenmaal uit een groot aantal dooddoeners als "men ziet eenvoudig dat", "de lezer kan gemakkelijk controleren dat", "it is obvious that", "it follows by well-known techniques". Op zichzelf is dit niet laakbaar, zolang men de ontbrekende stappen maar kan invullen.

(3b) *Logica als vak.* Onder dit hoofd valt een veelheid van richtingen, die niet zo direct aan te geven zijn. Zelfs het "Handbook of Mathematical Logic" en het "Handbook of Philosophical Logic" behandelen maar een bescheiden deel van de logica. In ieder geval vallen onder dit hoofd alle "meta-stellingen", zoals de stellingen van Gödel, Skolem-Löwenheim, Herbrand, Gentzen en vele anderen. Onder het hoofd "Logica" vallen semantische onderzoekingen, bewijstheorie,verzamelingsleer, algorithmen, categorische methoden, etc.

Bovendien valt onder dit hoofd een nieuwere tak van de logica, de z.g. *toegepaste logica* die zich verhoudt tot de zuivere logica zo ongeveer als de experimentele natuurkunde tot de theoretische natuurkunde. De toepassingen vallen binnen een groot aantal disciplines, maar vooral op het gebied van de informatica zijn de toepassingen verrassend en veelvuldig. De informatica heeft het belang van de logica na enig aarzelen erkend door het gebied als 'Grondslagen van de Informatika" in te lijven.

In hoeverre kan de wiskundige en informaticus voorbijgaan aan (3b)? Dat hangt voor een groot deel af van het specifieke onderwerp waarin men werkt. Er zijn delen van de wiskunde waarin extra kennis van de theoretische logica geen enkele voorsprong geeft, maar er zijn andere delen waarin men zonder logische en meta-logische apparatuur niet ver komt. Kortom, het nut van een verdere studie van de logica hangt sterk van de context af.

Globaal gezien komt een typisch logische training pas ter discussie in een vrij laat stadium van de wiskundige opvoeding. In de allereerste plaats moet men langs natuurlijke wegen een vanzelfsprekende waardering en instelling van de leerling ten opzichte van het bewijzen kweken; de normale wiskundestof geeft daar meer dan genoeg gelegenheid toe. Met enige nadruk op *natuurlijk*; men kan het gebruik van logica ook demonstreren aan het type logische puzzles dat vooral door Raymond Smullyan zo populair geworden is, maar dan is er een levensgroot risico dat logica en "bewijzen" door de leerling alleen maar gezien wordt als een uiterst gezochte aangelegenheid, iets dat zozeer op grappige en vooral gezochte situaties slaat dat het niet als normaal gezien wordt. Bovendien zijn dit soort logische puzzles verre van triviaal, het risico bestaat dat de leerling er eerder door afgeschrikt wordt. Kortom, Smullyan is eerder stof voor hen die al weten waar logica en bewijzen goed voor is en die smaak hebben voor leuke problemen.

In de tweede plaats is een verdere analyse van en bezinning op bewijstechnieken een belangrijk desideratum. Aan de hand van zo'n verdieping van het logisch inzicht kan men een precisie bereiken die voor de dagelijkse wiskunde ruim voldoende is.

Literatuur

[C] R.L. Constable et al. *Implementing Mathematics with the Nuprl Proof Development System*. Prentice-Hall, Englewood Cliffs, New Jersey. 1986

[D1] D. van Dalen. *Filosofische grondslagen van de wiskunde*.Van Gorcum, Assen. 1978

[D2] D.van Dalen. *Logic and Structure* (2nd ed) Springer Verlag,Berlin. 1983.

[F] G. Frege. *Grundgesetze der Arithmetik, begriffsschriftlich abgeleitet*. Jena.1893,1903.

[G] G. Gentzen. *Collected Papers*. (ed. M. Szabo). North-Holland Publ.Co.,Amsterdam. 1969.

[J] T. Jech About the axiom of choice. In *Handbook of Mathematical Logic*, Ed. J. Barwise. North-Holland Publ. Co.,Amsterdam. 1977. 345-370.

[K] S. Kripke. *Wittgenstein on rules and private language*. Blackwell, Oxford.1982.

[L] I. Lakatos. *Proofs and Refutations*, Cambridge University Press, Cambridge.1976.

[N] R.P. Nederpelt. *De taal van de Wiskunde*. Versluys, Almere. 1987.

[P] B. Pascal. *On geometrical demonstration* in Pascal. Encyclopaedia Britannica, Inc.Chicago. 1952.

[Pr] D.Prawitz *Natural Deduction*, Almquist & Wiksell. 1956.Uppsala,

[S] R. Smullyan. *The lady or the tiger?* Pelican Books, Harmondsworth. 1982.

[Su1] G.Sundholm. Systems of deductions. In *Handbook of Philosophical Logic*, Vol.I (eds.D.Gabbay, F.Guenthner), Reidel,Dordrecht. 1983, pp.133-188

[Su2] G.Sundholm. Proof Theory and Meaning. In *Handbook of Philosophical Logic*, Vol..III (eds. D.Gabbay, F.Guenthner),Reidel, Dordrecht. 1986, pp.471-506.

[T-D] A.S. Troelstra, D. van Dalen. *Constructivism in Mathematics.I,II.* North-Holland Publ. Co. Amsterdam. 1988.

HOOFDSTUK III

MACHINALE VERIFICATIE VAN REDENERINGEN

Een beschrijving van het AUTOMATH project

N.G. de Bruijn

vertaald en bewerkt door P.W.H. Lemmens

1. MOTIVATIE EN ACHTERGRONDEN.

In deze bijdrage beschrijven we het AUTOMATH-project. We doen dat in twee gedeelten. In dit eerste deel zullen we het voornamelijk hebben over motivatie en achtergronden. In het tweede deel geven we een voorbeeld. In beide gevallen zullen we niet al te diep ingaan op de taal AUTOMATH zelf. Voor meer uitgebreide details aangaande de definitie van AUTOMATH verwijzen we naar [2], [5] en vooral [10]. Voor het eerste deel is [4] als voornaamste bron gebruikt. Ook zijn stukken ingevoegd uit [3] en [5].

Laten we meteen vaststellen dat AUTOMATH een wiskundige taal is en geen programmeertaal. Niettemin hebben die twee soorten talen veel gemeenschappelijk en kan men in beide gevallen met vrucht gebruik maken van constructies en ideeën uit de andere groep.

Het AUTOMATH-project is ontstaan in 1966. Het uitgangspunt was de wens om een taal te ontwikkelen waarin hele wiskundige theorieën op zo'n preciese manier kunnen worden opgeschreven dat de juistheid door een automaat kan worden vastgesteld, terwijl de taal toch nauw verband moest houden met de manier waarop een wiskundig werk gewoonlijk wordt geschreven. De funktie van de automaat is die van een "listening machine", een zeer kritische luisteraar of lezer, die verifieert of het betoog verloopt volgens nauwkeurig vastgelegde afleidingsregels. Om die taak te kunnen uitvoeren moet de taal zeker een formele taal zijn.

Mogelijk had Leibniz ook een idee voor een dergelijke taal in gedachten, maar dat werd niet ontwikkeld doordat er in die tijd geen ervaring bestond in formele talen.

Het idee is een zodanige taal te maken, dat alles wat we daarin syntactisch correct opschrijven te interpreteren is als correcte wiskunde. Onder syntactisch correct verstaan we hier: correct volgens de grammaticale regels van de taal, daarbij inbegrepen correcte verwijzingen naar dingen die eerder zijn gezegd. Dit zou bijvoorbeeld het schrijven van een uitgebreide wiskundige encyclopedie kunnen zijn, waaraan iedereen (mensen, maar ook machines) mag bijdragen wat hij wil, en elke bijdrage die syntactisch wordt geaccepteerd veilig kan worden gebruikt door anderen. Het idee van een geformaliseerde encyclopedie was al opgekomen bij, en gedeeltelijk uitgevoerd door G. Peano rond 1900, maar dat was nog verre van wat automatisch leesbaar mag heten.

Om het nog iets duidelijker te maken stellen we ons een zeer uitgebreid boek voor over (bijvoorbeeld) complexe funktietheorie, dat geen voorkennis veronderstelt. Het begint dus met hoofdstukken over logica en afleidingsregels, verzamelingenleer, getalsystemen, wat meetkunde en topologie, enzovoorts, en er wordt nooit iets gebruikt dat niet afgeleid is in het boek, tenzij het expliciet is opgeschreven als axioma. Verder veronderstellen we dat het boek geschreven is zonder een enkel hiaat. Niets wordt overgelaten aan de lezer.

De opdracht van het verifiëren op syntactische juistheid kan worden overgelaten aan een computer. Omdat het verifiëren alleen de vraag betreft of de tekst is geschreven volgens de voorschriften, moeten we toegeven dat de taak van het verifiëren net zo menselijk is als de taak van het schrijven van de tekst. Toch hebben we het idee van een computer vastgehouden om een norm te stellen: wat een computer niet kan doen, kan niet automatisch worden genoemd. Bovendien hebben computers enkele praktische voordelen ten opzichte van mensen. Zij nemen alle details serieus en worden nooit moe. De menselijke schrijver is geneigd om zo nu en dan enkele details te veranderen in het geloof dat zulks geen consequenties heeft in andere gedeelten van de tekst; in dit opzicht is de computer meedogenloos.

