TECHNISCHE HOGESCHOOL EINDHOVEN
Afdeling Algemene Wetenschappen
Onderafdeling der Wiskunde

INLEIDING

tot de

MODERNE WISKUNDE

Prof. Dr. N.G. de Bruijn

najaar 1965

Bibl Mag

Prof Seidel

Onderafdeling der Wiskunde

Afd. Algemene Wetenschappen

INLEIDING TOT DE MODERNE WISKUNDE

College van

prof. dr. N.G. de Bruijn

TECHNISCHE HOGESCHOOL EINDHOVEN

Inhoudsbeschrijving

Inleiding tot de

MODERNE WISKUNDE

najaarssemesterjaar 1965

JdG, 18 Juli 2005

Syllabus Inleiding tot de Moderne Wiskunde

door Prof.dr.N.G.de Bruijn

Woord vooraf. Deze inleiding heeft tot doel om een aantal begripsvormingen te behandelen die in alle delen van de wiskunde optreden. Niet overal is naar volledigheid gestreefd; hier en daar is op een enigszins populaire wijze aansluiting gezocht aan de kennis van de schoolwiskunde.

De volgorde van de paragrafen is nogal willekeurig, en doet misschien vreemd aan. Dat komt doordat de stof zich tot een aantal af en toe los van elkaar staande zaken beperkt.

Er is geen serieuze poging gedaan om de grondslagen van de wiskunde te behandelen. Zo wordt niet gesproken over de eisen waaraan in de wiskunde de axioma's, definities, stellingen en bewijzen moeten voldoen. Evenmin wordt gepoogd een houdbare definitie van het begrip "verzameling" te geven.

§.1 Logica. Het is niet de bedoeling hier "de logica" te behandelen; dat is een vak op zichzelf. Het is ook niet nodig: de hoeveelheid logica die in de wiskunde dagelijks wordt gebruikt, is bij ieder weldenkend mens aanwezig. We wijzen hier slechts op enkele punten, en geven enkele belangrijke notaties.

Beweringen. We beschouwen allerlei beweringen, ook wel "volzinnen" of "uitspraken" genoemd. Gemakshalve stellen we vaak een bewering voor door één enkele hoofdletter.

Zo'n letter kan evengoed een juiste als een onjuiste bewering voorstellen. Voorbeeld: A = "2 + 2 = 4"; B = "3 × 6 < 7".

Ontkenning. Is B een bewering, dan is $\neg$ B (spr.: niet-B) de notatie voor de ontkenning van B. Steeds is òf B òf $\neg$ B waar.
Voorbeeld: " $\neg$ (2 + 2 = 4)" betekent "2 + 2 $\neq$ 4";
" $\neg$ (3 × 6 < 7)" betekent "3 × 6 $\geqslant$ 7".

Conjunctie. De uitspraak "A en B" (notatie A & B) is slechts waar als A en B beide waar zijn.
Voorbeeld: "(2 + 2 = 4)&(3 × 3 = 5)" is onwaar;
"$\neg$ {(2 + 2 = 4) & (3 × 3 = 5)}" is waar.

Disjunctie. De uitspraak "A of B" (notatie $A \vee B$) betekent

$$\neg\{(\neg A) \,\&\, (\neg B)\},$$

en is dus slechts waar als niet beide onwaar zijn. In de dagelijkse spreektaal wordt "of" vaak (en dan meestal beklemtoond) in uitsluitende zin gebruikt: één van beide maar niet allebei. Als wij dat willen aanduiden, zullen we de zinswending "òf A, òf B" gebruiken, maar we voeren daarvoor geen afzonderlijke notatie in.
Voorbeeld: "$(2 \times 2 = 4) \vee (3 \times 3 = 5)$" is waar;
"$(2 \times 2 = 4) \vee (3 \times 3 = 9)$" is waar.

Implicatie. De veelgebruikte formule $A \Rightarrow B$ is een afkorting van de uitspraak "$(\neg A) \vee B$". We kunnen hem in woorden brengen met: "als A waar is, dan is B ook waar".

$A \Rightarrow B$ is waar in de volgende gevallen: A en B waar,
A onwaar en B waar, A onwaar en B onwaar.
$A \Rightarrow B$ is onwaar slechts als: A waar en B onwaar.

We zeggen voor $A \Rightarrow B$ ook vaak: "B volgt uit A",
"A impliceert B".

Let op, dat met deze beweringen niet wordt uitgesproken, dat A waar is, en ook niet, dat B waar is.

Zo is bijvoorbeeld:

(1) $(2 \times 2 = 5) \Rightarrow$ elk paard heeft 7 poten

een juiste implicatie, onverschillig of paarden nu 4, 5 of 7 poten hebben. In het gewone spraakgebruik kent men zulke implicaties bijna niet. Men denkt gewoonlijk bij een uitspraak "als A, dan B" aan oorzaak en gevolg: A is een oorzaak voor B, of A is een reden voor B ("Als het regent, dan blijf ik thuis"), of althans een verklaring voor B ("Als de vlag uithangt, dan is het een nationale feestdag"). Evenzeer staat men vreemd tegenover uitspraken als:

(2) als het regent, dan is $2 \times 2 = 4$.

In de wiskunde komen vreemdsoortige implicaties als (1) of (2) herhaaldelijk voor, ze vallen echter niet altijd op, want wiskundige beweringen zijn meestal minder gemakkelijk op waarheid te onderzoeken

dan de vraag of het al dan niet regent. Ze worden daardoor meestal niet als vreemdsoortig aan de kaak gesteld. Natuurlijk is het verkrijgen van zulke implicaties geen doel op zichzelf; ze worden slechts gebruikt om er verdere conclusies uit te trekken.

Men wil bijv. van een getal g, waarvan zekere eigenschappen gegeven zijn, bewijzen, dat het nul is. Men geeft een indirect bewijs: uit de onderstelling dat $g \neq 0$ is, leidt men met behulp van de gegeven eigenschappen iets af dat kennelijk onjuist is. Men bewijst bijvoorbeeld $(g \neq 0) \Rightarrow (2 + 1 = 2)$. Uit het feit dat deze implicatie voor ons getal g juist is, volgt direct, dat $g = 0$. Het komt ook wel voor, dat men afleidt: $(g \neq 0) \Rightarrow (g = 0)$. Uit het feit dat deze implicatie juist is, volgt evenzeer, dat $g = 0$.

Het gewone taalgebruik is ook niet consequent in het eisen van een duidelijke relatie tussen de beide leden van een implicatie. Ingeburgerd is bijv.: "Als tweede Paasdag op woensdag valt, dan ben ik een boon". En ook in een zin als deze: "Als je niets meer van me hoort, dan kom ik" is A moeilijk als reden of oorzaak voor B te verklaren.

In de dagelijkse spreektaal wordt de volgorde vaak omgedraaid. Men zegt bijv.: "Ik stop, als het rode licht brandt". Soms wordt hiermee tegelijk bedoeld: "Ik stop niet, als het rode licht niet brandt". Om zulke misverstanden te vermijden zullen we aan de volgorde "als ..., dan ..." de voorkeur geven.

Equivalentie. De beweringen A en B heten equivalent, als het niet waar is, dat één van de twee waar en de andere onwaar is.
Notatie $A \Leftrightarrow B$. Men zegt vaak hiervoor: "A geldt dan en slechts dan, als B geldt". Men kan ook zeggen, dat $A \Leftrightarrow B$ betekent, dat $A \Rightarrow B$ en $B \Rightarrow A$ beide waar zijn.

Om in een bepaald geval $A \Leftrightarrow B$ te bewijzen, is het ook voldoende te laten zien, dat

$$A \Rightarrow B \text{ en } \neg A \Rightarrow \neg B.$$

Veelal maakt men de fout, dat men

$$A \Rightarrow B \text{ en } \neg B \Rightarrow \neg A$$

bewijst en denkt, dat men daarmee $A \Leftrightarrow B$ heeft bewezen.

Contrapositie van een implicatie. Is $A \Rightarrow B$, dan is ook $\neg B \Rightarrow \neg A$. De laatste implicatie heet de contrapositie van de eerste, en is ermee gelijkwaardig.

Omkering van een implicatie. $B \Rightarrow A$ heet de omkering van $A \Rightarrow B$. Soms is de omkering van een juiste implicatie ook nog waar, en soms niet. Het is enigszins vaag om over de omkering van een stelling te spreken, want een stelling heeft niet altijd het karakter van één enkelvoudige implicatie.

Opgaven: Ga na, dat $A \,\&\, B$ hetzelfde betekent als $\neg[(\neg A) \vee (\neg B)]$,

$A \Rightarrow B$ hetzelfde betekent als $\neg[A \,\&\, (\neg B)]$,

$A \vee B$ hetzelfde betekent als $(\neg A) \Rightarrow B$,

$\neg(A \,\&\, B)$ hetzelfde betekent als $(A \Rightarrow \neg B)$.

Ga na, dat $(2 + 1 = 4) \vee (3 = 3)$ en $(2 = 3) \vee (2 = 2)$ juiste uitspraken zijn.

Beginnelingen protesteren vaak tegen een juiste uitspraak als $3 \geqslant 3$ ($p \geqslant q$ is gedefiniëerd als $(p > q) \vee (p = q)$, of wat hetzelfde betekent, als $\neg(p < q)$).

Quantoren. Laat $B(x)$ een uitdrukking zijn waarin op één of meer plaatsen de letter x optreedt, en waarin men nog voor x allerlei dingen kan substitueren. De letter x heet een variabele. Gemakshalve beperken we ons tot het substitueren van dingen van een nader afgesproken soort, bijv. reële getallen. $B(x)$ is bijv. een uitdrukking zoals $x > 3$, $x^2 = 4$, $x^2 + 2x + 1 = (x + 1)^2$.

We gebruiken nu de formule:

$$\forall x\,[B(x)]$$

om te beweren dat bij elke mogelijke vervanging van de letter x door een ding van de beschouwde soort, de uitdrukking $B(x)$ in een ware bewering overgaat. $\forall$ heet de universele quantor en ook wel het al-symbool. Evenzo beweert

$$\exists x\,[B(x)]$$

dat er minstens één mogelijkheid bestaat om voor x iets te substitueren zó dat $B(x)$ een juiste bewering wordt. $\exists$ heet de existentiële quantor, of het existentiesymbool.

Voorbeelden: $\forall x(x^2 + 1 > 0)$.

$\forall x[x^2 + 2x + 1 = (x + 1)^2]$.

$\forall x[(x > 0) \Rightarrow (x^2 + x > 0)]$.

$\exists x(x^2 = 4)$.

$\exists x[(x > 0) \,\&\, (x < 1)]$.

$\exists x[(x^2 < 0) \Rightarrow (x = 1)]$.

$\exists x[(x = 1) \Rightarrow (x^2 < 0)]$.

Al deze uitspraken zijn juist.

Merk op, dat voor elke bewering B(x) geldt:

$$\neg[\forall x(B(x))] \Leftrightarrow \exists x[\neg B(x)],$$
$$\exists x[B(x)] \Leftrightarrow \neg[\forall x(\neg B(x))],$$
$$\neg \exists x[B(x)] \Leftrightarrow \forall x[\neg B(x)].$$

De letter x had betrekking op dingen van een zekere soort. Als het zeker is, dat er dingen van die soort bestaan, dan geldt de implicatie

$$\forall x(B(x)) \Rightarrow \exists x(B(x)).$$

Nodige en voldoende voorwaarden. Als $\forall x(A(x) \Rightarrow B(x))$, dan zegt men vaak, dat A(x) een voldoende voorwaarde voor B(x) is. Is $\forall(x)(\neg A(x) \Rightarrow \neg B(x))$, dan heet A(x) een nodige voorwaarde voor B(x). Is A(x) tegelijk nodig en voldoende voor B(x), dan noemt men A(x) en B(x) equivalent.

Voorbeelden: $g > 0$ is nodig opdat $g-1 > 0$ is; het is echter niet voldoende;
$g > 0$ is voldoende opdat $g+1 > 0$ is; het is echter niet nodig.

Vrije en gebonden variabelen. In de uitspraak $\forall x(B(x))$ mag de letter x door elke andere letter worden vervangen, mits geen verwarring ontstaat met letters die reeds een vastgestelde betekenis hebben. Waar het om gaat is, dat we twee keer hetzelfde symbool gebruiken. Dus

$$\forall x(B(x)) \Leftrightarrow \forall y(B(y)) \Leftrightarrow \forall \S\, (B(\S)).$$

Het geeft echter verwarring om te schrijven $\forall 4(B(4))$ of $\forall B(B(B))$.