De snelheid van de computer is nauwelijks een probleem, omdat we er niet veel meer van verwachten dan wat een menselijke schrijver kan doen. De problemen waarmee we wel te maken hebben, betreffen de organisatie van het geheugen in de hedendaagse computersystemen. De wiskundige heeft verschillende soorten geheugens: snelle en langzame gedeelten van de hersenen, het vel papier waarop hij aan het werken is, zijn eigen recente aantekeningen, de boeken op zijn bureau, de bibliotheek van zijn instituut, en tenslotte andere bibliotheken die hij kan raadplegen als de bibliotheek van zijn instituut niet toereikend is. Vergelijkbaar hiermee kan het geheugen van het computersysteem naast het interne geheugen nog bestaan uit schijven, etc. Zowel in het geval van de mens als in dat van de machine moet de gebruiker beslissen wat waar op te slaan. In het geval van de computer is het zeer wel mogelijk dat technologische verbeteringen van grote en snelle geheugens in de toekomst een oplossing zullen bieden voor deze opslagproblemen.

Men moet in het oog blijven houden dat het raamwerk der geformaliseerde wiskundige redeneringen niet hetzelfde is als "de wiskunde". De computer die de geformaliseerde redeneringen heeft doorgewerkt en beaamd, heeft er nog bitter weinig van begrepen. Hij zal misschien in staat zijn het gelezene te onthouden en later te gebruiken om nieuwe teksten te keuren, maar hij heeft niets begrepen van motiveringen en interpretaties. Men zal hem misschien met enige moeite wat creatief vermogen kunnen geven, maar hij zal daarbij niet geleid worden door ideeën uit de aanschouwingswereld, en evenmin door smaak of gevoel voor waarde. Het geformaliseeerde raamwerk is slechts een armzalig deel der wiskunde; de neergeschreven redenering is de afsluiting van het denkproces, en niet het denkproces zelf.

Het werk aan de ontwikkeling van AUTOMATH heeft nieuwe gezichtspunten geopend op de fundamenten van de wiskunde, zeker wat betreft de structuur ervan. Er bestaat een populair geloof (niet gedeeld door de schrijver), dat een geheel bevredigende basis voor wiskunde moeilijk of helemaal niet bereikt kan worden. De Principia Mathematica (1910-1913) van A.N.Whitehead (1861-1947) en B.A.W.Russell (1872-1970) droeg tot dit geloof bij (omdat de Principia Mathematica te ingewikkeld is). En het was moeilijk geworden door G.Cantor's (1845-1918) alephs (dit is een brij van taal en metataal). Nu, aan het eind van de twintigste eeuw, is het Paradijs van Cantor vrij algemeen aanvaard. Mogelijk zullen de wiskundigen van de eenentwintigste eeuw echter vinden dat het ondanks haar schoonheid een wankele basis voor de wiskunde is.

Zeker zal de taal van de wiskunde in de toekomst veranderen. De Grieken bestudeerden in de oudheid geometrische figuren. Geometrische figuren vormen echter slechts een povere benadering van een wiskundige taal. Van der Waerden [21] merkt op dat de Grieken ondanks hun inventiviteit werden gehinderd bij verdere ontwikkelingen door hun notatie voor de gehele getallen (daardoor hadden ze niet genoeg symbolen meer over). Een van de grootste verdiensten van de Arabieren was de invoering van letter-variabelen. Toen de moderne algebraïsche notatie in Europa bekend werd, was R. Descartes (1596-1650) in staat om de meetkunde in deze nieuwe taal te "formaliseren". Zelfs de ontwikkeling van de decimale notatie vergemakkelijkte al de verbreiding van een stuk wiskunde. Wellicht zit er een moraal in het verhaal van het gebrek aan een goede taal voor de Griekse wiskundigen. G.W. Leibniz's droom van een universele wetenschappelijke taal waarin denken wordt vervangen door rekenen is een uitbreiding van Descartes' gedachte.

G. Boole (1815-1864) ging uit van een soortgelijk idee. Hij ontwikkelde een taal voor een stuk logica, maar zijn werk had geen raakvlakken met de gewone wiskunde van zijn tijdgenoten. De zeer uitgebreide taal van Whitehead en Russell waarin logica en wiskunde verenigd zijn, en de grootse structuur ervan, hebben we reeds eerder genoemd. Ook het werk van G. Peano (1858-1932) is al eerder ter sprake geweest.

L.E.J. Brouwer (1881-1966), L. Kronecker (1823-1891) en H. Weyl (1885-1955) verwierpen de gedachte dat de wiskunde geheel zou kunnen worden geformaliseerd. Cantor's theorieën gaven aanleiding tot veel paradoxen, waarvan sommige (zoals Russell's paradox) nieuwe definities noodzakelijk maakten. Het is geenszins zeker dat er geen nieuwe tegenstrijdigheden meer zullen opduiken. Brouwer was een voorstander van constructivisme, maar zijn publicaties geven de indruk dat het hem aan een goede taal mankeerde om zijn kritiek te uiten. Brouwer's intuïtionisme leek erg veel ingewikkelde redeneringen te veroorzaken, en kreeg daarom niet veel steun. Recentelijk heeft E. Bishop [1] nieuw leven geblazen in de ideeën van Brouwer.

Direct vanaf het begin was het maken van iets universeels een van de doelstellingen bij het AUTOMATH-project. Dit is een nadeel ten opzichte van systemen die slechts kleine stukken wiskunde beogen te bewerken, zoals propositionele logica, predikatenlogica, etc. De voorwaarde van universaliteit heeft tot gevolg dat er geen resultaten verwacht mogen worden op het gebied van het vinden van bewijzen van stellingen. Dat onderwerp (theorem proving) is zo moeilijk dat het alleen kans van slagen kan hebben in die situaties waar de problemen en de methoden zich afspelen in een zeer beperkt gebied, en waar de taal en de syntactische analyse precies toegesneden zijn op de situatie. Sedert 1960 hebben John McCarthy, J.A. Robinson [19], J.B. Rosser, Hao Wang en anderen zich geworpen op het machinaal bewijzen van stellingen. Hun algoritmen leiden tot bewijzen die in het algemeen weinig overeenkomst vertonen met bewijzen die een wiskundige zou leveren. De voortgang sinds 1970 is weinig indrukwekkend. Wel wordt met vrucht gebruikt gemaakt van de mogelijkheid om een "theorem prover" de details te laten invullen van een bewijs waarvan men zelf de grote lijn aangeeft. Aan de hand van de respons van de machine is het dan vaak mogelijk om het bewijs te verbeteren of duidelijker te maken (zie [24]).

AUTOMATH is een taal waarin we boeken kunnen schrijven die bestaan uit opeenvolgende stukken tekst die men "zinnen" zou kunnen noemen. De syntactische correctheid van een zin hangt af van de vorige zinnen. Voorlopig zijn we voornamelijk geïnteresseerd in boeken die vrijwel zin voor zin lijken op een gewone mathematische tekst, en zullen we ons niet bezighouden met de formulering van gedachten die een menselijke wiskundige niet zou hebben.

We moeten ons realiseren dat geen enkele taal alle mathematische aktiviteit kan omvatten. Taal en notatie mogen van invloed zijn op het krijgen van ideeën, maar het zou de wiskunde dood maken als we zouden eisen dat ook het ontstaan van ideeën uitsluitend binnen een strak geformaliseerde taal moet kunnen worden beschreven. In het bijzonder is er niet veel uitzicht op de mogelijkheid om geometrische of fysische intuïtie te vangen in een operationeel formeel kader. Puur taalkundig bezien lijkt het al moeilijk om duidelijke natuurlijke taal te vervangen door iets formelers. Psychologisch houdt het begrijpen van wiskunde gewoonlijk meer in (soms echter minder) dan het controleren op correctheid: het zien van een mathematische situatie die harmonisch past bij reeds vertrouwde situaties kan het gevoel van een gerust geweten teweeg brengen. Men veronderstelt dat hierbij ook het onderbewustzijn een rol speelt.

Zelfs als we geen volledige formalisering willen, maar bij iedere stap slechts gewone, betrouwbare wiskunde, dan al zouden we hele stukken wiskunde om zeep brengen, zeker in de eerste stadia van de ontwikkeling ervan. Belangrijke stukken wiskunde zijn ontstaan op basis van fundamentele fouten of door het invullen van wezenlijke gedeelten voorlopig te vergeten. Zonder te weten welke mooie dingen er daarmee te beleven zijn, zou men nooit de energie hebben kunnen opbrengen of methoden hebben ontwikkeld om de fout of het hiaat te herstellen en zo indeıdaad aan de overzijde te komen. In bepaalde gevallen is het voor de wiskunde goed geweest dat men pas inzag dat er een fout of een hiaat was, nádat men uitvoerige ervaring had opgedaan met het nieuwe materiaal.

Laten we eens proberen het produceren van volledig geformaliseerde wiskunde te beschrijven als een soort produktieproces. Met als uiteindelijke doel het maken van een AUTOMATH-boek, onderscheiden we de volgende fasen:

(i) mathematische ideeën,

(ii) formele definities en bewijzen,

(iii) een erg precies gedetailleerde beschrijving hiervan,

(iv) een boek in een tussen-taal,

(v) een AUTOMATH-boek.

We hebben (iv) ingevoegd omdat AUTOMATH niet zo gemakkelijk te schrijven is, wegens zijn universaliteit. Het meeste wiskundige materiaal betreft slechts een klein gedeelte van de wiskunde, met algemeen bekende tradities over afkortingen en bondige formuleringen. Boeken van type (iii) zijn geschreven in wat we een probleem-gerichte taal zouden kunnen noemen.

Wat voor soort mensen hebben we nodig voor dit produktieproces? Voor het scheppen van (i) moeten we de Grote Wiskundige hebben (hiermee bedoelen we niet een speciale wiskundige van topklasse: elke wiskundige kan zo nu en dan groot zijn). Om van (i) naar (ii) te komen hebben we de Goede Wiskundige nodig, die het gebied en de daarin gebruikte technieken beheerst.

De fasen (i) en (ii) hebben vanzelfsprekend niets van doen met AUTOMATH; ze spelen zich af binnen de gewone wiskundige praktijk.

Om het produkt van (ii) geheel in de bij (iii) gewenste vorm te brengen is een Competent Wiskundige nodig. Ook hij moet het onderwerp kennen, in ieder geval moet hij om kunnen gaan met de gebruikelijke afkortingen die daarin worden gebezigd.

De overgangen van (iii) naar (iv), van (iv) naar (v) en de uiteindelijke verificatie van (v) kunnen worden gedaan door goedkope krachten. Veel hiervan, vooral de verificatie van (v), kan worden overgelaten aan erg goedkope arbeid in de vorm van een computer.

Er zijn veel dingen die het gebruik van een universele taal zoals AUTOMATH zou kunnen bewerkstelligen. Sommige hiervan zijn op zichzelf geen voldoende motivatie voor het AUTOMATH-project, maar de totaliteit ervan lijkt belangrijk genoeg om de moeite waard te zijn. We doelen op twee groepen: *verifiëren* en *begrijpen.*

Wanneer we "verifiëren" zeggen, dan is het eerste waar we aan denken het controleren van lange moeizame bewijzen, waarin de ketting net zo zwak is als de zwakste schakel, en waarbij vaak de betrouwbaarheid van het bewijs niet wordt ondersteund door intuïtie of ervaring. In het bijzonder kan men zulke situaties verwachten in gecompliceerde combinatorische problemen waarbij een groot aantal gevallen en daar weer subgevallen van moeten worden nagegaan. In deze klasse vinden we ook problemen over de semantiek van computerprogramma's, specificatie versus uitvoering: doet een programma wat er van wordt beloofd? Het aantal elementaire bewerkingen dat gedaan wordt en de hoeveelheid administratie die bijgehouden moet worden kunnen zo groot zijn dat menselijke methoden erg onbetrouwbaar worden. In dit kader moeten we ook aandacht schenken aan de problemen die de samenwerking van mensen met mensen enerzijds en mensen met machines anderzijds met zich brengt. In beide gevallen is een strak communicatieschema noodzakelijk. Het lijkt de moeite waard om in dit gebied onderzoek te verrichten, omdat geweldig grote sommen geld worden uitgegeven aan computersoftware en omdat het zeker van belang is te weten te komen wat daarvan betrouwbaar is en wat niet.

Laten we nu eens kijken naar dingen die vallen onder de term "begrijpen". Allereerst merken we op dat alleen al het hebben van een vaste goed gedefinieerde taal voor de wiskunde een voordeel op zichzelf is. Het maakt het ons mogelijk om mathematische gesprekken te verdelen in (i) het zeggen van dingen in de taal, (ii) het bediscussiëren hoe dingen in de taal worden gezegd, en (iii) het verbinden van dingen die in de taal worden gezegd met dingen uit een andere wereld, zoals gewone wiskunde, fysische realiteit, etc. Aan (ii) kunnen we het begrip "meta-taal", en aan (iii) het begrip "interpretatie" verbinden.

De meeste wiskundigen hebben geen duidelijk idee over de fundamenten van hun eigen vak. Dit is misschien gedeeltelijk de schuld van de logici die, ten gevolge van het vinden van veel interessante technische problemen in hun vak, hun oorspronkelijke opdracht, het bouwen van een fundament, hebben verwaarloosd. Veel wiskundigen hebben een vaag denkbeeld dat predikaten-logica plus verzamelingentheorie een complete basis vormen voor hun eigen werk, maar wanneer ze dieper ingaan op deze gebieden dan ontdekken ze tot hun verrassing dat logica en verzamelingentheorie ook bestaan uit mathematische aktiviteit! In plaats van het vinden van een fundament voor het mathematische patroon axioma's - definities - afleidingsregels - bewijzen - stellingen, lijkt het wel of overal datzelfde patroon weer opduikt. Wat ontbreekt is een goede taal. In feite wordt dit in AUTOMATH heel duidelijk. Deze taal bevat nauwelijks iets dat logica genoemd kan worden, en wanneer we eenmaal beschikken over AUTOMATH en daarin dingen correct (syntactisch gezien) zeggen, dan is de vraag naar wat axioma's, afleidingsregels, definities, veronderstellingen, stellingen, etcetera zijn, een vraag in de metataal. Het antwoord op die vraag is afhankelijk van de interpretatie. Of we iets een definitie of een stelling of iets anders noemen heeft geen enkel effect op de resultaten van een AUTOMATH-boek: zoals het er staat is het simpelweg correct.

Een ander oogmerk in de richting van "begrijpen" is de analyse van complexiteit. Sommige zaken zijn moeilijker dan andere, en een volledig formele presentatie kan dat duidelijk maken. Het is mogelijk om stukken wiskunde te klassificeren naar hun "diepte". De wiskunde van de 19-de eeuw was zeker dieper dan die van de 18-de eeuw. Enigszins schetsmatig kan men stellen dat men in de 18-de eeuw wel kon spreken over funkties die expliciet geconstrueerd waren, maar dat men niet kon zeggen "zij f een funktie", omdat het woord "funktie" toen tot de meta-taal behoorde. Zo zou men ook kunnen zeggen dat 18-de eeuwse wiskunde in het algemeen kan worden beschreven in PAL, de subtaal van AUTOMATH die we krijgen door de lambda-calculus uit AUTOMATH weg te laten.

In dit verband kan nog worden opgemerkt dat AUTOMATH de historische volgorde geweld aandoet. Al in PAL worden zulke zaken als "bewijzen" behandeld op dezelfde manier als dingen zoals "getallen", terwijl zelfs in de tweede helft van de 20-ste eeuw de meeste wiskundigen het gevoel hebben dat een "bewijs" een begrip is uit de meta-taal en dat een "getal" een "object" is. De ideeën over wat een object is en wat niet, zijn gewoonlijk vaag. Het verschil tussen objecten en niet-objecten loopt blijkbaar parallel aan het onderscheid tussen taal en meta-taal: men vindt dat een object iets is dat met een symbool kan worden aangeduid. Veel mensen geloven dat het beter is om te praten over verzamelingen dan over predikaten. In plaats van te zeggen dat x voldoet aan het predikaat P, vormen ze de verzameling van alle dingen die aan dat predikaat voldoen, en zeggen dan dat x tot die verzameling behoort. Misschien wordt dit veroorzaakt doordat men predikaten niet als objecten wenst te zien. Velen vatten het begrip predikaat op als iets uit de syntax, "een logische uitdrukking".

Terugkomend op "begrijpen": dikwijls is al gezegd dat wiskunde wordt onderwezen door intimidatie en geleerd door imitatie. De enige manier om uit te vinden in welke mate dit waar is, is alles te coderen in een erg strakke taal.

Tenslotte kan men onder het kader "begrijpen" nog de invloed rekenen die elke nieuwe notatie kan hebben op de ontwikkeling van de wiskunde, om het even of om zo'n invloed gevraagd is of niet.

Behalve "verifiëren" en "begrijpen" zijn er enkele praktische voordelen verbonden aan het feit dat machines kunnen omgaan met de wiskunde die we maken. Bijvoorbeeld kunnen we ons voorstellen dat we aan een machine een boek geven over analytische getaltheorie en vragen: "Ik ben alleen geïnteresseerd in de Priemgetalstelling. Druk alles af wat nodig is voor deze stelling en laat al het andere weg" (Sommigen beweren dat E.Landau zo'n machine was; hij schreef zijn boeken op die manier). Of we kunnen zeggen: "Druk Stelling 325 af, en vanaf het allereerste begin alle definities die nodig zijn om te lezen wat de stelling zegt". In dit geval zullen ook alle bewijzen worden weggelaten.

Om iets te laten zien van hoe een wiskundige redenering er uitziet in een AUTOMATH-boek, moeten we een beetje uitleg geven over de taal. Eerst merken we op dat die boeken zijn gestructureerd in geneste "blokken" van zinnen: twee blokken liggen òf geheel buiten elkaar, òf een ervan ligt geheel binnen het andere. De eerste zin van een blok heeft een speciale vorm. De interpretatie ervan is dat we een variabele introduceren die binnen het blok mag worden gebruikt, of dat een veronderstelling wordt gemaakt die in het hele blok als een waarheid wordt behandeld. Buiten het blok is de variabele niet beschikbaar, en is de veronderstelling krachteloos.

De zinnen hebben alle de vorm:

> "In de context A wordt de naam B gedefinieerd door C en dat heeft type D".

Hierin is B een nieuwe identificator, een naam die niet in eerdere regels is gebruikt. In elke zin wordt dus één nieuwe naam geïntroduceerd. Men kan deze namen vrij kiezen, mits onderling verschillend. C en D zijn expressies (uitdrukkingen), op voorgeschreven wijze opgebouwd uit eerder ingevoerde identificatoren en een aantal verbindingen zoals haakjes, streepjes, komma's etc. Sommige zinnen (de blokopeners) hebben alleen maar een streep (—) op de plaats van C (interpretatie: hier wordt een variabele ingevoerd door hem een naam te geven en te zeggen welk type hij heeft). In iedere zin is de A de string van eerder ingevoerde blokopenende en nog niet afgedankte identificatoren. De A-stukken van de zinnen tonen de blokstruktuur van het boek. Voor iedere zin correspondeert dat A-deel met het nest van blokken dat die zin omvat.

Soms is de C geen uitdrukking, maar het speciale tweeletterig symbool "PN". De zinnen waarin het C-deel PN is, dienen voor het invoeren van primitieve begrippen, die niet worden gedefinieerd. Deze dingen krijgen alleen een naam en een type, maar geen definitie; desalniettemin kunnen ze van dan af aan worden gebruikt. Een "PN-zin" is geen blokopener, hij komt zomaar ergens in een blok voor.