Er is een wezenlijk verschil tussen de uitdrukkingen als B(x) enerzijds en $\forall x(B(x))$ anderzijds. Zolang x alleen maar een variabele is, is B(x) geen bewering, doch het wordt een bewering, wanneer we voor de letter x iets substitueren. $\forall x(B(x))$ is wel een bewering, maar hierin mogen we niet substitueren. Wanneer we daarin x door een bepaald object, bijv.

het getal 3, vervangen, komt er iets te staan dat we niet hebben gedefinieërd.

De letter x in $\forall x(B(x))$ noemt men een gebonden variabele. Een vrije variabele is een letter waarvoor we nog substitutiemogelijkheden hebben. In een bewering staan nooit vrije variabelen. Alleen in stukken van beweringen komen vrije variabelen voor. In B(x) is x een vrije variabele, maar B(x) is dan ook geen bewering. Het kan wel als een stuk van een bewering optreden, bijv. in $\forall x(B(x))$ of $\exists x(B(x))$.

In de praktijk spreekt men vaak slechts stukken van beweringen uit, teneinde uitvoerige herhalingen te vermijden.

Ook buiten de logische symboliek komt het onderscheid tussen vrije en gebonden variabelen voor. In een uitdrukking als

$$(a - 1)\ \Sigma_{k=0}^{n}\ a^k = a^{n+1} - 1$$

zijn a en n vrije variabelen, en k is een gebonden variabele. In de volzin: "Voor elk reëel getal a en voor elk natuurlijk getal n geldt:

$$(a - 1)\ \Sigma_{k=0}^{n}\ a^k = a^{n+1} - 1",$$

zijn echter ook a en n gebonden variabelen (onverschillig of de volzin juist of onjuist is).

De (straks nog te bespreken) gewoonte om al-symbolen aan het begin van een zin weg te laten maakt het vaak moeilijk om het verschil tussen vrije en gebonden variabelen te zien. Die gewoonte houdt immers in, dat men met een stuk van een formule de gehele formule bedoelt!

Veelal komen in de wiskunde beweringen voor met verschillende quantoren achter elkaar. Is B(x,y) een uitdrukking die de beide letters x en y bevat, dan kan men bijv. de bewering

$$\forall x\ \exists y[B(x,y)]$$

beschouwen. Deze beweert, dat voor elke x de uitdrukking $\exists y[B(x,y)]$ waar is. Ga na, dat voor elke uitdrukking B(x,y) de volgende regels juist zijn:

$$\forall x\ \forall y[B(x,y)] \iff \forall y\ \forall x[B(x,y)]$$
$$\exists x\ \exists y[B(x,y)] \iff \exists y\ \exists x[B(x,y)]$$
$$\exists x\ \forall y[B(x,y)] \implies \forall y\ \exists x[B(x,y)].$$

Er is geen grootste getal ⇒ Er is een grootst getal.

De laatste implicatie mag niet altijd worden omgekeerd. Zo is bijv. $\forall y\ \exists x(x > y)$ juist, maar $\exists x\ \forall y(x > y)$ is onjuist. Op ieder doosje past een deksel, maar er bestaat geen deksel dat op alle doosjes past.

Van een bewering $B(x,y,\ldots)$ met quantoren ervoor kunnen we op machinale wijze de ontkenning vormen door de $\forall$'s door $\exists$'s te vervangen en omgekeerd, en tevens B door $\neg B$ te vervangen. Ga na, dat de ontkenning van

$$\forall x\ \exists y\ \forall z\ \exists w\ \exists v\ [B(x,y,z,w,v)],$$

wordt gevormd door

$$\exists x\ \forall y\ \exists z\ \forall w\ \forall v\ [\neg B(x,y,z,w,v)].$$

Opgaven: Ga na, of de volgende uitspraken al dan niet juist zijn:

$$\forall x\ \exists y\ \forall z\ (z > x \Rightarrow z > y),$$
$$\exists x\ (x > 3 \Rightarrow\ \forall y\ [(y > x)\ \vee\ (y = 1)]),$$
$$\forall x\ \exists y\ \forall z\ (x < y < z).$$

Taalgebruik. Bij het vertalen van ingewikkelde logische formules naar de spreektaal moet men zeer voorzichtig te werk gaan. Men moet een zin bouwen waarin de volgorde der woorden nauwkeurig overeenstemt met de volgorde der logische symbolen (terwijl de gewone omgangstaal doorgaans vele variaties op de volgorde toelaat). Vaak is het moeilijk, doordat de taal niet de ruime mogelijkheden tot het plaatsen van haakjes kent.

Deze bezwaren worden dikwijls ondervangen door het invoeren van nieuwe woorden, die voor een stuk van zo'n formule in de plaats treden. Op die manier kan bijv. de juiste uitspraak

$$\neg\ \exists x\{(x > 0)\ \&\ \forall y[(y > 0) \Rightarrow x \leqslant y]\},$$

die te lezen is als: "er is geen x die positief is en tevens kleiner is dan elk ander positief getal y", door invoering van de term "kleinste positief getal" worden bekort tot "er is geen kleinste positief getal". Dezelfde bewering kan ook worden geschreven als

$$\forall x[(x > 0) \Rightarrow \exists y(0 < y < x)]$$

("bij elke positieve x is er een positieve y die nog kleiner is").
Ga na, dat beide formules equivalent zijn, door toepassing van de volgende omzettingsregels, en ga voor elke omzettingsregel afzonderlijk de juistheid na.

$$\neg\,\exists x(B(x)) \iff \forall x(\neg B(x)),$$
$$\neg\,(A \,\&\, B) \iff A \Rightarrow \neg B,$$
$$\neg\,\forall y(B(y)) \iff \exists y(\neg B(y)),$$
$$\neg\,[(y > 0) \Rightarrow (x \leq y)] \iff 0 < y < x.$$

Vaak laat men bij het vertalen de universele symbolen die aan het begin van een formule voorkomen, eenvoudig weg. Men zegt bijv.: "het kwadraat van een reëel getal is ≥ 0" i.p.v. "voor elk reëel getal is het kwadraat ≥ 0". En men zegt $(a + b)(a - b) = a^2 - b^2$ i.p.v. $\forall\, a\, \forall b[(a + b)(a - b) = a^2 - b^2]$. Met universele symbolen die verderop in de formule staan, mag men beslist niet zo luchthartig omspringen. Een zin als de volgende is onduidelijk: "Bij een cirkel is er een punt te vinden, zó dat een lijn door dat punt de cirkel snijdt". (Minstens één lijn? Elke lijn?).

De ontkenning van een bewering B vertaalt men het veiligste door: "het is niet waar dat B". Pas daarna kan men nagaan welke taalkundige vereenvoudigingen die zin toelaat. Vaak wordt de zin onduidelijk in de schrijftaal doordat de betekenis sterk van de intonatie gaat afhangen.

In verband met de gewoonte om al-symbolen aan het begin van een zin weg te laten, is bijzondere voorzichtigheid geboden. De ontkenning van $B(x)$ is $\neg B(x)$. *Bedoelt men echter met* $B(x)$, *dat* $\forall x(B(x))$, *dan is* de ontkenning niet $\forall x[\neg B(x)]$ doch $\neg\forall x(B(x))$, of $\exists x[\neg B(x)]$. In het laatste geval mag de quantor niet worden weggelaten.

Wil men bijv. uit het ongerijmde de volgende stelling bewijzen:

"de hoogtelijnen van een driehoek gaan door één punt",

dan moet men van de ontkenning uitgaan. Wanneer we zouden uitgaan van "de hoogtelijnen van een driehoek gaan niet door één punt", en tijdens het verdere betoog deze uitspraak op verschillende driehoeken toepassen, dan zou uit het bereiken van een tegenspraak niet volgen, dat van elke driehoek de hoogtelijnen door één punt gaan, doch slechts, dat er een driehoek bestaat waarbij ze door één punt gaan.

Nog enkele voorbeelden van taalkundige bezuinigingen:

$$\forall x[x > 0 \Rightarrow B(x)]$$

betekent: "Voor alle x geldt, dat als $x > 0$ is, ook $B(x)$ waar is".
Korter: "Voor alle positieve x geldt $B(x)$". Evenzo heet:

$$\exists x[(x > 0) \,\&\, B(x)]$$

"Er is een x die aan $x > 0$ en tegelijk aan B(x) voldoet".
Korter: "Er is een positieve x waarvoor B(x) geldt".

Een zeker gevaar in de taal schuilt in het woord "is", dat meestal niet gelijkheid of equivalentie, maar een gecamoufleerde implicatie aanduidt. Laat S(x) de zin "x is een schoorsteenveger" en M(x) de zin "x is een mens" voorstellen. Nu bedoelt men met de zin

"Een schoorsteenveger is een mens"

te zeggen, dat $\forall x[S(x) \Longrightarrow M(x)]$ en niet dat $\forall x[S(x) \Longleftrightarrow M(x)]$. Daarom doen we beter om een iets sterkere formulering te kiezen als we een equivalentie bedoelen.

Merk op, dat een zin als "een hond is geen vis" wèl equivalent is met "een vis is geen hond", en zelfs met "geen vis is een hond" en "geen hond is een vis" (dit hangt samen met het feit dat de uitspraken $A \Longrightarrow \neg B$ en $B \Longrightarrow \neg A$ hetzelfde betekenen).

Het teken = zullen we uitsluitend gebruiken voor "is hetzelfde als".

De spreektaal kent nog enkele quantoren waarvoor we geen speciaal symbool invoeren. We kunnen ze echter in $\forall$'s en $\exists$'s uitdrukken, en desgewenst uitsluitend in $\forall$'s of uitsluitend in $\exists$'s. We geven er enkele aan met mogelijke vertalingen in formules erbij:

"Geen enkele x voldoet aan B(x)": $\forall x[(\neg B(x))]$
of $\neg[\exists x(B(x))]$;

"Niet elke x voldoet aan B(x)" : $\neg[\forall x(B(x))]$,
of $\exists x[\neg B(x)]$;

"Hoogstens één x voldoet aan B(x)": $\neg\exists x\exists y[(x \neq y)\&B(x)\&B(y)]$,
of $\forall x\forall y[(x \neq y) \Longrightarrow (B(x) \Longrightarrow \neg B(y))]$,
of $\forall x\forall y[(B(x)\&B(y)) \Longrightarrow x = y]$;

"Eén en slechts één x voldoet aan B(x)" : $\exists x[(B(x))\& \forall y(B(y) \Longrightarrow x = y)]$.

Slotopmerking. Het is zeker niet de bedoeling van het voorafgaande om het logisch denken voortaan door het mechanisch werken met symbolen te vervangen (daartoe zou deze paragraaf trouwens totaal onvoldoende zijn). Voor ons doel dienen de logische formules ter ondersteuning van het denken en ter overdracht van gedachten, waarbij veelal formules veiliger zijn dan de gewone taal.

§ 2. Verzamelingen. We doen alsof het begrip "verzameling" bekend is.

De objecten waaruit een verzameling is opgebouwd heten de elementen van de verzameling. Het feit dat een object a een element is van een verzameling V, wordt uitgedrukt door de formule $a \in V$. De ontkenning daarvan is $a \notin V$.

Verzamelingen kunnen op verschillende manieren worden gevormd.

1°. Door (als dat kan) de elementen in zekere volgorde op te noemen. Bijv. de verzameling die bestaat uit de getallen 3, 8, 11. Deze verzameling geven we aan met $\{3, 8, 11\}$. Men bedenke, dat $\{3, 8, 11\}$ hetzelfde betekent als bijv. $\{8, 3, 11\}$.

2°. Door het noemen van een eigenschap: de verzameling is dan de verzameling van alle objecten die deze eigenschap hebben. Drukken we de eigenschap uit door B(x) (d.w.z. een ding heeft de eigenschap dan en slechts dan als het bij substitutie B(x) tot een ware uitspraak maakt), dan geven we de verzameling aan met

$$\{x \mid B(x)\}.$$

Voorbeelden: $\{x \mid x$ is een reëel getal en $x > 2\}$ stelt voor de verzameling van alle reële getallen > 2. Zijn C en D punten in de elementaire planimetrie, dan stelt

$$\{P \mid P \text{ is een punt en } PC = PD\}$$

de middelloodlijn van CD voor. Algemeen betekent: "meetkundige plaats van de punten met de eigenschap B" niets anders dan $\{P \mid B(P)\}$ (toevoegingen als "P is een punt" laat men meestal weg, omdat ze door het verband waarin de zin voorkomt, wel kunnen worden gemist).