We moeten nog de mogelijkheid vermelden dat het D-deel van een zin geen expressie is, maar het vierletterig symbool "TYPE". Zulke zinnen introduceren een nieuw type d.m.v. een definitie, of d.m.v. het opvoeren van een variabele, of d.m.v. het invoeren van een primitief begrip. Dit gebeurt dus weer in drie vormen: het C-deel is een expressie, of een streep of PN.

Het bovenstaande beschrijft ruwweg de struktuur van de taal PAL, die we eerder hebben genoemd. De talen van de AUTOMATH-familie ontstaan uit PAL door het toevoegen van een soort getypeerde lambda-calculus. Daarop gaan we hier niet in.

We zeggen een paar dingen over de interpretatie. Ten eerste is de context (het A-deel) iets wat gewoonlijk in de wiskunde niet expliciet wordt opgeschreven. Iets ervan kan worden afgeleid uit bijvoorbeeld de indeling in hoofdstukken en paragrafen, andere stukken van de context kunnen worden opgespoord door de voorgaande tekst nauwgezet te lezen. Het B-deel heeft de vertrouwde betekenis van het geven van een naam aan een nieuw object dat we maken of veronderstellen. De interpretatie van de C- en D-delen is zoals we hebben beschreven: B wordt gedefinieerd door C en dat heeft type D. Laten we hier voor deze typering even het symbool ":" gebruiken, dus $C : D$. In de natuurlijke taal zeggen we dingen als "3 is een getal", maar omdat het woord "is" wordt gebruikt voor veel verschillende dingen, geven we de voorkeur aan "3 : getal".

Sommige van de typen die we zullen gebruiken hebben een interpretatie die op die van verzamelingen lijkt. In plaats van "3 : getal" zou men kunnen denken aan "$3 \in \mathbf{N}$", maar we moeten echt oppassen ":" niet te verwarren met "$\in$". In AUTOMATH is het type van een ding C (dus de D met $C : D$) uniek bepaald, en kan worden achterhaald door middel van een algoritme. Met $3 \in \mathbf{N}$ is dat niet het geval, omdat $3 \in S$ geldt voor iedere verzameling die 3 bevat (bijv. $3 \in \{1, 2, 3\}$).

Er zijn ook andere typen dan die welke op verzamelingen lijkende interpretaties hebben. De meest belangrijke zijn de propositionele typen. In overeenstemming met deze interpretatie, correspondeert het type D met een propositie p, en het C-deel met een bewijs voor p. Met de bewijzen kunnen we manipuleren: als ze afhangen van variabelen dan mogen we voor die variabelen expressies substitueren, op dezelfde manier als dat gebeurt bij objecten die van variabelen afhangen. Dit heeft tot gevolg dat een gemodificeerd bewijs (gemodificeerd door substituties) wordt geaccepteerd als een bewijs voor de bijbehorende gemodificeerde propositie. Merk op dat het B-deel van de zin een naam is voor het bewijs C, en niet voor de met D samenhangende propositie. De zin kan een stelling genoemd worden; later kan die stelling worden toegepast door te refereren aan B. Merk ook op dat het merendeel van de stelling-zinnen alleen maar hulpstappen zijn die uiteindelijk leiden naar één belangrijke stelling-zin, die een wiskundige pas echt een stelling zou noemen; hij zou het niet de moeite waard vinden om de andere zinnen zelfs maar lemma's te noemen.

Er zijn ook blok-openers met een propositionele interpretatie. Dat zijn zinnen die lijken op: "zij x een bewijs voor de propositie p". Deze zinnen introduceren dus aannamen die in het hele blok geldig zijn. En er kunnen zinnen zijn waarin het C-deel PN is. Deze maken het mogelijk om de geldigheid van een propositie in te voeren als een axioma. Dit zijn de drie typen propositionele zinnen: stellingen, veronderstellingen en axioma's.

Als we dat willen, kunnen we nieuwe typen creëren, en ook mogen we interpretaties kiezen. Bijvoorbeeld: als we een mathematische theorie willen maken over constructies met passer en lineaal in de vlakke meetkunde, dan hoeven we niet persé de moeizame weg te nemen van het coderen van constructies als verzamelingen (passend bij het dogmatisch idee dat alles een verzameling is; voor kritiek verwijzen we naar [7]), maar we kunnen ook direct een type "constructie" introduceren.

Iets dergelijks zou men ten aanzien van computerprogramma's kunnen doen. Voor iedere verzameling Ω introduceren we een type "programma(Ω)". We interpreteren C : programma(Ω) als "C is een programma dat werkt op de toestandsruimte Ω". Met PN-zinnen voeren we primitieve programma's in en construeren daaruit grotere programma's uit kleinere componenten. Met andere woorden, we beschrijven de syntax van een programmeertaal in hetzelfde boek waarin de logica en de wiskunde staat (tussen de laatste twee is geen essentieel verschil). Vervolgens kunnen we, in hetzelfde boek, axioma's ontwikkelen over de primitieve begrippen van de programmeertaal. En we kunnen, weer in hetzelfde boek, allerlei stellingen afleiden zoals logische stellingen (afgeleide afleidingsregels), mathematische stellingen, semantische stellingen, speciale programma's, en semantische resultaten over die programma's. De verschillende stukken kunnen door elkaar gevlochten zijn. Zo kan een wiskundige behandeling van de grootste gemene deler bijvoorbeeld voorkomen in een getaltheorisch kader, maar ook als een beschrijving van een computerprogramma om de grootste gemene deler te bepalen, met daarbij een bewijs dat het computerprogramma termineert en inderdaad de waarde van de getaltheoretische funktie g.g.d. oplevert (zie [8] voor expliciete en uitvoerige voorstellen omtrent de semantische behandeling van ALGOL-achtige talen). Het zou geen kwaad kunnen om de syntax en de semantiek van twee verschillende programma's te behandelen in één boek, en in dat boek te bewijzen dat programma P_1 in taal Q_1 hetzelfde semantisch effect heeft als programma P_2 in taal Q_2. Dit soort bewijzen kunnen lang zijn en veel precies peuterwerk vragen. Toch zijn ze vaak belangrijk, en het zijn typisch gevallen waar automatische verificatie op haar plaats is.

Wanneer we een boek zoals boven beschreven, in verband brengen met de buitenwereld, dan zijn er vele mogelijkheden voor interpretatie. Zolang we geen verder formalisme hebben om met interpretatie om te gaan, moeten we onszelf ervan "overtuigen" dat de primitieve begrippen (het doet er niet toe van welke aard ze zijn: logisch, wiskundig, syntactisch of semantisch) uitdrukken wat ze geacht worden te betekenen in de buitenwereld. En we moeten onszelf ervan "overtuigen" dat de interpretaties van de primitieven weer interpretaties induceren van het verdere materiaal, en dat interpretaties van de eindresultaten mogelijk zijn zonder de stukken van het boek tussen de primitieven en die eindresultaten te interpreteren. Dan zijn we er zeker van dat de interpretaties van de eindresultaten mathematisch correct zijn.

Bij computertalen is de interpretatie complexer dan bij gewone wiskundige teksten, maar toch niet essentieel verschillend ervan. Interpretatie blijft altijd gebeuren op een nogal intuïtieve basis, zolang de "buitenwereld" niet volledig is geformaliseerd.

Tot besluit van dit eerste deel geven we een overzicht van wat er is bereikt door de AUTOMATH-groep aan de Technische Universiteit Eindhoven, waar het AUTOMATH-project tot ongeveer 1976 financieel ondersteund is door Z.W.O. (nu N.W.O.).

(i) Er zijn programma's gemaakt die talen verifiëren, en die zijn nu beschikbaar in interactieve vorm. Teksten kunnen zin voor zin worden aangeboden aan de machine, die reageert binnen ten hoogste een paar seconden. Als het programma een zin niet accepteert, krijgt men een complete diagnose over gemaakte fouten. Deze diagnose stelt degene die de tekst intikt gewoonlijk in staat om deze te verbeteren, eventueel na (bijvoorbeeld telefonisch) overleg met de wiskundige die de tekst heeft gemaakt. De interactieve mogelijkheden van de nu werkende versies zijn minder uitgebreid dan die van het oorspronkelijke programma, dat heeft gewerkt van 1975 tot 1988 en intensief is gebruikt.

(ii) Wat het theoretische werk over de talen uit de AUTOMATH-familie betreft, zijn bijna alle doelstellingen gerealiseerd (zie vooral [11] en [15]). Opgemerkt moet worden, dat er enige overlap is met werk van anderen ([12], [13]) die onafhankelijk de logica hebben geïnterpreteerd in termen van getypeerde lambda-calculus, ongeveer tegelijk met de start van het AUTOMATH-project. Van later werk moet vooral [14] genoemd worden.

(iii) Om het geheel uit te proberen is E.Landau's "Grundlagen der Analysis" vertaald. Dit is gedaan door L.S. van Benthem Jutting. Bij deze vertaling [18] is geen poging ondernomen om de tekst ten behoeve van een vergemakkelijkte vertaling anders in te delen. Men heeft daarentegen Landau's tekst zo precies mogelijk gevolgd, alle nadelen daarvan op de koop toenemend. We hopen dat de zo verkregen ervaring van dienst zal zijn bij de beslissing welke tussen-taal het meest geschikt is voor meer algemeen gebruik.

2. EEN VOORBEELD VAN EEN AUTOMATH-TEKST

We geven een voorbeeld van een stukje wiskunde dat niet al te triviaal is, niet al te moeilijk, en tegelijk toch niet overbekend. Bovendien speelt "logica" eigenlijk geen rol in dit voorbeeld. Het onderwerp komt uit de algebra, en behandelt de condities die voldoende zijn opdat een gegeven algebraïsch systeem een commutatieve groep is (met optelling als groepsoperatie). Dit blijkt gemakkelijker te worden door in plaats van optelling uit te gaan van aftrekking. De condities worden dan eenvoudige identiteiten, en er is niet meer zoiets als de eenduidige oplosbaarheid van de vergelijking $a + x = b$. Wanneer we uitgaan van de aftrekking, dan zijn het bestaan van een element 0 met

$$\begin{aligned} &\text{axiomaA}(x): \quad x - 0 = x \\ &\text{axiomaB}(x): \quad x - x = 0 \end{aligned}$$

en de algemene regel

$$\text{axiomaC}(x, y, z): \quad x - (y - z) = z - (y - x)$$

voldoende (mits we de rol van de gelijkheidsaxioma's even vergeten) om de groepseigenschappen te verifiëren van de optelling, die wordt gedefinieerd door

$$\text{definitie}(x, y): \quad x + y = x - (0 - y).$$

Zo bewijst men de commutativiteit van de optelling met de redenering

$$\begin{aligned} &x + y = x - (0 - y) \quad \{\text{definitie}(x, y)\} \\ &x - (0 - y) = y - (0 - x) \quad \{\text{axiomaC}(x, 0, y)\} \\ &y - (0 - x) = y + x \quad \{\text{definitie}(y, x)\} \end{aligned}$$

Dit kunnen we samenvatten in het resultaat

$$\text{commutatief}(x, y): \quad x + y = y + x$$

Vervolgens kan de associativiteit worden bewezen door

$(x+y)+z = (x-(0-y))+z \quad \{\text{definitie}(x,y)\}$
$(x-(0-y))+z = (x-(0-y))-(0-z) \quad \{\text{definitie}((x-(0-y)),z)\}$
$(x-(0-y))-(0-z) = z-(0-(x-(0-y))) \quad \{\text{axiomaC}((x-(0-y)),0,z)\}$
$z-(0-(x-(0-y))) = z-((0-y)-(x-0)) \quad \{\text{axiomaC}(0,x,(0-y))\}$
$z-((0-y)-(x-0)) = z-((0-y)-x) \quad \{\text{axiomaA}(x)\}$

Nu merken we op dat we in de voorgaande zinnen bewezen hebben

$$\text{lemma}(x,y,z): \quad (x+y)+z = z-((0-y)-x)$$

en gaan weer verder met

$z-((0-y)-x) = x-((0-y)-z) \quad \{\text{axiomaC}(z,(0-y),x)\}$
$x-((0-y)-z) = (z+y)+x \quad \{\text{lemma}(z,y,x)\}$
$(z+y)+x = x+(z+y) \quad \{\text{commutatief}((z+y),x)\}$
$x+(z+y) = x+(y+z) \quad \{\text{commutatief}(z,y)\}$

Hiermee is bereikt

$$\text{associatief}(x,y,z): \quad (x+y)+z = x+(y+z).$$

We hebben bovenstaande bewijzen expres al zo geformuleerd dat ze een beetje gaan lijken op de manier waarop AUTOMATH werkt. Maar het is nog lang niet precies genoeg. Zo moet de vertaling in AUTOMATH ook zinnen bevatten waarin expliciet staat dat uit $a=b$ en $b=c$ volgt $a=c$. Bovendien hebben we in een van de zinnen uit het bewijs opgeschreven

$$z-(0-(x-(0-y))) = z-((0-y)-(x-0)) \quad \{\text{axiomaC}(0,x,(0-y))\}.$$

Voor de lezer is het duidelijk dat we axiomaC hebben toegepast op een term uit het linkerlid, en hij ziet onmiddellijk welke term het betreft. Voor een computer is dat niet zo vanzelfsprekend. We kunnen het hem gemakkelijker maken door de volgende verfijningen

$$\text{axiomaD}(x,y,z): \quad \text{als } x=y, \text{ dan } z-x=z-y$$

$0-(x-(0-y)) = (0-y)-(x-0) \quad \{\text{axiomaC}(0,x,(0-y))\}$
$z-(0-(x-(0-y))) = z-((0-y)-(x-0))$
$\{\text{axiomaD}((0-(x-(0-y))),((0-y)-(x-0)),z)\}$

Maar nu zitten we nog met het probleem dat AUTOMATH moet gaan zoeken in de tekst naar de zinnen die bepaalde veronderstellingen waar maken. Dit kan allemaal worden opgelost door elke zin een identificator mee te geven, en veronderstellingen als parameters op te nemen. Het ligt dan ook tamelijk voor de hand om $x-y$ te schrijven als diff(x,y) en $x+y$ als sum(x,y) en $a=b$ als IS(a,b).

We presenteren nu een stukje uit een AUTOMATH-boek waarin uitgaand van de equivalentierelatie "IS" (zinnen 6, 7, 9, 13) en van de volgende axioma's voor "diff"

ax1: als $x=y$, dan $x-z=y-z$ (zin 14)
ax2: als $x=y$, dan $z-x=z-y$ (zin 15)

ax3: $x - 0 = x$ (zin 16)
ax4: $x - x = 0$ (zin 17)
ax5: $x - (y - z) = z - (y - x)$ (zin 18),

over "sum" wordt bewezen:

th1: als $x = y$, dan $x + z = y + z$ (zin 21)
th2: als $x = y$, dan $z + x = z + y$ (zin 23)
th3: $x + 0 = x$ (zin 25)
th4: $x + y = y + x$ (zin 26)
th5: $(x + y) + z = x + (y + z)$ (zin 52)
th6: $y + (x - y) = x$ (zin 66)
th7: als $y + z = x$, dan is $z = x - y$ (zin 80)

Merk op dat de axioma's A t/m D uit de inleiding respectievelijk overeenkomen met ax3, ax4, ax5, ax2, dat de commutativiteit uitgedrukt wordt door th4 en de associativiteit door th5.

De stellingen th1 en th2 laten zien dat de optelling goed is gedefinieerd. In feite is "=" een equivalentierelatie, en de optelling moet daarmee compatibel zijn. Voor de aftrekking wordt het compatibel zijn met "=" geëist in de axioma's ax1 en ax2.

De stellingen th6 en th7 geven samen de eenduidige oplosbaarheid naar z van $y + z = x$, immers th6 zegt "$z = x - y$ is een oplossing", en th7 zegt "als z een oplossing is dan geldt $z = x - y$".

De nummers van de zinnen zijn slechts toegevoegd ten behoeve van de bespreking. In AUTOMATH zijn deze nummers overbodig, want elke zin wordt uniek bepaald door zijn identificator. We herinneren nog even aan de syntax van een zin in AUTOMATH: context, identificator, definitie (bewijs), type (propositie). Als scheidingstekens hiertussen gebruiken we respectievelijk "#", ":=" en ":".

Om het herhalen van de soms lange contexten te vermijden, geven we van elke context alleen de laatste variabele, de z.g. context-indicator aan. Als de context bijvoorbeeld $x : A,\ y : B,\ z : C$ is, behoeven we slechts de context-indicator z te vermelden. In de zin waar z is opgevoerd, is C en ook y te lezen, in de zin waar y is opgevoerd, is ook B en x te lezen, enz. Zo zijn uit de context-indicatoren de contexten te reconstrueren.

In het begin voorzien we de AUTOMATH-tekst van tamelijk uitvoerig commentaar. Na afloop zullen we nog enige algemene opmerkingen maken.

(1) — # real := PN : TYPE

Eerst wordt het type "real" ingevoerd. Het is een primitief begrip (PN), we weten er nog niets van. Al het nodige moet nog bekend worden gemaakt. We kunnen "real" interpreteren als de verzameling van de reële getallen, maar even goed is de interpretatie als een willekeurige groep. Tenslotte is "real" slechts een naam.

(2) — # 0 := PN : real

0 is geen variabele, maar een constante van het type real.

(3) — # x := — : real
(4) x # y := — : real

x en y zijn variabelen van het type real. Omdat we het later vaak zullen hebben over "operaties" die van x en y afhangen, voeren we y in binnen de context van x. Als we dan in het vervolg iets willen zeggen over x en y, hoeven we alleen y als context-indicator op te geven. Daarmee behoort dan ook x tot de context.

(5) y # diff := PN : real

"diff" is gedefinieerd met y als context-indicator, dus de context van diff is x,y (in deze volgorde). Diff is iets dat afhangt van x en y, en dat iets van het type real "oplevert". Wanneer we het type "real" interpreteren als de verzameling van de reële getallen, dan is diff(x,y) een reëel getal.

(6) y # IS := PN : TYPE

Deze "IS" is een "propositioneel type", liever gezegd een "bewijsklasse". (Vaak wordt de typering van IS aangegeven met IS: PROP in plaats van IS: TYPE; hier zullen wij dat niet doen.)

IS heeft x,y als context. We merken op dat er niet eerst een propositie is ingevoerd waarvan IS(x,y) de bewijsklasse is. In ons verhaal is het niet nodig die propositie (we bedoelen de propositie x=y) een naam te geven. Weer moet uit nader te formuleren eigenschappen blijken dat IS(x,y) te interpreteren valt als het type van alle bewijzen voor x=y.

(7) x # refl := PN : IS(x,x)

IS wordt aangeroepen in een andere context (namelijk die van alleen x) dan waarin IS gedefinieerd is (die van x,y). In deze context heeft IS zonder meer geen betekenis. Daarom moet IS expliciet verschijnen als IS(x,x), zodat we weten welke expressies zijn gesubstitueerd voor de parameters x en y van IS. De checker controleert of deze substituties toegelaten zijn (aantal en type).