3°. Door het voortbrengen met behulp van een andere verzameling. Beschouw bijv. de verzameling van alle getallen die ontstaan door in de uitdrukking $x^2 + x$ een geheel getal te substitueren. Deze geven we aan met

$$V = \{x^2 + x \mid x \in G_h\},$$

als G_h de verzameling van alle gehele getallen voorstelt. Men zou ook met de eerder genoemde notatie kunnen volstaan door te schrijven:

$$V = \{ y \mid \exists x [(x \in G_h) \& x^2 + x = y]\}.$$

Het feit dat bijv. 0 "om twee redenen" tot V behoort ($0^2 + 0 = 0$ en $(-1)^2 + (-1) = 0$) doet niet terzake. Een getal behoort tot V of het

behoort niet tot V; een onderscheiding als "dubbel tot V behoren" zullen we niet maken.

Om zekere uitspraken een algemener geldigheid te geven, voeren we ook de lege verzameling in (notatie ϕ), die geen enkel element heeft.

Zeer vaak zullen we uitspraken tegenkomen van het type: "alle elementen van V hebben de eigenschap B", dus

$$\forall x[(x \in V) \Rightarrow B(x)].$$

Deze formules zullen we nu afkorten tot:

$$\forall_{x \in V} B(x).$$

Evenzo wordt de uitspraak: "Er is een element in V dat de eigenschap B heeft", dus

$$\exists x[(x \in V) \ \& \ B(x)]$$

afgekort tot:

$$\exists_{x \in V} B(x).$$

Men past een analoge afkorting toe in gevallen als

$$\forall x[(x > 1) \Rightarrow B(x)] \text{ : afkorting } \forall_{x>1} B(x)),$$

waarbij het onderschrift $x > 1$ een afkorting is voor $x \in \{y \mid y > 1\}$.

In de wiskunde schrijft men zeer vaak regels als:

$$B(x) \qquad (x \in V).$$

Daarmee is bedoeld: $\forall_{x \in V} B(x)$.

Voorbeeld: $x^2 + x > 6 \qquad (x > 2)$.

Men gebruike deze notatie echter nooit voor de existentiebewering $\exists_{x \in V} B(x)$. (Deze slechte gewoonte schijnt een traditie te zijn geworden bij de middelwaardestelling uit de differentiaalrekening).

Inclusierelatie. Zijn V_1 en V_2 verzamelingen, en is $\forall_{x \in V_1} (x \in V_2)$ (d.w.z. $\forall x[x \in V_1 \Rightarrow x \in V_2]$), dan heet V_1 een deelverzameling van V_2. Notatie $V_1 \subset V_2$, of $V_2 \supset V_1$. In het bijzonder geldt $V \subset V$ voor elke verzameling V. Is $V_1 \subset V$, $V_1 \neq V$, dan heet V_1 een echte deelverzameling van V.

In het bijzonder is $\phi \subset V$ voor elke verzameling V, waar ϕ de lege verzameling voorstelt.

Doorsnede. Zijn V_1 en V_2 verzamelingen, dan heet de verzameling

$$\{x \mid (x \in V_1) \,\&\, (x \in V_2)\}$$

de doorsnede van V_1 en V_2. Wij geven die aan met $V_1 \cap V_2$.

Is de doorsnede leeg, dan heten V_1 en V_2 disjunct.

Vereniging. Zijn weer V_1 en V_2 verzamelingen, dan heet de verzameling

$$\{x \mid (x \in V_1) \vee (x \in V_2)\}$$

de vereniging van V_1 en V_2. We geven die aan met $V_1 \cup V_2$.

Verschil. Zijn V_1 en V_2 verzamelingen dan heet

$$\{x \mid x \in V_1 \,\&\, x \notin V_2\}$$

het verschil van V_1 en V_2. Notatie $V_1 \setminus V_2$. Dit begrip wordt ook gebruikt als V_2 geen deel van V_1 is.

Opgave: Bewijs, dat voor alle verzamelingen V_1, V_2, V_3

$$(V_1 \cap V_2) \cap V_3 = V_1 \cap (V_2 \cap V_3)$$
$$(V_1 \cup V_2) \cup V_3 = V_1 \cup (V_2 \cup V_3)$$
$$V_1 \cap (V_2 \cup V_3) = (V_1 \cap V_2) \cup (V_1 \cap V_3)$$
$$V_1 \cup (V_2 \cap V_3) = (V_1 \cup V_2) \cap (V_1 \cup V_3).$$
$$V_1 \cup V_2 = (V_1 \setminus V_2) \cup (V_1 \cap V_2) \cup (V_2 \setminus V_1)$$
$$(V_1 \cup V_2) \setminus V_3 = (V_1 \setminus V_3) \cup (V_2 \setminus V_3).$$

§ 3. Natuurlijke getallen. Daarmee bedoelen we de getallen 1, 2, 3, 4, ... dus de positieve gehele getallen. In deze rij is een volgorde aanwezig: 2 volgt op 1, 3 volgt op 2, enz. We drukken dat even uit door te schrijven $\varphi(1) = 2$, $\varphi(2) = 3$, ...

Bij deze toevoeging kunnen we enkele regels opmerken, die we echter niet kunnen bewijzen. We zullen deze nu als axioma's aannemen, en komen dan tot het volgende axiomasysteem, dat in 1899 door Peano voor het systeem N der natuurlijke getallen werd opgesteld.

Axioma A. Er is een element in N dat de naam 1 draagt.

Axioma B. Er is een toevoeging, die aan elke $n \in N$ een $m \in M$ toevoegt. Deze bij n aangewezen m geven we met $\varphi(n)$ aan (in § 5 zullen we uitvoeriger over zulke toevoegingen spreken). De toevoeging $n \to \varphi(n)$

voldoet aan:

1°. $\forall_{n\in N}[\varphi(n) \neq 1]$;

2°. $\forall_{n\in N}\,\forall_{m\in N}[(\varphi(n) = \varphi(m)) \Rightarrow n = m]$;

3°. Is V een deelverzameling van N, en geldt $1 \in V$ en ook $\forall_{n\in V}[\varphi(n) \in V]$, dan is $V = N$.

Op grond van deze axioma's kunnen, nadat optelling, vermenigvuldiging, ongelijkheden, etc. zijn gedefiniëerd, alle bekende eigenschappen van de natuurlijke getallen worden afgeleid. (Zie bijv. E. Landau, Grundlagen der Analysis, of H.A. Thurston, The number system). Dan blijkt ook, dat voor alle $n \in N$ geldt $\varphi(n) = n + 1$.

Volledige inductie. Op de in Axioma B, 3° uitgedrukte eigenschap (en mede op de formule $\varphi(n) = n + 1$) berust de bewijsmethode der volledige inductie. Dit is een methode om een formule van het type $\forall_{k\in N}(B(k))$ te bewijzen. De methode bestaat uit twee stappen:

1°. Men bewijst $B(1)$.

2°. Men bewijst $\forall_{n\in N}(B(n) \Rightarrow B(n + 1))$. D.w.z.: uit de onderstelling dat $B(n)$ juist is, leidt men af, dat $B(n + 1)$ juist is.

Hiermee is $B(k)$ voor alle $k \in N$ bewezen. Zij n.l. V de verzameling

$$V = \{k \mid (k \in N) \,\&\, B(k)\},$$

dan is $1 \in V$ en $\forall n(n \in V \Rightarrow \varphi(n) \in V)$, zodat $V = N$. Derhalve geldt $B(k)$ voor alle $k \in N$.

Opmerking: Veiligheidshalve hebben we twee verschillende letters (k en n) gebruikt. Men kan dan zinswendingen gebruiken als: "Is $B(k)$ juist voor $k = n$, dan is $B(k)$ juist voor $k = n + 1$". Wat men wel eens hoort zeggen is: "Is $B(n)$ juist voor n, dan is $B(n)$ juist voor $n + 1$" of: "dan is $B(n)$ juist voor $n = n + 1$".

In de formuleringen zoals we die boven gaven, komen echter nergens k en n tegelijk in één zin voor, zodat we rustig overal n kunnen schrijven. We zullen dat in het vervolg steeds doen, want de lezer is nu gewaarschuwd. Alleen in voorbeeld 1 is de letter k nog aangehouden.

Voorbeeld 1: Te bewijzen, dat voor elke $k \in N$ geldt:

$$1^3 + 2^3 + 3^3 + \ldots + k^3 = \tfrac{1}{4}k^2(k + 1)^2.$$

Bewijs: Voor k = 1 is de formule juist. Nu de inductiestap: We moeten bewijzen, dat voor elke n ∈ N geldt:

$$[1^3 + 2^3 + \ldots + n^3 = \tfrac{1}{4}n^2(n+1)^2] \Longrightarrow [1^3 + 2^3 + \ldots + (n+1)^3 = \tfrac{1}{4}(n+1)^2(n+2)^2].$$

Dit volgt uit het feit dat de linkerleden $(n+1)^3$ verschillen, en de rechterleden eveneens:

$$\tfrac{1}{4}(n+1)^2(n+2)^2 - \tfrac{1}{4}n^2(n+1)^2 = (n+1)^2 \cdot \tfrac{1}{4}[(n+2)^2 - n^2] = (n+1)^3.$$

Voorbeeld 2: Te bewijzen $\forall_{n\in N}(2^n > n)$.

Bewijs: Voor n = 1 is de formule juist: $2^1 > 1$. Voorts moet worden bewezen, dat voor alle n ∈ N geldt:

$$2^n > n \Longrightarrow 2^{n+1} > n + 1.$$

Uit $2^n > n$ volgt inderdaad $2^{n+1} = 2 \cdot 2^n > 2n = n + n \geq n + 1$, dus $2^{n+1} > n + 1$.

Voorbeeld 3: Te bewijzen: Is W een niet-lege deelverzameling van N, dan heeft W een kleinste element, d.w.z.:

$$\exists_{w\in W} \forall_{u\in W} (u \geq w).$$

Bewijs: Neem aan, dat W geen kleinste element heeft. We bewijzen nu, door volledige inductie, dat voor alle n ∈ N geldt $\forall_{w\in W}(w > n)$. Voor n = 1 is dit juist (anders was 1 het kleinste getal van W). We bewijzen nu, dat voor elke n ∈ N geldt:

$$\forall_{w\in W}(w > n) \Rightarrow \forall_{w\in W}(w > n + 1).$$

Uit het linkerlid volgt n.l., dat n + 1 ∉ W (anders zou n + 1 het kleinste element van W zijn). Hiermee is nu door volledige inductie bewezen, dat $\forall_{w\in W}(w > n)$ voor elke n ∈ N. Kies nu n gelijk aan een element van W, dan komt er een tegenspraak.

Soms wordt de volgende variant van de methode der volledige inductie gebruikt: Om $\forall_{n\in N}B(n)$ te bewijzen toont men aan, dat B(1) juist is, en dat uit de onderstelling dat

$$B(1), B(2), \ldots, B(n)$$

alle juist zijn, de juistheid van B(n + 1) volgt.

Dat ook deze middelen tot het doel leiden blijkt door de bewering:

$$C(n) = B(1) \,\&\, B(2) \,\&\, B(3) \,\&\, \ldots \,\&\, B(n)$$

te beschouwen, en $\forall_{n \in \mathbb{N}} C(n)$ door volledige inductie te bewijzen.

Opmerkingen: De merkwaardige situatie doet zich vaak voor, dat een sterkere bewering gemakkelijker door inductie is te bewijzen dan een zwakkere. Zo is bijv. de uitspraak dat voor alle $n \in N$ de som $1^3 + 2^3 + \ldots + n^3$ het kwadraat van een geheel getal is, een juiste bewering, want in voorbeeld 1 hebben we een sterkere bewering bewezen: het is het kwadraat van $\frac{1}{2}n(n + 1)$. Voor de zwakkere stelling mislukt het inductiebewijs echter. Uit "$1^3 + \ldots + n^3$ is een kwadraat" volgt niet op eenvoudige wijze "$1^3 + \ldots + (n + 1)^3$ is een kwadraat". Jammer genoeg is de uitspraak "een kwadraat + $(n + 1)^3$ is weer een kwadraat" onjuist.

Vaak is het een grote kunst om voor een bepaald doel een inductief bewijsbare bewering op te stellen.

Opgave: Van de foutieve stelling: "Alle mensen zijn even oud" is hieronder een foutief bewijs gegeven. Spoor de fout op in het "bewijs".
"Bewijs": Laat B(n) de volgende bewering zijn:

> In een verzameling van n personen komen er geen twee van verschillende leeftijd voor.