"refl" is een axioma over IS.

(8) y # u := — : IS(x,y)

Hier wordt een variabele u ingevoerd. De interpretatie ervan is, dat in de context u de propositie IS(x,y) waar is. Eigenlijk is u dus de naam van een veronderstelling. De context van u is x,y, dus is het hier in feite niet nodig om expliciet IS(x,y) te schrijven.

(9) u # symm := PN : IS(y,x)

"symm" is het tweede axioma over IS. De context-indicator is u, dus de context is x,y,u. Nu moet wel expliciet IS(y,x) worden geschreven, want IS zonder meer zou IS(x,y) betekenen. Interpretatie: onder de veronderstelling u (IS(x,y)) geldt IS(y,x).

(10) y # z := — : real
(11) z # v := — : IS(x,y)
(12) v # w := — : IS(y,z)
(13) w # trans := PN : IS(x,z)

Het derde en laatste axioma over IS. De context is x,y,z,v,w (ga na). Onder de veronderstellingen IS(x,y) en IS(y,z) geldt IS(x,z). Uit refl (7), symm (9) en trans blijkt dat IS een equivalentierelatie is. De variabele v is van hetzelfde type (is dezelfde propositie) als u. Wegens de geneste structuur is het nodig om v apart in te voeren. Een andere mogelijkheid zou zijn geweest

(10) u # z := — : real
(12) z # w := — : IS(y,z)
(13) w # trans := PN : IS(x,z)

De context van "trans" is dan x,y,u,z,w. Nu besparen we een zin (11), maar dat is slechts een zeer tijdelijk voordeel. Immers, we zullen vaak uitspraken willen doen over x,y,z zonder u te veronderstellen. Dat zou alleen kunnen als we dan een nieuwe variabele z' declareren in de context x,y. Bovendien is het bovenstaande alternatief slecht te lezen omdat daarin de parameters van trans ongeordend zijn naar hun type.

(14) v # ax1 := PN : IS(diff(x,z),diff(y,z))
(15) v # ax2 := PN : IS(diff(z,x),diff(z,y))
(16) x # ax3 := PN : IS(diff(x,0),x)
(17) x # ax4 := PN : IS(diff(x,x),0)
(18) z # ax5 := PN : IS(diff(x,diff(y,z)),diff(z,diff(y,x)))

De axioma's voor diff. Merk op dat ax1 en ax2 de context x,y,z,v hebben. Daarbij wordt dus IS(x,y) verondersteld. De axioma's ax1 en ax2 zeggen dat diff compatibel is met de equivalentierelatie IS.

(19) y # sum := diff(x,diff(0,y)) : real

De definitie van "sum".

(20) — # lem1 := ax3(0) : IS(diff(0,0),0)
(21) v # th1 := ax1(x,y,diff(0,z),v) : IS(sum(x,z),sum(y,z))
(22) v # lem2 := ax2(x,y,0,v) : IS(diff(0,x),diff(0,y))
(23) v # th2 := ax2(diff(0,x),diff(0,y),z,lem2) : IS(sum(z,x),sum(z,y))
(24) x # lem3 := ax2(diff(0,0),0,x,lem1) : IS(sum(x,0),diff(x,0))
(25) x # th3 := trans(sum(x,0),diff(x,0),x,lem3,ax3(x)) : IS(sum(x,0),x)
(26) y # th4 := ax5(x,0,y) : IS(sum(x,y),sum(y,x))

Een aantal lemma's en stellingen over sum. Hier ziet men erg duidelijk hoe AUTOMATH functioneert. We illustreren dat aan th2.

th2 (23) zegt IS(sum(z,x),sum(z,y)), en is gesteld in de context x,y,z,v, dus onder de veronderstelling IS(x,y). Het bewijs daarvan krijgen we door in ax2 (15) voor de parameters x,y,z,v de aangegeven substituties in te vullen.

Doen we dit, dan ontstaat IS(diff(z, diff(0,x)), diff(z, diff(0,y))) uit ax2. Deze expressie is inderdaad tekstueel gelijk aan de expressie die uit IS(x,y) ontstaat door sum(z,x) voor x en sum(z,y) voor y te substitueren volgens de definitie van sum (19).

Voor de parameter v in ax2 moeten we lem2 substitueren; v is van type IS(x,y) en dat gaat bij de substitutie van diff(0,x) voor x en diff(0,y) voor y inderdaad over in het type van lem2.

(27) z # r1 := diff(x,diff(0,y)) : real
(28) z # r2 := diff(0,r1) : real
(29) z # r3 := diff(diff(0,y),diff(x,0)) : real
(30) z # r4 := diff(diff(0,y),x) : real
(31) z # lem4 := ax5(0,x,diff(0,y)) : IS(r2,r3)
(32) z # lem5 := ax2(diff(x,0),x,diff(0,y),ax3(x)) : IS(r3,r4)
(33) z # lem6 := trans(r2,r3,r4,lem4,lem5) : IS(r2,r4)
(34) z # r5 := sum(sum(x,y),z) : real
(35) z # lem7 := ax5(r1,0,z) : IS(r5,diff(z,r2))
(36) z # r6 := diff(z,r4) : real
(37) z # lem8 := ax2(r2,r4,z,lem6) : IS(diff(z,r2),r6)
(38) z # r7 := diff(x,diff(diff(0,y),z)) : real
(39) z # lem9 := trans(r5,diff(z,r2),r6,lem7,lem8) : IS(r5,r6)
(40) z # lem10 := ax5(z,diff(0,y),x) : IS(r6,r7)
(41) z # lem11 := trans(r5,r6,r7,lem9,lem10) : IS(r5,r7)
(42) z # r8 := sum(sum(z,y),x) : real
(43) z # lem12 := lem9(z,y,x) : IS(r8,r7)
(44) z # lem13 := symm(r8,r7,lem12) : IS(r7,r8)

(45) z # lem14 := trans(r5,r7,r8,lem11,lem13) : IS(r5,r8)
(46) z # lem15 := th4(z,y) : IS(sum(z,y),sum(y,z))
(47) z # r9 := sum(sum(y,z),x) : real
(48) z # r10 := sum(x,sum(y,z)) : real
(49) z # lem16 := th1(sum(z,y),sum(y,z),x,lem15) : IS(r8,r9)
(50) z # lem17 := th4(sum(y,z),x) : IS(r9,r10)
(51) z # lem18 := trans(r5,r8,r9,lem14,lem16) : IS(r5,r9)
(52) z # th5 := trans(r5,r9,r10,lem18,lem17) :
IS(sum(sum(x,y),z),sum(x,sum(y,z)))
(53) y # r11 := diff(0,diff(x,y)) : real
(54) y # r12 := diff(y,diff(x,0)) : real
(55) y # lem19 := ax5(0,x,y) : IS(r11,r12)
(56) y # lem20 := ax2(diff(x,0),x,y,ax3(x)) : IS(r11,diff(y,x))
(57) y # lem21 := trans(r11,r12,diff(y,x),lem19,lem20) : IS(r11,diff(y,x))
(58) y # r13 := sum(y,diff(x,y)) : real
(59) y # r14 := diff(y,diff(y,x)) : real
(60) y # r15 := diff(x,diff(y,y)) : real
(61) y # lem22 := ax2(r11,diff(y,x),y,lem21) : IS(r13,r14)
(62) y # lem23 := ax5(y,y,x) : IS(r14,r15)
(63) y # lem24 := ax2(diff(y,y),0,x,ax4(y)) : IS(r15,diff(x,0))
(64) y # lem25 := trans(r13,r14,r15,lem22,lem23) : IS(r13,r15)
(65) y # lem26 := trans(r13,r15,diff(x,0),lem25,lem24) : IS(r13,diff(x,0))
(66) y # th6 := trans(r13,diff(x,0),x,lem26,ax3(x)) : IS(sum(y,diff(x,y)),x)
(67) z # r16 := sum(diff(0,y),sum(z,y)) : real
(68) z # lem27 := th6(z,diff(0,y)) : IS(r16,z)
(69) z # lem28 := symm(r16,z,lem27) : IS(z,r16)
(70) y # r17 := sum(diff(0,y),x) : real
(71) y # r18 := sum(x,diff(0,y)) : real
(72) y # lem29 := th4(diff(0,y),x) : IS(r17,r18)
(73) z # t := — : IS(sum(y,z),x)
(74) t # lem30 := trans(sum(z,y),sum(y,z),x,th4(z,y),t) : IS(sum(z,y),x)
(75) t # lem31 := th2(sum(z,y),x,diff(0,y),lem30) : IS(r16,r17)
(76) t # lem32 := trans(r16,r17,r18,lem31,lem29) : IS(r16,r18)
(77) t # lem33 := trans(z,r16,r18,lem28,lem32) : IS(z,r18)
(78) t # lem34 := lem33(x,y,diff(x,y),th6) : IS(diff(x,y),r18)
(79) t # lem35 := trans(diff(x,y),r18,z,lem34,symm(z,r18,lem33)) :
IS(diff(x,y),z)
(80) t # th7 := symm(diff(x,y),z,lem35) : IS(z,diff(x,y))

OPMERKINGEN

Altijd wanneer een identificator die geen variabele is, wordt aangehaald nadat er veranderingen van de context hebben plaatsgevonden, moet die identificator voorzien zijn van de nodige parameters, in aantal en respectievelijke typen overeenstemmend met de context waarin die identificator is gedeclareerd. Dit kan soms achterwege blijven, bijvoorbeeld wanneer er geen veranderingen in de context zijn geweest sinds de invoering van de identificator, en men niet expliciet andere parameters wil gebruiken. Dit laatste doet zich bijvoorbeeld voor in zin 43, waar lem9 wordt aangehaald met parameters (z,y,x). Zonder deze expliciete aanduiding zou lem9(x,y,z) bedoeld zijn, waarmee lem12 exact hetzelfde als lem9 zou zijn.