B(1) is waar (want in een verzameling van 1 persoon komen geen twee verschillende personen voor). Nu $B(n) \Rightarrow B(n + 1)$. Zij V een verzameling van n personen, en zij p een nieuwe persoon. We moeten laten zien, dat p even oud is als alle $v \in V$. We kiezen een persoon v_o uit V. Nu beschouwen we de verzameling W die uit V ontstaat door v_o door p te vervangen. Deze bestaat weer uit n personen, dus zijn ze alle even oud (op grond van B(n)). Dus p is even oud als alle $v \in V$ (even afgezien van v_o). Maar v_o was even oud als alle andere v's uit V, dus p is even oud als alle $v \in V$. Hiermee is B(n + 1) afgeleid uit B(n) (d.w.z. we hebben bewezen, dat het niet voorkomt, dat B(n) waar is en tegelijk B(n + 1) onwaar).

§ 4. Afbeeldingen.

Laat V en W twee verzamelingen zijn met elementen van willekeurige aard. We vormen nu de nieuwe verzameling bestaande uit alle symbolen (v,w), waarin v een element van V en w een element van W is. Deze verzameling geven we met $V \times W$ aan:

$$V \times W = \{(v,w) \mid (v \in V) \,\&\, (w \in W)\}.$$

Deze $V \times W$ heet het cartesisch product van V en W (naar aanleiding van het feit dat Descartes de punten van het platte vlak interpreteerde als getallenparen (x,y), waarin x en y de coördinaten van het betreffende punt voorstellen).

Een deelverzameling F van $V \times W$ heet een afbeelding van V in W, als

$$\forall_{v \in V} \text{ [er is precies één } w \in W \text{ zó dat } (v,w) \in F].$$

In plaats van afbeelding van V in W zegt men ook wel "op V gedefiniëerde functie met waarden in W".

Is F een afbeelding van V in W en is v een element van V, dan wordt die éne $w \in W$ die aan $(v,w) \in F$ voldoet, aangeduid met: het beeld van v bij de afbeelding F, of de bij v behorende functiewaarde, en wordt aangegeven met het symbool F(v).

Doorgaans zegt men: een afbeelding van V in W is een voorschrift volgens welk aan elk element van V één element van W is toegevoegd, en in dat verband wordt F de grafiek van de afbeelding genoemd. Het meer ingewikkelde verhaal dat we hierboven gaven, dient om de vaagheid van het woord "voorschrift" te verschuiven naar de reeds geaccepteerde vaagheid van het woord "verzameling".

De verzameling van alle afbeeldingen van V in W wordt wel door W^V aangegeven.

Voorbeelden van afbeeldingen: Projectie van een lijn op een andere. De afbeelding die aan elk reëel getal x het kwadraat x^2 toevoegt. De afbeelding die in § 4 met φ werd aangeduid.
In de laatste twee gevallen hebben we afbeeldingen van V in zichzelf.

Is F een afbeelding van V in W, dan heet de verzameling F(V) gedefiniëerd door $F(V) = \{F(v) \mid v \in V\}$, het beeld van V. Dit beeld is dus een deel van W.

Is F een afbeelding van V in W, en is $F(V) = W$ (dus $\forall_{w \in W} \exists_{v \in V} (F(v)=w)$), dan zeggen we, dat F een afbeelding van V op W is.

Is F een afbeelding van V op W, en is elk element van W het beeld van precies één element van V, dan heet F een éénéénduidige afbeelding van V op W. In dat geval is er een inverse afbeelding G van W op V, gedefiniëerd als volgt: Is $w \in W$, en is v het element van V met $F(v) = w$, dan is $G(w) = v$. (Wil men nog aan de parendefinitie vasthouden, dan kan men zeggen:

$$G = \{(w,v) \mid (v \in V) \,\&\, (w \in W) \,\&\, ((v,w) \in F)\}).$$

Kennelijk is

$$\forall_{v \in V}\ (G(F(v)) = v),$$
$$\forall_{w \in W}\ (F(G(w)) = w).$$

Voorbeelden: 1. Laat l en m rechte lijnen zijn in het platte vlak, en laat F de afbeelding zijn van l in m, die aan elk punt $P \in l$ zijn loodrechte projectie op m toevoegt. Wanneer heeft deze afbeelding een inverse, en wat is dan die inverse?

2. Laat V de verzameling van alle gehele getallen zijn, en zij F de afbeelding van V in zichzelf, gedefiniëerd door:

$$F(x) = x + 1 \qquad (x \in V).$$

Door welke formule is de inverse afbeelding gegeven?

§ 5. Equivalentierelaties.

Zij V een verzameling, en R een deelverzameling van $V \times V$, dus een verzameling van symbolen (u,v) met $u \in V$, $v \in V$. We zeggen dan, dat R een binaire relatie op V is, en we schrijven:

$$u\ R\ v \quad \text{i.p.v.} \quad (u,v) \in R.$$

Uit u R v behoeft niet v R u te volgen.

Er zijn vele voorbeelden te geven van zulke relaties in de wiskunde.

1°. De gelijkheid op een willekeurige verzameling: u R v dan en slechts dan als $u = v$.

2°. Op de verzameling der gehele getallen: de relaties $<, >, \leq, \geq$.

3°. In de verzameling van alle figuren van het platte vlak: de relatie $\sim$ (gelijkvormigheid) en $\cong$ (congruentie).

4°. In de verzameling van alle punten van het platte vlak, de relatie die aanduidt, dat de afstand tussen u en v kleiner is dan 1.

5°. In de verzameling van alle rechte lijnen van het platte vlak: de relatie u//v (evenwijdigheid).

Een binaire relatie R op V heet een equivalentierelatie als R aan de volgende eisen voldoet:

E 1. $\forall_{v \in V}\ (v\ R\ v)$ d.i. R is reflexief

E 2. $\forall_{u \in V}\ \forall_{v \in V}\ (u\ R\ v \Longrightarrow v\ R\ u)$ d.i. R is symmetrisch

E 3. $\forall_{u \in V}\ \forall_{v \in V}\ \forall_{w \in V}[\{(u\ R\ v)\ \&\ (v\ R\ w)\} \Longrightarrow u\ R\ w]$ d.i. R is transitief.

Merk op, dat slechts de voorbeelden 1°, 3° en 5° equivalentierelaties vormen (als men bij 5° tenminste twee samenvallende lijnen ook nog evenwijdig noemt). Bij 2°: $<$ is niet reflexief en niet symmetrisch; $\leq$ is wèl reflexief maar niet symmetrisch. Bij 4°: Niet transitief.

Equivalentieklassen. Zij $\sim$ een equivalentierelatie op V. Is v een element van V, dan heet de verzameling

$$\{u \mid u \in V \;\&\; u \sim v\}$$

de equivalentieklasse van v.

Uit E1, E2 en E3 volgt, dat equivalente elementen dezelfde equivalentieklasse hebben.

Een deelverzameling van V heet een equivalentieklasse als het de equivalentieklasse van een zekere $v \in V$ is. Verder is gemakkelijk in te zien: De equivalentieklassen zijn twee aan twee disjunct en de vereniging van alle equivalentieklassen is V zelf.

Met de relatie $\sim$ correspondeert dus een z.g. klassenindeling van V, en wel zó, dat

(1) $\qquad u \sim v \Longleftrightarrow$ u en v liggen in dezelfde klasse.

Gaat men omgekeerd uit van een klassenindeling van V, dan kan men een binaire relatie $\sim$ maken door (1) als definitie van $\sim$ te beschouwen. Laat zien, dat $\sim$ dan weer aan de drie eisen voor een equivalentierelatie voldoet.

Definitie door abstractie. Het komt in de wiskunde zeer vaak voor, dat men nieuwe begrippen vormt door in een bekende verzameling een equivalentierelatie te beschouwen en vervolgens over de equivalentieklassen te gaan spreken. De equivalentieklassen zijn dan de nieuwe objecten.

Een vertrouwd voorbeeld is de definitie van "aantal". Men vormt daartoe een equivalentierelatie, waarbij "drie paarden", "drie appels", "drie centen", ... alle onderling equivalent zijn. De equivalentieklasse duidt men aan met het woord "drie". Het aantal "drie" heet dan gedefinieerd door abstractie (abstractie = aftrekking. Wat afgetrokken is, zijn de woorden "paarden", "appels", "centen", ...). We zullen deze aantalsdefinitie nog nauwkeuriger bekijken in § 6.

Een ander bekend voorbeeld is dat van "richting". Beschouw de verzameling V van alle rechten in het platte vlak. De relatie $l \sim m$ zal betekenen $l \mathbin{/\!/} m$ (we zeggen ook dat $l \mathbin{/\!/} l$). Deze voldoet aan E1, 2, 3. In plaats van

nu zeer onduidelijk te zeggen: "een richting is datgene wat gemeenschappelijk is aan een stel evenwijdige lijnen", definiëren we nu:

"een richting is een equivalentieklasse".

Is ρ een richting, dan zeggen we, dat de lijn l de richting ρ heeft (of dat ρ de richting van l is), als $l \in \rho$.

We concluderen verder: l en m hebben dan en slechts dan dezelfde richting als $l \,//\, m$.

Andere bekende voorbeelden zijn de gebruikelijke definities van gehele getallen en van breuken. We komen daarop nog terug in § 8.

In § 9 zullen we door abstractie de "restklassen" definiëren.

Vaak spreekt men bij een definitie door abstractie over <u>identificatie</u>. Men spreekt bijv. over "drie appels", "drie paarden", en merkt op een gegeven ogenblik, dat de appels en de paarden volmaakt onbelangrijk zijn bij het beoogde doel. Men zegt dan, dat men van de soort der objecten afziet, of dat men "drie appels" en "drie paarden" voortaan als hetzelfde zal beschouwen. Natuurlijk heeft men niet het recht om zoiets zonder meer te zeggen. Waar zouden we zo naar toe gaan? Het "recht" kan echter ontleend worden aan de overgang op equivalentieklassen. Daarbij ontstaat de plicht om de equivalentie te formuleren, en te controleren dat die equivalentie aan E1, 2, 3 voldoet.

Laat V een verzameling, en $\sim$ daarop een equivalentierelatie zijn. $E(x)$ een uitspraak zijn over elementen van V, die voldoet aan

$$\forall_{x \in V}\, \forall_{y \in V}\, ((E(x) \,\&\, x \sim y) \Longrightarrow E(y)).$$

In zo'n geval is het dikwijls zinvol een uitspraak $E'(K)$ in te voeren, die uitspreekt dat $E(x)$ juist is voor alle $x \in K$. Voor elke equivalentieklasse K geldt dat óf $E(x)$ juist is voor alle $x \in K$ óf onjuist is voor alle $x \in K$. Is dus $E'(K)$ onjuist, dan is $E(x)$ voor geen enkele $x \in K$ juist.

<u>Voorbeeld</u>: Loodrechte stand van richtingen in het platte vlak.

§ 6. <u>Machtigheid, kardinaalgetallen</u>.

In de collectie van alle verzamelingen voeren we de volgende equivalentierelatie in, die <u>gelijkmachtigheid</u> heet. We zeggen, dat de verzamelingen V en W gelijkmachtig zijn (notatie is weer $V \sim W$), als er een éénéénduidige afbeelding van V op W bestaat.

Laat zien, dat $\sim$ aan E1, 2, 3 voldoet.

Een klasse van onderling gelijkmachtige verzamelingen heet een kardinaalgetal of machtigheid.

Zeer belangrijk is het begrip eindige verzameling.

We beginnen met op te merken dat, als n en m natuurlijke getallen zijn, de verzamelingen

$$\{1, 2, \ldots, n\} \quad \text{en} \quad \{1, 2, \ldots, m\}$$

slechts dan gelijkmachtig zijn als $n = m$. Dit is de z.g. hoofdeigenschap van het tellen. Om dit te bewijzen geven we $\{1, 2, \ldots, n\}$ met V_n aan, en definiëren we W door:

$$W = \{n \mid (n \in N) \;\&\; \exists_{m \in N}\, (m \neq n \;\&\; V_n \sim V_m)\}.$$

We moeten bewijzen, dat W leeg is. Was W niet leeg, dan was er een kleinste getal in W. Dit noemen we n. Er is nu een m met $V_n \sim V_m$, $m \neq n$. Zij F de éénéénduidige afbeelding van V_n op V_m, en zij $F(n) = k$. Gemakkelijk is in te zien dat $n > 1$.

Zij H de éénéénduidige afbeelding van V_m op zichzelf, gegeven door:

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

Nu is de afbeelding $a \to H(F(a))$ een éénéénduidige afbeelding van V_n op V_m. Daarbij is $H(f(n)) = H(k) = m$. Door deze afbeelding wordt nu V_{n-1} éénéénduidig op V_{m-1} afgebeeld. Dus $V_{n-1} \sim V_{m-1}$ en $n - 1 \neq m - 1$. Derhalve $n - 1 \in W$, in strijd met de onderstelling dat n de kleinste was. Hiermee is uit het ongerijmde aangetoond, dat W leeg is.

Een verzameling V heet eindig als er een natuurlijk getal n bestaat zó, dat

$$V \sim \{1, 2, 3, \ldots, n\},$$

en de machtigheid van V wordt dan ook met de letter n aangeduid. We zeggen ook, dat n het aantal elementen van V is. Bovendien wordt ook de lege verzameling eindig genoemd; het betreffende kardinaalgetal wordt met 0 aangeduid.

Is V niet eindig, dan heet V oneindig. We zullen echter zien, dat de oneindige verzamelingen niet alle onderling gelijkmachtig zijn.

Een verzameling V is dan en slechts dan oneindig, als V éénéén-duidig op een echt deel van V kan worden afgebeeld. Een oneindige verzameling bevat steeds een deelverzameling die gelijkmachtig is met N (N = verzameling der natuurlijke getallen). We laten het bewijs van deze beweringen achterwege.

Een verzameling V heet <u>aftelbaar</u> als $V \sim N$. We zullen nu een niet-aftelbare oneindige verzameling aangeven.

We beschouwen afbeeldingen F van N op de verzameling $\{0,1\}$. Zo'n afbeelding is ook te beschrijven door een oneindige rij van nullen en énen, bijv.

$$(0, 0, 1, 1, 0, 1, 0, 0, 0, \ldots),$$

die ontstaat door achtereenvolgens F(1), F(2), F(3), ... op te schrijven. De verzameling van alle mogelijke rijen van dit type noemen we V.

Duidelijk is, dat V niet eindig is (heeft men n zulke rijen, dan is er steeds een nieuwe aan te geven). Neem nu aan, dat V aftelbaar is. Er is dan een éénéénduidige afbeelding van V op N, bijv.

$$\begin{aligned} 1 &\to (\underline{0}, 0, 1, 1, 0, 1, 0, 0, 0, \ldots) = F_1 \\ 2 &\to (0, \underline{1}, 0, 1, 1, 0, 1, 1, 1, \ldots) = F_2 \\ 3 &\to (1, 0, \underline{1}, 1, 0, 0, 1, 0, 0, \ldots) = F_3. \end{aligned}$$

Construeer nu een nieuwe rij als volgt: Beschouw de rij

$$(0, 1, 1, \ldots)$$

die ontstaat door de onderstreepte cijfers achter elkaar te zetten (het is de rij $F_1(1), F_2(2), F_3(3), \ldots$). Maak uit deze een andere, door overal 0 door 1 en 1 door 0 te vervangen. Noem deze nieuwe rij F. Dan is F niet gelijk aan één der F_n's (F wijkt op de n-de plaats van F_n af). Het was dus geen afbeelding van N <u>op</u> V maar alleen <u>in</u>, in strijd met de onderstelling.

De machtigheid van W heet de <u>machtigheid van het continuum</u> (de naam hangt samen met het feit dat W gelijkmachtig is met de verzameling der reële getallen, maar dat bewijzen we nu niet).

Een belangrijke stelling is nog: De vereniging van aftelbaar vele aftelbare verzamelingen is weer aftelbaar.

Bewijs: Laat $V_1, V_2, V_3, \ldots$ elk aftelbaar zijn, en zij V de vereniging van alle V_n's. De elementen van V_k geven we aan met $v_{k1}, v_{k2}, v_{k3}, \ldots$,

Nu is V opgebouwd uit de elementen:

$$v_{11},\ v_{12},\ v_{21},\ v_{13},\ v_{22},\ v_{31},\ v_{14},\ v_{23},\ v_{32},\ v_{41},\ v_{15},\ \ldots\ .$$

Laat hieruit elk element weg dat reeds eerder voorkwam. Wat overblijft kan worden genummerd.

Toepassing: De verzameling van alle rationale getallen is aftelbaar.

Som en product van kardinaalgetallen. De som van twee kardinaalgetallen is als volgt gedefiniëerd. Laat a en b kardinaalgetallen zijn. Kies een verzameling V die de machtigheid a heeft, en een verzameling W met de machtigheid b. We kunnen W zó kiezen, dat de doorsnede van V en W leeg is. Het kardinaalgetal c van de vereniging V ∪ W noemen we nu de som van de kardinaalgetallen a en b. Gemakkelijk is in te zien, dat c niet afhangt van de speciale keuzen van V en W die we hebben gemaakt. Het product van a en b is gedefiniëerd als de machtigheid van het cartesische product $V \times W$.

Men kan laten zien, dat voldaan is aan de gewone regels voor de optelling en vermenigvuldiging: $a + b = b + a$, $a + (b + c) = (a + b) + c$, $ab = ba$, $a(bc) = (ab)c$, $a(b + c) = ab + ac$ (we laten de bewijzen achterwege).

Zijn a en b eindige kardinaalgetallen, dus niet-negatieve gehele getallen, dan stemmen $a + b$ en ab met de ons bekende som en product overeen.

Stellingen als: "bij gegeven a en b is er hoogstens één x met $a + x = b$", en "hoogstens één y met $ay = b$", gaan echter verloren als men van de eindige kardinaalgetallen op oneindige overstapt. Stellen we de machtigheid der aftelbare verzamelingen door $\aleph_o$ voor, dan is bijv.

$$\aleph_o + \aleph_o = \aleph_o \quad \text{en ook} \quad \aleph_o + 0 = \aleph_o;$$
$$\aleph_o\ \aleph_o = \aleph_o \quad \text{en ook} \quad \aleph_o \cdot 1 = \aleph_o.$$

Om dit in te zien, bedenke men, dat de vereniging van twee aftelbare verzamelingen weer aftelbaar is, resp. dat de vereniging van aftelbaar vele aftelbare verzamelingen weer aftelbaar is.

§ 7. Verschillende betekenissen van het woord "oneindig"

Dit woord wordt in de wiskunde in een aantal uiteenlopende betekenissen gebruikt. In verschillende gevallen is het eigenlijk overbodig,

doch door het gebruik geijkt. We geven enkele voorbeelden:

a. "als n loopt van 1 tot ∞" betekent "$\forall_{n\in\mathbb{N}}$".
b. "als x loopt van 1 tot ∞" betekent "$\forall_{x>1}$".

Uit de omgevende tekst blijkt eigenlijk pas welk van de gevallen a of b men op het oog heeft. Het feit dat men gehele getallen bij voorkeur met letters als n, m, k, ... aanduidt, en reële getallen met a, b, ..., x, y, ... is daarbij een steun.

Denk vooral niet, dat het symbool ∞ een getal voorstelt!

c. "Oneindige verzameling". Hiervan is de betekenis in § 6 uiteengezet.
d. "oneindig ver punt" betekent in de meetkunde: "een richting". (zie § 5). Tegenwoordig zegt men meestal "oneigenlijk punt" i.p.v. "oneindig ver punt".
e. "de rechte op oneindig" betekent: de verzameling van alle richtingen in het platte vlak.
f. "Oneindige rij" betekent: een functie gedefinieerd op de verzameling der natuurlijke getallen. Men kan de functiewaarden rangschikken in dezelfde volgorde als de natuurlijke getallen zelf, en schrijft dan

$$a_1, a_2, a_3, \ldots$$

als a_n het ding voorstelt dat door de functie aan het natuurlijke getal n is toegevoegd.
g. "oneindige reeks" betekent: een uitdrukking van de vorm

$$a_1 + a_2 + a_3 + \ldots$$

d.w.z. een rij getallen verbonden door plustekens.
h. "oneindig interval" betekent: een verzameling reële getallen van de vorm $\{x \mid x > a\}$ of $\{x \mid x \geq a\}$ e.d. Om deze intervallen aan te duiden gebruikt men vaak het symbool ∞: $\{x \mid x > a\}$ wordt met (a,∞) aangeduid. Ook een symbool $-\infty$ komt hier op het toneel: $\{x \mid x < a\}$ wordt met $(-\infty,a)$ genoteerd.
i. Is f de functie, gedefinieerd door:

$$\forall_{x\neq 1}\left(f(x) = \frac{1}{x-1}\right)$$

dan is voor x = 1 de functie niet gedefinieerd. Uit een soort ergernis daarover en in verband met het feit dat f(x) in absolute

waarde zeer groot is, als x erg dicht bij 1 ligt, zegt men wel eens "f(1) is oneindig". Dit is een gevaarlijk gebruik, dat zoveel mogelijk vermeden moet worden. (Het lijkt n.l. een uitspraak te zijn over f(1), doch f(1) is niet gedefiniëerd!)

j. "n nadert tot oneindig". Dit betekent op zichzelf helemaal niets. Slechts zekere samenstellingen hebben betekenis, als: a_n nadert tot nul als n tot oneindig nadert.

k. Aan het systeem der complexe getallen voegt men wel eens een extra element toe dat ∞ wordt genoemd. Dit completeert het complexe getallenvlak tot de z.g. complexe bol. Evenzo voegt men wel eens aan het systeem der reële getallen twee nieuwe elementen toe, n.l. $-\infty$ en $+\infty$, waardoor het z.g. systeem der gegeneraliseerd reële getallen ontstaat.

§ 8. Ontwikkeling van het getalbegrip

Oorspronkelijk betekende het woord "getal" eenvoudig "aantal", dus "natuurlijk getal". Langzamerhand is men voor steeds grotere klassen van objecten eveneens het woord "getal" gaan gebruiken. Tegenwoordig is de betekenis van het woord getal tot stilstand gekomen, om "complex getal" aan te duiden. In vele gevallen zal men het echter in beperkter zin gebruiken. Welke zin dat is, blijkt dan wel uit het verband.

We onderscheiden de volgende getallenverzamelingen:

a. Natuurlijke getallen (1, 2, 3, ...). Tegenwoordig rekenen vele auteurs ook de 0 tot de natuurlijke getallen; wij zullen dit niet doen.

b. Gehele getallen. Ontstaan door de negatieve gehele getallen -1, -2, ... en de 0 aan het systeem der natuurlijke getallen toe te voegen.

c. Rationale getallen. Ontstaan door aan het vorige systeem de breuken toe te voegen.

d. Reële getallen. Ontstaan door de z.g. irrationale getallen toe te voegen.

e. Complexe getallen. Ontstaan door de z.g. imaginaire getallen toe te voegen.

De bovenstaande beschrijvingen suggereren definities te zijn, maar zijn het niet, zolang de toe te voegen objecten niet precies zijn gedefiniëerd.

De geschetste volgorde is niet precies de historische: zo zijn bijv. de negatieve getallen veel later ingevoerd dan de positieve breuken. Men heeft trouwens in het verleden heel veel met bepaalde getallensystemen gewerkt zonder ze nauwkeurig gedefiniëerd te hebben, geleid door een zekere intuïtie. Voor de reële getallen heeft deze toestand bijv. duizenden jaren bestaan.

We vermelden hier in het kort de definities van de systemen a t.e.m. e. De verzamelingen van alle natuurlijke getallen hebben we reeds eerder N genoemd. Voor de andere systemen gebruiken we de symbolen G_h, R_t, R_e, C_x (er bestaan echter geen algemeen ingeburgerde symbolen voor). Onze beschrijvingen zullen niet volledig zijn, en dienen uitsluitend om een beeld van de ontwikkeling te geven.

a. Voor de natuurlijke getallen vermeldden we reeds de axioma's van Peano. In § 5 noemden we de eigenschappen van optelling en vermenigvuldiging. Verder is het een geordend systeem: we schrijven $p < q$ (of $q > p$) als in de rij der natuurlijke getallen q later optreedt dan p. Men kan dan nog stellingen bewijzen van de vorm:

$$\forall_{p,q,r,s \in N} [((p > q) \,\&\, (r \geq s)) \Longrightarrow p + r > q + s]$$
$$\forall_{p,q,r \in N} [\; p > q \Longrightarrow rp > rq \;].$$

b. Is $a \in N$, $b \in N$, dan is er hoogstens één x met $x \in N$, $b + x = a$. Maar het is niet altijd waar, dat er minstens één zo'n x bestaat. Om aan deze misstand een einde te maken, voeren we als volgt een nieuw systeem in. We gaan uit van het cartesisch product $N \times N$. Daarin definiëren we een equivalentierelatie: de paren (a,b) en (c,d) (met $a \in N$, $b \in N$, $c \in N$, $d \in N$) noemen we equivalent als $a + d = b + c$. Men kan laten zien, dat dit een equivalentierelatie is. De equivalentieklassen worden nu gehele getallen genoemd.

In dit systeem kan men de begrippen som, product en volgorde definiëren, en daarvoor een aantal regels afleiden die we hier niet zullen noemen.