Merk ook op dat uit bovenstaand voorbeeld blijkt dat een AUTOMATH-boek geen van tevoren bepaalde vorm heeft. Zo is bijvoorbeeld het invoeren in zin 27 van r1, en verderop van r2, etc., louter gedaan om het voor de mens, die de tekst moet aanleveren, leesbaar te houden. Ook is het voordelig voor rekentijd en geheugen van de computer: lange uitdrukkingen kosten veel rekentijd en veel geheugen. Men zou zin 33 ook kunnen opschrijven zonder gebruik te maken van de zinnen 27 t/m 32. Hier kan persoonlijke smaak een rol spelen.

Een ander punt van smaak betreft de context. Het is niet zonder belang, voor mens en machine, dat de context zo eng mogelijk is. Dat heeft aan de ene kant het voordeel dat er geen overbodige veronderstellingen gemaakt worden (de zinnen zijn dan meer algemeen geldig), en aan de andere kant bespaart het de machine die de tekst moet verifiëren een hoop werk, want die zal van elke gebruikte identificator telkens weer nagaan of het type goed is, of de parameters passen etcetera.

In de inleiding tot dit voorbeeld hebben we slechts vier axioma's A, B, C, D genoemd voor "diff", terwijl de AUTOMATH-tekst er vijf bevat. Dat vijfde (als $x = y$ dan is $x - z = y - z$) speelde geen rol bij de in de inleiding besproken associativiteit. Maar ook voor de andere doeleinden is dat axioma niet echt nodig: ax1 (14) kan na zin 18 worden afgeleid uit de voorafgaande tekst van het AUTOMATH-boek. De preciese uitwerking laten we over aan de lezer.

Tenslotte merken we op dat de gepresenteerde tekst in feite is geschreven in PAL, de subtaal van AUTOMATH die we krijgen door de lambda-calculus uit AUTOMATH weg te laten. Men ziet hieruit dat PAL reeds in staat is het wezen van het wiskundige bedrijf (axioma's, definities, stellingen, bewijzen) te vatten. In zekere zin kan men zeggen dat de wiskunde van vóór 1800 in PAL kan worden uitgedrukt. Pas als men wil werken met variabelen die funkties voorstellen, heeft men bij formalisatie de behoefte aan lambda-calculus.

De oorsprong van het voorbeeld komt uit [6]. Een complete uitwerking in AUTOMATH van de theorie in [6] is gerealiseerd door J.T. Udding ([20]).

3. LITERATUUR

[1] Bishop, E., *Foundations of Constructive Analysis*, McGraw-Hill, 1967.

[2] de Bruijn, N.G., *The mathematical language AUTOMATH, its usage, and some of its extensions*, Symposium on Automatic Demonstration (Versailles, December 1968), Lecture notes in Mathematics, Vol. 125, pp. 29-61, Springer Verlag, 1970.

[3] de Bruijn, N.G., *Machinale Verificatie van Redeneringen*, Voordracht K.N.A.v.W., Verslag van de gewone vergadering der Afd. Natuurkunde, 78, No. 10, 1969.

[4] de Bruijn, N.G., *The AUTOMATH Mathematics Checking Project*, Proc. Symp. APLASM, Vol. 1, ed. P. Braffort, Orsay, France, 1973.

[5] de Bruijn, N.G., *AUTOMATH, a language for mathematics*, Notes (prepared by B. Fawcett) of a series of lectures in the Séminaire de Mathématiques Supérieures, Les Presses de l'Université de Montréal, 1971.

[6] de Bruijn, N.G., *Defining reals without the use of rationals*, Proc. Kon. Nederl. Akad. Wet. ser. A, 79 (= Indag. Math. 38), 100-108 (1976).

[7] de Bruijn, N.G., *Set theory with type restrictions*, In *Infinite and finite sets* ed. A.H. Hajnal, R. Rado, Vera T. Sós. Vol. I, pp. 205-214. North-Holland Publishing Company, Amsterdam, 1975.

[8] de Bruijn, N.G., *A system for handling syntax and semantics of computer programs in terms of the mathematical language AUTOMATH*, Rapport, Onderafdeling Wiskunde, Technische Universiteit, Eindhoven, 1973.

[9] de Bruijn, N.G., *A survey of the project AUTOMATH*, in *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, edited by J.P. Seldin and J.R. Hindley, pp. 579-606, Academic Press, 1980.

[10] van Daalen, D.T., *A description of AUTOMATH and some aspects of its language theory*, Proc. Symp. APLASM, Vol. 1, ed. P. Brafford, Orsay, France, 1973; herdrukt in Jutting [16].

[11] van Daalen, D.T., *The language theory of AUTOMATH*, Proefschrift, Technische Universiteit Eindhoven, 1980.

[12] Girard, J.Y., *Une extension de l'interprétation de Gödel à l'analyse, et son application à l'élimination des coupures dans l'analyse et la théorie des types*, Proc. 2nd Scandinavian Logic Symp. (editor Fenstad), North-Holland Publishing Company, Amsterdam, 1970.

[13] Howard, W.A., *The formulae-as-types notion of construction*, mimeographed in 1969. Herdrukt in: *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, edited by J.P. Seldin and J.R. Hindley, pp. 479-490, Academic Press, 1980.

[14] Martin-Löf, P., *An intuitionistic theory of types*, niet gepubliceerd, 1972.

[15] Nederpelt, R.P., *Strong normalization in a typed lambda calculus with lambda structured types*, Proefschrift, Technische Universiteit, Eindhoven, 1973.

[16] Jutting, L.S. van Benthem, *The development of a text in AUT-QE*, Proc. Symp. APLASM, Vol. 1, ed. P. Braffort, Orsay, France, 1973.

[17] Jutting, L.S. van Benthem, *Checking Landau's* Grundlagen *in the AUTOMATH system*, Proefschrift, Technische Universiteit Eindhoven 1977. Mathematical Centre Tracts nr. 83, Math. Centrum Amsterdam, 1979.

[18] Jutting, L.S. van Benthem, *A translation of Landau's* Grundlagen *in AUTOMATH*, vol. 1-5, Onderafdeling Wiskunde, Technische Universiteit Eindhoven, 1976.

[19] Robinson, J.A., *Theorem Proving on the Computer*, Journal ACM, 10 (1963), p.163.

[20] Udding, J.T., *A theory of real numbers and its presentation in AUTOMATH*, Afstudeerscriptie, Technische Universiteit Eindhoven, Onderafdeling Wiskunde, februari 1980, 3 delen, 1980.

[21] van der Waerden, B.L., *Science Awakening*, Groningen, 1961.

[22] Zandleven, I., *A verifying program for AUTOMATH*, Proc. Symp. APLASM, Vol. 1, ed. P. Braffort, Orsay, France, 1973.

[23] Zucker, J., *Formalization of classical mathematics in AUTOMATH*, In *Colloque International de Logique (Clermont-Ferrand 18-25 Juillet 1975)*. pp. 135-145, Ed. CNRS, Paris, 1977.

[24] Shankar, N., *Observations on the use of computers in proof checking*, Notices of the AMS, 34 (1988), 804-805.

Index

MC SYLLABI

1.1 F. Göbel, J. van de Lune. *Leergang besliskunde, deel 1: wiskundige basiskennis.* 1965.

1.2 J. Hemelrijk, J. Kriens. *Leergang besliskunde, deel 2: kansberekening.* 1965.

1.3 J. Hemelrijk, J. Kriens. *Leergang besliskunde, deel 3: statistiek.* 1966.

1.4 G. de Leve, W. Molenaar. *Leergang besliskunde, deel 4: Markovketens en wachttijden.* 1966.

1.5 J. Kriens, G. de Leve. *Leergang besliskunde, deel 5: inleiding tot de mathematische besliskunde.* 1966.

1.6a B. Dorhout, J. Kriens. *Leergang besliskunde, deel 6a: wiskundige programmering 1.* 1968.

1.6b B. Dorhout, J. Kriens, J.Th. van Lieshout. *Leergang besliskunde, deel 6b: wiskundige programmering 2.* 1977.

1.7a G. de Leve. *Leergang besliskunde, deel 7a: dynamische programmering 1.* 1968.

1.7b G. de Leve, H.C. Tijms. *Leergang besliskunde, deel 7b: dynamische programmering 2.* 1970.

1.7c G. de Leve, H.C. Tijms. *Leergang besliskunde, deel 7c: dynamische programmering 3.* 1971.

1.8 J. Kriens, F. Göbel, W. Molenaar. *Leergang besliskunde, deel 8: minimaxmethode, netwerkplanning, simulatie.* 1968.

2.1 G.J.R. Förch, P.J. van der Houwen, R.P. van de Riet. *Colloquium stabiliteit van differentieschema's, deel 1.* 1967.

2.2 L. Dekker, T.J. Dekker, P.J. van der Houwen, M.N. Spijker. *Colloquium stabiliteit van differentieschema's, deel 2.* 1968.

3.1 H.A. Lauwerier. *Randwaardeproblemen, deel 1.* 1967.

3.2 H.A. Lauwerier. *Randwaardeproblemen, deel 2.* 1968.

3.3 H.A. Lauwerier. *Randwaardeproblemen, deel 3.* 1968.

4 H.A. Lauwerier. *Representaties van groepen.* 1968.

5 J.H. van Lint, J.J. Seidel, P.C. Baayen. *Colloquium discrete wiskunde.* 1968.

6 K.K. Koksma. *Cursus ALGOL 60.* 1969.

7.1 *Colloquium moderne rekenmachines, deel 1.* 1969.