Het zojuist beschreven systeem bestaat uit geheel nieuwe objecten, zodat we niet kunnen zeggen, dat het een uitbreiding is van N. We zullen nu N in G_h "inbedden". Dat gaat als volgt:

Er bestaat een éénéénduidige afbeelding van N in G_h, gedefiniëerd door:

$$n \rightarrow \{(n + 1, 1)\},$$

d.w.z. aan het getal $n \in N$ wordt de klasse toegevoegd waarin het paar $(n + 1, 1)$ voorkomt. Laten we het beeld van n bij deze afbeelding even door n' voorstellen, en laat N' de verzameling $\{n' \mid n \in N\}$ aanduiden (dus $N' \subset G_h$). Dan geldt:

$$\forall_{n\in N,\ m\in N}[(n + m)' = n' + m']$$
$$\forall_{n\in N,\ m\in N}[(nm)' = n'm']$$
$$\forall_{n\in N,\ m\in N}(n > m \Longleftrightarrow n' > m').$$

Dit betekent, dat alle uitspraken in het systeem N kunnen worden vertaald tot uitspraken in het systeem N'; alleen de <u>namen</u> zijn veranderd. We noemen de systemen N en N' isomorf t.a.v. de begrippen optelling, vermenigvuldiging en volgorde. Het kan geen kwaad om de getallen n en n' als gelijk te beschouwen, want in geen enkele uitspraak over optelling, vermenigvuldiging of volgorde kan dat enige verwarring geven.

Dit is een beetje ruw gezegd, want we weten niet wat het betekent als we zeggen, dat we twee verschillende dingen als gelijk beschouwen. We zeggen het alleen ter bekorting, want anders worden alle verdere uitspraken over onze systemen belast met het woord "isomorfie" en met gecompliceerde zinswendingen. Letterlijk genomen is het echter onzin. Een dergelijke, eigenlijk verboden, identificatie komt veel vaker voor dan men denkt. Jan spreekt bijv. over de natuurlijke getallen 1, 2, 3, 4, 5, 6, ... en Piet spreekt over I, II, III, IV, V, VI, ... Er is dan een isomorfie tussen de mogelijke uitspraken van Jan en Piet. We zijn direct geneigd om te zeggen, dat ze over dezelfde getallen spreken, doch alleen andere namen gebruiken. In feite spreken ze over verschillende dingen.

<u>c</u>. De uitbreiden van G_h tot R_t gaat op soortgelijke wijze als die van N tot G_h. We beschouwen daartoe weer paren (a,b), doch beperken ons nu tot paren met $b \neq 0$. We definiëren de equivalentie deze keer door

$$(a,b) \sim (c,d) \Longleftrightarrow ad = bc.$$

De verzameling van alle equivalentieklassen noemen we R_t. Ook in dit systeem R_t kan men optelling, vermenigvuldiging en volgorde definiëren, en daarvoor een aantal regels afleiden.

We kunnen G_h in R_t inbedden door de afbeelding

$$g \in G_h, \text{ dan } g \to \{(g,1)\}.$$

$\{(g,1)\}$ stelt de klasse voor waarin het paar $(g,1)$ voorkomt.

Met R_t is een systeem verkregen waarin zowel de aftrekking als de deling onbeperkt uitvoerbaar is, behalve het delen door 0. De regels voor de optelling en vermenigvuldiging kunnen we uitdrukken door te zeggen, dat R_t een commutatief lichaam is (zie § 11). De regels voor de ordening zijn de volgende:

$$\begin{aligned}
&\forall_{a,b} && (\text{òf } a = b,\ \text{òf } a < b,\ \text{òf } b < a),\\
&\forall_{a,b,c} && [(a < b \ \&\ b < c) \Longrightarrow a < c],\\
&\forall_{a,b,c} && (a < b \Longrightarrow a + c < b + c),\\
&\forall_{a,b,c} && [(a < b \ \&\ c > 0) \Longrightarrow ac < bc].
\end{aligned}$$

d. De uitbreiding van R_t tot R_e wordt in de analyse behandeld. De uitbreiding dient o.a. om het limietbegrip groter toepasbaarheid te geven.

e. De uitbreiding van R_e tot C_x gaat bijv. als volgt: Beschouw alle paren (a,b) $(a \in R_e,\ b \in R_e)$. We voeren geen equivalentierelatie in. We definiëren product en som door:

$$(a,b) + (c,d) = (a+c, b+d) \qquad (a,b)(c,d) = (ac-bd, ad+bc).$$

Volgorde wordt niet gedefiniëerd. Inbedding van R_e in C_x door $a \to (a,0)$. Het paar $(0,1)$ wordt i genoemd.

C_x vormt weer een commutatief lichaam.

Een voorbeeld waaruit het nut van de complexe getallen duidelijk spreekt is het volgende: Elke hogeremachtsvergelijking heeft in het lichaam C_x minstens één wortel. Daar ook de complexe getallen in de analyse worden behandeld, zullen we niet op deze eigenschappen ingaan.

§ 9. Elementaire rekenkunde

Deze houdt zich bezig met eigenschappen van gehele getallen. In deze paragraaf zullen we, ook als het niet uitdrukkelijk wordt gezegd, alle Latijnse letters gehele getallen laten voorstellen.

a heet <u>deelbaar op</u> b, b <u>deelbaar door</u> a, als $\exists c(ac = b)$.
Notatie: $a \mid b$.

b heet <u>ondeelbaar</u> als $\forall a[(a \mid b) \Longrightarrow (a = \pm 1 \text{ of } a = \pm b)]$.

p heet <u>priemgetal</u> als p ondeelbaar is en $p > 1$. De kleinste priemgetallen zijn 2, 3, 5, 7, 11, 13, 17, ...

We vermelden zonder bewijs:

1. Is p priem, $p \mid ab$, dan is $p \mid a$ of $p \mid b$.
2. (Hoofdstelling der rekenkunde). Elk natuurlijk getal n is te schrijven als product van een (eindig) aantal priemfactoren (waaronder gelijke mogen voorkomen). Twee verschillende ontbindingen van n in priemfactoren verschillen slechts in de volgorde der factoren.

Laat a en b gehele getallen zijn, niet beide nul. Beschouw de verzameling

$$V = \{ax + by \mid x \in G_h,\ y \in G_h\}.$$

Het kleinste positieve getal uit V noemen we de G.G.D. (grootste gemene deler) van a en b. Stellen we deze door g voor, dan geldt:

$$c \in V \Longrightarrow g \mid c.$$

We kunnen n.l. c schrijven als ax + by, en ook als gq + r ($0 \leq r < g$), en we kunnen g schrijven als $ax_o + by_o$. Nu blijkt dat

$$r = a(x - qx_o) + b(y - qy_o),$$

dus $r \in V$. Was $0 < r < g$, dan was g niet het kleinste positieve element van V. Dus r = 0, en dus c = qg, q.e.d. Dus alle getallen van V zijn veelvouden van g.

Omgekeerd ligt elk veelvoud van g in V:

$$kg = k(ax_o+by_o) = a(kx_o) + b(ky_o) \in V.$$

Daar ook a en b in V liggen (kies x = 1, y = 0, resp. x = 0, y = 1), blijkt dat $g \mid a$ en $g \mid b$.

Verder is elke gemeenschappelijke deler van a en b deelbaar op g:

$$d \mid a \ \&\ d \mid b \longrightarrow d \mid g,$$

eenvoudig omdat g de vorm ax + by heeft.

De G.G.D. van a en b wordt gewoonlijk met (a,b) aangeduid.

Gemakkelijk zien we nu: Is p een priemgetal, en a niet deelbaar door p, dan is er een geheel getal x zó dat ax een p-voud +1 is. Want (a,p) is een deler van p, dus = 1 of = p, maar daar a niet door p deelbaar is, en wel door (a,p), is $(a,p) \neq p$, dus (a,p) = 1. Dus 1 heeft de vorm ax + py.

Hiermee bewijst men de eerder genoemde stelling: is $p \mid ab$ dan is $p \mid a$ of $p \mid b$. Is n.l. niet $p \mid a$, dan is er een x zó dat ax een p-voud +1 is, dus (ab)x een p-voud + b. Daar ab een p-voud is, blijkt dat b een p-voud is.

Zij m een natuurlijk getal. We kunnen dan in G_h een equivalentierelatie invoeren door de afspraak

$$a \sim b \longleftrightarrow m \mid (a - b).$$

Ga na, dat het een equivalentierelatie is. In plaats van $a \sim b$ schrijft men

$$a \equiv b \pmod{m}.$$

(Spreektaal: a congruent met modulo m). m heet de modulus van de congruentie.

De equivalentieklassen heten <u>restklassen</u>, of uitvoeriger: restklassen modulo m. Het aantal bedraagt m.

Ga na, dat

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a + c \equiv b + d \pmod{m} \\ ac \equiv bd \pmod{m}. \end{array}\right.$$

Laat α en β restklassen mod m voorstellen. Laat a een getal uit α zijn, en b een getal uit β. Noem $a + b = c$, en geef de restklasse waartoe c behoort met γ aan. Ga na, dat γ niet afhangt van de speciale keuze van a uit α en van b uit β. De klasse γ heet de <u>som</u> van α en β: notatie $\gamma = \alpha + \beta$.

Evenzo wordt het product $\alpha\beta = \delta$ gedefiniëerd door de afspraak dat δ de klasse van ab is.

De genoemde bewerkingen voldoen aan de volgende regels (0 stelt de klasse voor waarin het getal 0 ligt, en 1 de klasse waarin het getal 1 ligt):

$$\begin{array}{ll} \forall_{\alpha,\beta,\gamma} & [\alpha+\beta = \beta+\alpha,\ \alpha+(\beta+\gamma) = (\alpha+\beta)+\gamma,\ \alpha+0 = \alpha] \\ \forall_{\alpha,\beta} & [\text{er is één en slechts één } \xi \text{ met } \alpha + \xi = \beta] \\ \forall_{\alpha,\beta,\gamma} & [\alpha\beta = \beta\alpha,\ \alpha(\beta\gamma) = (\alpha\beta)\gamma,\ 1.\alpha = \alpha,\ \alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma]. \end{array}$$

Deze eigenschappen worden uitgedrukt door te zeggen, dat de restklassen mod m een <u>commutatieve ring</u> vormen (zie § 11).

Is de modulus een priemgetal p, dan geldt bovendien:

$$\forall_{\alpha\neq 0}\ \forall_{\beta}\ (\alpha\xi = \beta \text{ éénduidig oplosbaar}).$$

Om dit te bewijzen laten we zien, dat, als p niet deelbaar is op a, er bij gegeven a en b een x is met $ax \equiv b \pmod{p}$, dus $p \mid ax - b$. M.a.w. dat b de vorm $ax + py$ heeft. Voldoende hiertoe is, dat b deelbaar

is door de G.G.D. van a en p. Deze G.G.D. is een deler van p, dus =1 of =p. Daar de G.G.D. ook een deler van a is, is p zelf uitgesloten, dus de G.G.D. is 1. Daar b deelbaar is door 1, is nu de bewering bewezen.

De zojuist bewezen eigenschap zegt, tezamen met de ringeigenschappen, dat de restklassen mod p een commutatief lichaam vormen (zie § 11).

We bewijzen nog de volgende <u>stelling van Fermat</u>: Is p priem, dan is:

$$\forall_a \, [a^p \equiv a \pmod p].$$

Bewijs: Voor $a \equiv 0 \pmod p$ is de bewering juist. Voor $a \not\equiv 0 \pmod p$ geldt, dat de restklassen:

$$\{a\},\ \{2a\},\ \{3a\},\ \ldots,\ \{(p-1)a\}$$

alle verschillend zijn, en alle verschillend van 0 ($\{x\}$ betekent hier: de restklasse waarin x voorkomt). Derhalve zijn het, in de een of andere volgorde, de restklasse $\{1\},\ \{2\},\ \ldots,\ \{p-1\}$. Bijgevolg hebben de beide systemen hetzelfde product:

$$\{a\} \,.\, \{2a\} \,.\, \ldots \,.\, \{(p-1)a\} = \{1\}.\ \{2\} \,.\, \ldots \,.\, \{p-1\}.$$

Daar 1, 2, ..., p-1 niet door p deelbaar zijn, mogen we deze factoren links en rechts weglaten, en er blijft over:

$$\{a\} \,.\, \{a\} \,.\, \ldots \,.\, \{a\} = 1, \text{ d.i. } a^{p-1} \equiv 1 \pmod p.$$

We keren nog even terug naar het geval van een willekeurige modulus m. De restklasse α heet onderling ondeelbaar met m, als $\alpha = \{a\}$, en a met m de G.G.D. 1 heeft. Het systeem van alle met m onderling ondeelbare restklassen noemen we even M. Door toepassing van de hoofdstelling der rekenkunde is het niet moeilijk in te zien, dat

$$(\alpha \in M \ \&\ \beta \in M) \Longrightarrow \alpha\beta \in M,$$

en op dezelfde wijze als in het geval van de priemmodulus bewijst men, dat

$$(\alpha \in M \ \&\ \beta \in M) \Longrightarrow [(\xi \in M \ \&\ \alpha\xi = \beta) \text{ éénduidig oplosbaar}].$$

Op grond van deze eigenschappen, samen met de z.g. associatieve wet, zeggen we, dat M een <u>groep</u> is (zie § 10).