7.2 *Colloquium moderne rekenmachines, deel 2.* 1969.

8 H. Bavinck, J. Grasman. *Relaxatietrillingen.* 1969.

9.1 T.M.T. Coolen, G.J.R. Förch, E.M. de Jager, H.G.J. Pijls. *Colloquium elliptische differentiaalvergelijkingen, deel 1.* 1970.

9.2 W.P. van den Brink, T.M.T. Coolen, B. Dijkhuis, P.P.N. de Groen, P.J. van der Houwen, E.M. de Jager, N.M. Temme, R.J. de Vogelaere. *Colloquium elliptische differentiaalvergelijkingen, deel 2.* 1970.

10 J. Fabius, W.R. van Zwet. *Grondbegrippen van de waarschijnlijkheidsrekening.* 1970.

11 H. Bart, M.A. Kaashoek, H.G.J. Pijls, W.J. de Schipper, J. de Vries. *Colloquium halfalgebra's en positieve operatoren.* 1971.

12 T.J. Dekker. *Numerieke algebra.* 1971.

13 F.E.J. Kruseman Aretz. *Programmeren voor rekenautomaten; de MC ALGOL 60 vertaler voor de EL X8.* 1971.

14 H. Bavinck, W. Gautschi, G.M. Willems. *Colloquium approximatietheorie.* 1971.

15.1 T.J. Dekker, P.W. Hemker, P.J. van der Houwen. *Colloquium stijve differentiaalvergelijkingen, deel 1.* 1972.

15.2 P.A. Beentjes, K. Dekker, H.C. Hemker, S.P.N. van Kampen, G.M. Willems. *Colloquium stijve differentiaalvergelijkingen, deel 2.* 1973.

15.3 P.A. Beentjes, K. Dekker, P.W. Hemker, M. van Veldhuizen. *Colloquium stijve differentiaalvergelijkingen, deel 3.* 1975.

16.1 L. Geurts. *Cursus programmeren, deel 1: de elementen van het programmeren.* 1973.

16.2 L. Geurts. *Cursus programmeren, deel 2: de programmeertaal ALGOL 60.* 1973.

17.1 P.S. Stobbe. *Lineaire algebra, deel 1.* 1973.

17.2 P.S. Stobbe. *Lineaire algebra, deel 2.* 1973.

17.3 N.M. Temme. *Lineaire algebra, deel 3.* 1976.

18 F. van der Blij, H. Freudenthal, J.J. de Iongh, J.J. Seidel, A. van Wijngaarden. *Een kwart eeuw wiskunde 1946-1971, syllabus van de vakantiecursus 1971.* 1973.

19 A. Hordijk, R. Potharst, J.Th. Runnenburg. *Optimaal stoppen van Markovketens.* 1973.

20 T.M.T. Coolen, P.W. Hemker, P.J. van der Houwen, E. Slagt. *ALGOL 60 procedures voor begin- en randwaardeproblemen.* 1976.

21 J.W. de Bakker (red.). *Colloquium programmacorrectheid.* 1975.

22 R. Helmers, J. Oosterhoff, F.H. Ruymgaart, M.C.A. van Zuylen. *Asymptotische methoden in de toetsingstheorie; toepassingen van naburigheid.* 1976.

23.1 J.W. de Roever (red.). *Colloquium onderwerpen uit de biomathematica, deel 1.* 1976.

23.2 J.W. de Roever (red.). *Colloquium onderwerpen uit de biomathematica, deel 2.* 1977.

24.1 P.J. van der Houwen. *Numerieke integratie van differentiaalvergelijkingen, deel 1: eenstapsmethoden.* 1974.

25 *Colloquium structuur van programmeertalen.* 1976.

26.1 N.M. Temme (ed.). *Nonlinear analysis, volume 1.* 1976.

26.2 N.M. Temme (ed.). *Nonlinear analysis, volume 2.* 1976.

27 M. Bakker, P.W. Hemker, P.J. van der Houwen, S.J. Polak, M. van Veldhuizen. *Colloquium discretiseringsmethoden.* 1976.

28 O. Diekmann, N.M. Temme (eds.). *Nonlinear diffusion problems.* 1976.

29.1 J.C.P. Bus (red.). *Colloquium numerieke programmatuur, deel 1A, deel 1B.* 1976.

29.2 H.J.J. te Riele (red.). *Colloquium numerieke programmatuur, deel 2.* 1977.

30 J. Heering, P. Klint (red.). *Colloquium programmeeromgevingen.* 1983.

31 J.H. van Lint (red.). *Inleiding in de coderingstheorie.* 1976.

32 L. Geurts (red.). *Colloquium bedrijfsystemen.* 1976.

33 P.J. van der Houwen. *Berekening van waterstanden in zeeën en rivieren.* 1977.

34 J. Hemelrijk. *Oriënterende cursus mathematische statistiek.* 1977.

35 P.J.W. ten Hagen (red.). *Colloquium computer graphics.* 1978.

36 J.M. Aarts, J. de Vries. *Colloquium topologische dynamische systemen.* 1977.

37 J.C. van Vliet (red.). *Colloquium capita datastructuren.* 1978.

38.1 T.H. Koornwinder (ed.). *Representations of locally compact groups with applications, part I.* 1979.

38.2 T.H. Koornwinder (ed.). *Representations of locally compact groups with applications, part II.* 1979.

39 O.J. Vrieze, G.L. Wanrooy. *Colloquium stochastische spelen.* 1978.

40 J. van Tiel. *Convexe analyse.* 1979.

41 H.J.J. te Riele (ed.). *Colloquium numerical treatment of integral equations.* 1979.

42 J.C. van Vliet (red.). *Colloquium capita implementatie van programmeertalen.* 1980.

43 A.M. Cohen, H.A. Wilbrink. *Eindige groepen (een inleidende cursus).* 1980.

44 J.G. Verwer (ed.). *Colloquium numerical solution of partial differential equations.* 1980.

45 P. Klint (red.). *Colloquium hogere programmeertalen en computerarchitectuur.* 1980.

46.1 P.M.G. Apers (red.). *Colloquium databankorganisatie, deel 1.* 1981.

46.2 P.G.M. Apers (red.). *Colloquium databankorganisatie, deel 2.* 1981.

47.1 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60: general information and indices.* 1981.

47.2 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 1: elementary procedures; vol. 2: algebraic evaluations.* 1981.

47.3 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 3A: linear algebra, part I.* 1981.

47.4 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 3B: linear algebra, part II.* 1981.

47.5 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 4: analytical evaluations; vol. 5A: analytical problems, part I.* 1981.

47.6 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 5B: analytical problems, part II.* 1981.

47.7 P.W. Hemker (ed.). *NUMAL, numerical procedures in ALGOL 60, vol. 6: special functions and constants; vol. 7: interpolation and approximation.* 1981.

48.1 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). *Colloquium complexiteit en algoritmen, deel 1.* 1982.

48.2 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). *Colloquium complexiteit en algoritmen, deel 2.* 1982.

49 T.H. Koornwinder (ed.). *The structure of real semisimple Lie groups.* 1982.

50 H. Nijmeijer. *Inleiding systeemtheorie.* 1982.

51 P.J. Hoogendoorn (red.). *Cursus cryptografie.* 1983.

CWI SYLLABI

1 Vacantiecursus 1984: *Hewet - plus wiskunde.* 1984.

2 E.M. de Jager, H.G.J. Pijls (eds.). *Proceedings Seminar 1981-1982. Mathematical structures in field theories.* 1984.

3 W.C.M. Kallenberg, et al. *Testing statistical hypotheses: worked solutions.* 1984.

4 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 1.* 1984.

5 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 2.* 1984.

6 P.J.M. Bongaarts, J.N. Buur, E.A. de Kerf, R. Martini, H.G.J. Pijls, J.W. de Roever. *Proceedings Seminar 1982-1983. Mathematical structures in field theories.* 1985.

7 Vacantiecursus 1985: *Variatierekening.* 1985.

8 G.M. Tuynman. *Proceedings Seminar 1983-1985. Mathematical structures in field theories, Vol.1 Geometric quantization.* 1985.

9 J. van Leeuwen, J.K. Lenstra (eds.). *Parallel computers and computations.* 1985.

10 Vacantiecursus 1986: *Matrices.* 1986.

11 P.W.H. Lemmens. *Discrete wiskunde: tellen, grafen, spelen en codes.* 1986.

12 J. van de Lune. *An introduction to Tauberian theory: from Tauber to Wiener.* 1986.

13 G.M. Tuynman, M.J. Bergvelt, A.P.E. ten Kroode. *Proceedings Seminar 1983-1985. Mathematical structures in field theories, Vol.2.* 1987.

14 Vacantiecursus 1987: *De personal computer en de wiskunde op school.* 1987.

15 Vacantiecursus 1983: *Complexe getallen.* 1987.

16 P.J.M. Bongaarts, E.A. de Kerf, P.H.M. Kersten. *Proceedings Seminar 1984-1986. Mathematical structures in field theories, Vol.1.* 1988.

17 F. den Hollander, H. Maassen (eds.). *Mark Kac seminar on probability and physics. Syllabus 1985-1987.* 1988.

18 Vacantiecursus 1988. *Differentierekening.* 1988.

19 R. de Bruin, C.G. van der Laan, J.R. Luyten, H.F. Vogt. *Publiceren met LATEX.* 1988.

20 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 1.* 1988.

21 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 2.* 1988.

22 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 3.* 1988.

23 J. van Mill, G.Y. Nieuwland (red.). *Proceedings van het symposium wiskunde en de computer.* 1989.

24 P.W.H. Lemmens (red.). *Bewijzen in de wiskunde.* 1989.