Het aantal elementen van M heet de <u>indicator van Euler</u>, en wordt met $\varphi(m)$ aangeduid. We vermelden (zonder bewijs) de formule voor $\varphi(m)$. Is $m = p_1^{k_1} \ldots p_t^{k_t}$ ($p_1, \ldots, p_t$ twee aan twee verschillende priemgetallen,

$k_1 > 0, \ldots, k_t > 0$), dan is

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_t}).$$

(Bijv. $\varphi(90) = 90(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 24$).

§ 10. Groepen

Laat G een verzameling zijn, waarbij een afbeelding van $G \times G$ in G gegeven is. Door deze afbeelding is dus aan elk paar $(a,b)(a \in G, b \in G)$ een element $c \in G$ toegevoegd. Als de woorden "vermenigvuldiging" en "product" in het systeem G nog geen vaste betekenis hebben, kunnen we deze c het "product" van a en b noemen, en met $a \times b$ of ab aanduiden. Met evenveel recht (en we zullen dit ook wel eens doen) kunnen we het de som noemen, en $a + b$ gebruiken. In het eerste geval zeggen we, dat de bewerking multiplicatief, in het tweede geval, dat zij additief is geschreven. Voorlopig houden we ons bij de multiplicatieve schrijfwijze.

Dat we de bewerking $(a,b) \to c$ vermenigvuldiging hebben genoemd $(ab = c)$, impliceert niet, dat noodzakelijk steeds $ab = ba$ zou moeten zijn. Is dit wèl steeds het geval, dan heet de vermenigvuldiging commutatief.

G heet een groep (t.o.v. de beschouwde bewerking), als

1°. $\forall_{a,b,c}[(ab)c = a(bc)]$.

2°. $\exists_e \forall_a[(ea = a) \ \& \ (xa = e \text{ is oplosbaar})]$.

De letters a, b, c, e, x stellen elementen van G voor.

We leiden eerst af dat een e die aan 2° voldoet, ook voldoet aan $\forall_a \ ae = a$. Kies een x met $xa = e$ en een y met $yx = e$. Dan is wegens $(yx)a = y(xa)$, ook $ea = ye$, dus $a = ye$. Dus $ae = (ye)e = y(ee) = ye = a$.

Vervolgens blijkt dat er slechts één e voldoet (voldoen e en e' beide, dan is $e'e = e'$ (neem $a = e'$) en $e'e = e$ (neem $a = e$), dus $e' = e$). Deze e wordt het eenheidselement van G genoemd. Verder blijkt uit 1° en 2°, dat $xa = e$ en $ay = e$ éénduidig oplosbaar zijn, en dat deze oplossingen gelijk zijn.

(Bewijs: Kies x zó, dat $xa = e$. Kies bij x een w zó, dat $wx = e$. Nu is $w = we = w(xa) = (wx)a = ea = a$, dus $w = a$. Derhalve is $ax = e$. Dus $ay = e$ heeft een oplossing, n.l. x. Verder volgt uit $az = e$, dat

$z = ez = (xa)z = x(az) = xe = x$, dus $z = x$. Elke oplossing van $ay = e$ is dus gelijk aan elke oplossing van $xa = e$. Derhalve zijn beide vergelijkingen éénduidig oplosbaar).

Uit de genoemde eigenschappen blijkt verder nog, dat voor alle a en b de vergelijkingen $ax = b$ en $ya = b$ éénduidig oplosbaar zijn. (Als $b = e$ is, hebben beide vergelijkingen dezelfde oplossing, maar voor willekeurige b is dit niet meer altijd waar.)

De oplossing van $ax = xa = e$ wordt de <u>inverse</u> van a genoemd, en met a^{-1} aangeduid.

<u>Voorbeelden</u>: 1. Een afbeelding f van het platte vlak in zichzelf heet een <u>beweging</u> als voor alle punten P en Q geldt, dat de afstand PQ gelijk is aan de afstand f(P)f(Q), terwijl van elke driehoek PQR de omloopszin dezelfde is als van de beelddriehoek f(P)f(Q)f(R).

We definiëren nu het product van de bewegingen f en g als $fg = h$, waarin h is gedefiniëerd door:

$$\forall_P[h(P) = f(g(P))].$$

h(P) ontstaat dus door eerst het beeld van P bij g te zoeken, en die g(P) weer aan de afbeelding f te onderwerpen.

De <u>identieke afbeelding</u> e is de afbeelding met $\forall_P(e(P) = P)$. Het is nu niet moeilijk om de regels 1^o en 2^o te bewijzen. De bewegingen vormen dus een groep, de z.g. bewegingsgroep van het platte vlak, en e is daarvan het eenheidselement.

Ga na, dat fg niet steeds hetzelfde is als gf.

De x met $xf = e$ heet de inverse van f en wordt met f^{-1} aangeduid. Het is de beweging die het resultaat van f weer teniet doet:
Is $f(P) = P'$ dan is $x(P') = P$.

2. We hadden zoëven een groep van afbeeldingen, een z.g. <u>transformatiegroep</u>. De getransformeerde objecten waren de punten van het vlak. We zullen nu een analoog geval beschouwen waarbij er slechts eindig vele objecten zijn.

We beschouwen n objecten, en geven die met 1, ..., n aan. De verzameling van deze n objecten heet V_n.

Een afbeelding van V_n op V_n is automatisch een éénéénduidige afbeelding. Zo'n afbeelding heet een permutatie. We geven zo'n permutatie met P aan, en P(i) betekent het beeld van het object i. (Soms duidt men met "permutatie" een ander begrip aan, n.l. de rij P(1), P(2),...,P(n).)

Als we het product weer definiëren door PQ = R, waarbij R is bepaald door $\forall_{i \in V_n} [R(i) = P(Q(i))]$, dan blijkt weer dat de verzameling van alle permutaties van V_n een groep wordt, de z.g. symmetrische groep bij n objecten. Het aantal elementen bedraagt: n!.

In de voorbeelden 3 t.e.m. 6 is met de groepsvermenigvuldiging bedoeld de vermenigvuldiging die we in die systemen al kenden.

3°. De rationale getallen $\neq 0$.
4°. De reële getallen $\neq 0$.
5°. De positieve reële getallen.
6°. De complexe getallen $\neq 0$.

In de voorbeelden 7 t.e.m. 12 zullen we de groepsbewerking optelling noemen, en daarmee is dan de in die systemen reeds bekende optelling bedoeld.

7°. De gehele getallen.
8°. De rationale getallen.
9°. De reële getallen.
10°. De complexe getallen.
11°. De (van een centraal punt uitgaande) vectoren in het platte vlak.
12°. De restklassen mod m.

De voorbeelden 3° t.e.m. 12° zijn commutatieve groepen. Een commutatieve groep wordt meestal abelse groep genoemd (naar N.H. Abel, 1802-1829).

§ 11. Ringen en lichamen

Dit zijn verzamelingen waarop twee bewerkingen zijn gedefinieerd, die we resp. optelling en vermenigvuldiging noemen. Zo'n systeem R heet een ring, wanneer:

1°. R is een abelse groep t.o.v. de optelling. Het eenheidselement daarvan wordt met 0 aangeduid.
2°. De vermenigvuldiging is associatief: $a(bc) = (ab)c$.
3°. De bewerkingen zijn verbonden door de distributieve wetten

$$a(b + c) = ab + ac \quad \text{en} \quad (b + c)a = ba + ca.$$

We spreken over een lichaam, als bovendien geldt:
4°. De elementen $\neq 0$ vormen een groep t.o.v. de vermenigvuldiging.

Een ring, resp. lichaam heet commutatief, als de vermenigvuldiging commutatief is.

Voorbeelden van ringen: De gehele getallen; de restklassen mod m.
Voorbeelden van lichamen: De rationale getallen; de reële getallen; de complexe getallen; de restklassen mod p (p priemgetal).

Al deze voorbeelden zijn commutatief.

§ 12. Geschiedenis der wiskunde

We zullen een zeer globaal overzicht geven van de ontwikkeling der wiskunde. Gemakshalve maken we een ruwe indeling in enkele rubrieken. Nauwkeurige scheidingslijnen tussen de verschillende gebieden zijn echter niet steeds te trekken. Men denke vooral niet, dat de verschillende takken van de wiskunde zich onafhankelijk van elkaar hebben ontwikkeld.

Algebra. Hoewel reeds in de oudheid de Indiërs, Babyloniërs en Egyptenaren geduchte rekenmeesters waren, is datgene wat we tegenwoordig algebra noemen daar niet tot hoge ontwikkeling gekomen. Het bleef ongeveer beperkt tot vergelijkingen van de eerste graad en een enkele toevallig eenvoudig oplosbare van hogere graad. Pas de Arabieren, die de kennis der oudheid (hoofdzakelijk via Spanje) omstreeks het einde der middeleeuwen naar de Westeuropese beschaving overbrachten, hebben het verder gebracht, dankzij hun techniek van het letterrekenen. Pas bij Descartes (1596 - 1650) vinden wij het letterrekenen grotendeels in zijn huidige vorm. De complexe getallen bleven van Leibniz (1646-1716) tot Gauss (1777-1855) in een waas van mystiek gehuld; hetzelfde geldt trouwens in iets mindere mate van de negatieve getallen. Overigens was tot ca. 1800 de algebra, wat de geest betreft, niet veel meer dan wat thans op de middelbare school wordt onderwezen.

Gauss was de eerste die vertrouwen in de complexe getallen had, en er door het maken van een meetkundig beeld (het complexe vlak) een hechtere grondslag aan gaf. Hij gaf het eerste bewijs van de stelling dat elke veelterm $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_o$ als product van lineaire factoren is te schrijven.

Tot in het begin van de 19e eeuw was het hoofdprobleem der algebra het oplossen van vergelijkingen van hogere graad door middel van worteltrekkingen (voor de graden 2, 3, 4 was dat reeds bekend in de tijd van Descartes). Pas in 1826 werd door Abel (1802-1829) bewezen, dat zulks in het algemeen onmogelijk was. Omstreeks dezelfde tijd valt het werk van Galois (1811-1832), die door het invoeren van het begrip permutatiegroep de theorie der algebraïsche vergelijkingen volledig opklaarde.

Hoofdzakelijk aan Cauchy (1789-1857) is de determinantentheorie te danken. Ook ontwikkelde Cauchy de groepentheorie zelfs tot een hoog niveau.

In de 19e eeuw beleefde de algebra een ontzagwekkende ontwikkeling, opgestuwd door de getallentheorie (algebraïsche getallenlichamen), de functietheorie (algebraïsche en elliptische functies, e.d.), meetkunde (invariantentheorie) en de verzamelingstheorie (Cantor 1845-1918)). Omstreeks 1900 brak de abstracte algebra baan (studie van lichamen, ringen, idealen, etc. los van het klassieke getalbegrip), sterk onder invloed van Hilbert (1862-1943). Overigens was het abstracte begrip "groep" reeds bij Cauchy aanwezig.

Analyse. Hieronder verstaat men tegenwoordig alles wat op de differentiaal- en integraalrekening steunt, of iets algemener: alles wat op het limietbegrip rust.

De differentiaal- en integraalrekening werd ongeveer gelijktijdig door Leibniz (1646-1716) en Newton (1642-1727) ontdekt, min of meer onafhankelijk van elkaar. De enige die in eigenlijke zin een directe voorloper genoemd mag worden, was Archimedes (287-212 v.C.), die met Newton en Gauss tot de grootste wiskundigen aller eeuwen wordt gerekend. Archimedes berekende allerlei oppervlakten en inhouden met een aan de integraalrekening zeer nauw verwante methode.

Reeds met Newton zette de grootscheepse toepassing van de analyse op de natuurwetenschappen in. Newton zelf veroverde het zonnestelsel ermee. In het bijzonder moet Euler (1707-1783) genoemd worden, die op de meest uiteenlopende gebieden baanbrekend werk verrichtte.

Hoofdzakelijk bij Cauchy (1789-1857) komt de theorie der complexe functies van een complexe veranderlijke (de z.g. functietheorie) tot een hechte fundering. Later gaf Riemann (1826-1866) op de functietheorie een geheel nieuwe visie, die leidde tot een fraaie afgesloten theorie van de algebraïsche functies.

Cauchy heeft de strengheid ingevoerd in de analyse. Vóór Cauchy werkte men slordig, vaak zonder behoorlijke definities, en min of meer intuïtief. Dit gaf herhaaldelijk tot ernstige fouten aanleiding. Zelfs Euler schreef, dat de oneindige reeks 1 - 1 + 1 - 1 + 1 - 1 ... de som $\frac{1}{2}$ had, zonder dat hij een definitie voor de som van een oneindige reeks had gegeven. (Inderdaad kan men met verschillende argumenten betogen, dat het wel eerlijk zou zijn als de som $\frac{1}{2}$ was, maar ook 0 is wel eerlijk).

Vóór Cauchy ging men uit van de gedachte dat allerlei begrippen (zoals getal, limiet, integraal, oneindig) bestonden zonder dat men ze gedefinieerd had. Men dacht, dat men ze slechts behoefde te analyseren; dat men uit de eigenschappen (die men enigszins experimenteel vaststelde) tot de ware inhoud van het begrip zou moeten komen. De voornaamste oorzaak voor deze vreemde geesteshouding is waarschijnlijk de geweldige toepasbaarheid van de analyse in de natuurwetenschappen en in de meetkunde, waardoor men een soort richtsnoer voor de waarheid kreeg. Natuurlijk hebben we nog restanten van deze geesteshouding over, maar deze hebben betrekking op meer fundamentele dingen, zoals het verzamelingsbegrip en de logica.

Een nieuwe denkrichting werd in de analyse gebracht door Hilbert (1862-1943). Deze voerde een vruchtbare meetkundige terminologie in: In een zekere klasse van functies noemt hij elke functie een punt; de gehele klasse heet een ruimte. Er ontstaan dan sterke analogieën met gewone vectorruimten, en de theorie der lineaire integraalvergelijkingen verschijnt als een voortzetting van de gewone lineaire algebra.

Getallentheorie. Hieronder verstaat men de leer der gehele getallen. De eenvoudigste begripsvormingen waren omstreeks 300 v.C. bij Euclides aanwezig. Deze bewijst bijv., dat er oneindig vele priemgetallen bestaan. De theorie der onbepaalde vergelijkingen (dat zijn vergelijkingen waarvan zowel de coëfficiënten als de onbekenden gehele getallen zijn) wordt aan Diophantus (ca. 250 n.C.) toegeschreven, maar schijnt in feite pas later door Arabische mathematici te zijn bewerkt.

Daarna gebeurde er tot Fermat (1601-1665) weinig waardevols. Fermat en Euler (1707-1783) voerden de congruentiesin. Van Fermat tot en met Gauss (1777-1855) hield de getallentheorie zich hoofdzakelijk bezig met

de vele problemen voortvloeiende uit de kwadratische vergelijking $x^2 + ax + b \equiv 0 \pmod{m}$. De 19e eeuw bracht een uitbreiding van het gebied der gehele getallen tot dat der gehele algebraïsche getallen (dat zijn wortels van vergelijkingen

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$ met gehele coëfficiënten $a_0, \ldots, a_{n-1}$): Dirichlet (1805-1859), Kummer (1810-1893), Dedekind (1831-1916).

Reeds door Euler werd de analyse toegepast op de getallentheorie, zij het op nogal formele wijze. Sinds Dirichlet en vooral sinds Riemann (1826-1866) kan men pas van analytische getallentheorie spreken. De belangrijkste vrucht daarvan werd in 1896 geplukt (Hadamard en De la Vallée Poussin): het bewijs van de reeds in 1797 door Legendre vermoede stelling dat $x^{-1}\pi(x)\log x \to 1$ (als $x \to \infty$), waarin $\pi(x)$ het aantal priemgetallen $\leq x$ is, en log x de z.g. natuurlijke logarithme voorstelt.

De getallentheorie is eeuwenlang een bron van inspiratie geweest: grote delen van de analyse, en nagenoeg de gehele moderne algebra, zijn voortgekomen uit getallentheoretische problemen. Thans schijnt deze rol van de getallentheorie ongeveer te zijn uitgespeeld.

Meetkunde. Wat in het V.H.M.O. als meetkunde wordt onderwezen is ongeveer de inhoud van de "Elementen" van Euclides (ca. 300 v.C.), een soort encyclopedie van de Griekse wiskunde. Bij de Grieken, en in het bijzonder bij Euclides, vinden we het eerst een opzet in de vorm van axioma's, definities, stellingen en bewijzen. Wat axioma's en definities betreft, was het werk van Euclides in onze ogen nog maar gebrekkig. We moeten echter bedenken, dat pas Hilbert een correct axiomasysteem voor de euclidische meetkunde gaf, en dat eigenlijk pas omstreeks 1900 de axiomatische methode van Euclides in andere delen van de wiskunde begon door te werken.

Meer dan 2000 jaar zijn de gedachten geconcentreerd geweest op het parallelenaxioma van Euclides. Dit had een heel ander karakter dan de andere, meer triviale, axiomata. Men stelde zich tot doel de waarheid daarvan te bewijzen. In de eerste helft van de vorige eeuw lukte het echter aan te tonen, dat het parallelenaxioma onbewijsbaar was, doordat men systemen construeerde (niet-euclidische meetkunde) waarin aan alle axioma's van Euclides voldaan was behalve aan het parallelenaxioma. Het had dus geen zin meer om te vragen of het parallelenaxioma waar of onwaar was.

Sindsdien is men ook anders gaan denken over axioma's. De vraag naar de "waarheid" van een axioma wordt niet meer gesteld. Een axiomasysteem legt een tak van wiskunde vast, en daarin wordt elke uit de axioma's afleidbare bewering een ware bewering genoemd. De axioma's zijn dus per definitie waar.

Wèl interesseert men zich voor de volgende vragen. 1. Zijn de axioma's van een systeem A onderling afhankelijk (d.w.z. kan één ervan uit de andere worden afgeleid)? 2. Zijn ze in strijd met elkaar? 3. Is er, onder aanname van een axiomasysteem B, iets te construeren dat aan de axioma's A voldoet?

Om terug te komen tot de meetkunde: tot aan Descartes (1596-1650) bleven de "Elementen" van Euclides de hoogst denkbare wijsheid. Descartes vond de analytische meetkunde uit. Om in de taal van onze dagen te spreken: hij construeerde een isomorfie tussen het euclidische vlak en het cartesische product $R_e \times R_e$ (R_e = verzameling der reële

getallen). Door deze coördinatisering werd het mogelijk, meetkundige problemen algebraïsch te formuleren, algebraïsch op te lossen, en tenslotte de oplossing weer meetkundig te interpreteren. Daardoor was men eindelijk verlost van de grilligheid der meetkundige methoden, waarin iedere systematiek ontbrak.

De analytische meetkunde kwam (ook in meer dimensies) in een korte tijd tot snelle ontwikkeling, en behalve de algebra kon ook direct de analyse op de meetkunde worden toegepast (differentiaalmeetkunde en mechanica).

De klassieke differentiaalmeetkunde kwam tot een zekere afsluiting bij Gauss. De moderne begint bij Riemann. Vóór Riemann was differentiaalmeetkunde de studie van krommen en oppervlakken gelegen in een euclidische ruimte. Riemann wist zich van die euclidische ruimte los te maken. Deze Riemannse differentiaalmeetkunde werd later de basis voor de relativiteitstheorie van Einstein (1879-1955).

Een meetkundige ontwikkeling in geheel andere richting is die der projectieve meetkunde, die zich bezighoudt met die meetkundige eigenschappen die door centrale projectie niet worden verstoord. Het fundament werd gelegd door Desargues (1593-1661), doch de bloeitijd van de projectieve meetkunde ligt omstreeks 1850 (o.a. Steiner 1796-1863)).

Een belangrijke moderne tak van meetkunde is de topologie. De topologie is begonnen als "gummi-meetkunde": de leer der meetkundige eigenschappen die niet veranderen bij continue vervorming. Bijv. de stelling van Jordan, die zegt, dat een gesloten kromme (zonder dubbelpunten) het platte vlak in twee gebieden verdeelt. Grotere waardering voor de topologie ontstond nadat Riemann en Klein (1849-1925) algebraïsche functies interpreteerden als functies op een gesloten oppervlak, waarbij het alleen om de topologie van het oppervlak ging.

Later is de topologie overgegaan tot de studie van het continuïteitsbegrip in algemenere ruimten. Toegepast op functieruimten laten zich nu belangrijke delen van de analyse desgewenst onder de topologie rangschikken.

De analytische meetkunde ontwikkelde zich in de tweede helft van de vorige eeuw in meer algebraïsche richting, en werd meer en meer gezien als de theorie der invarianten van algebraïsche vormen bij groepen van lineaire transformaties. Daarnaast was er een ontwikkeling gaande die de functietheoretische resultaten over algebraïsche en elliptische functies tot toepassing bracht.

Pas tegen het eind van die eeuw begon enige klaarheid te komen in het begrip "multipliciteit" van een punt van een algebraïsche kromme. Dit gaf aanleiding tot abstract algebraïsche beschouwingen; hieruit is de moderne algebraïsche meetkunde voortgekomen.

Toegepaste wiskunde. Er is geen duidelijke scheidingslijn tussen zuivere en toegepaste wiskunde. Onder toegepaste wiskunde verstaat men meestal datgene wat onmiddellijk met de toepassingen samenhangt.

Het is duidelijk, dat het begrip toegepaste wiskunde voortdurend verschuift.

Men kan bijv. bijna de gehele meetkunde der oudheid tot de toepassingen rekenen (geodesie, astronomie), slechts de structuur axioma-definitie - stelling - bewijs staat buiten de directe toepassing. De zuivere wiskunde ontstaat daar waar men zich voor de wiskunde als zodanig gaat interesseren, ongeacht de toepassingsmogelijkheid. Dat wat als zuiver ontstaat, kan later heel goed worden toegepast. Als voorbeelden noemen we de Riemannse meetkunde, die later in de relativiteitstheorie kwam,

en verder de Hilbertruimte en de groepsrepresentaties, die later in de quantummechanica werden toegepast. Aan de andere kant zijn grote delen van de wiskunde opgebouwd naar aanleiding van de behoeften van de natuurwetenschappen en de techniek.

De moderne wiskunde. De hedendaagse wiskunde voldoet aan hoge eisen van strengheid en vertoont de neiging tot steeds groter algemeenheid. Het streven is, alle bestaande resultaten te vervangen door analoge met een zeer veel wijdere strekking, teneinde met één theorie de meest uiteenlopende onderdelen te kunnen bestrijken. Deze veelal zeer vruchtbare abstractie wordt bijv. bereikt door de bestaande stellingen en bewijzen nauwkeurig na te gaan om te zien of er niet iets van de gegevens kan worden gemist.

Beroemd en berucht om dit streven is een groep Franse mathematici die onder de schertsnaam N. Bourbaki een soort encyclopaedie der moderne wiskunde uitgeeft.

§ 13. Waarom die strengheid? De eis naar strengheid wordt opgelegd door het verlangen om bewijzen te hebben. Een huis met een foutje kan nog heel goed bewoonbaar zijn, maar een bewijs met een foutje is helemaal geen bewijs.

De beginneling verwondert zich er altijd over, dat in de beginselen van de analyse zoveel moeilijke bewijzen voorkomen van zaken die wel bijna vanzelf schijnen te spreken. Dat komt doordat het begrip reëel getal enerzijds zo gecompliceerd is, en anderzijds zoveel voorstellingen uit onze aanschouwingswereld oproept waarmee we sinds lang vertrouwd zijn. Men bedenke weer, dat aan "bijna vanzelf spreken" geen enkele bewijskracht toekomt: een bijna-bewijs is helemaal geen bewijs.

De beginneling moge zich troosten met de gedachte, dat het vóór Cauchy nog veel moeilijker was om de analyse te leren.

Eén van de neigingen die de beginneling heeft is, om op grond van verschillende ervaringen, te denken, dat elke naar boven begrensde verzameling van reële getallen een grootste getal bevat. Gaat het over een verzameling als $\{x \mid 0 < x < 2\}$ dan zal hij weldra zijn fout inzien, maar in ingewikkelder gevallen vervalt hij weldra weer in de oude gewoonte.

Een typisch voorbeeld is dat van Steiner en het isoperimetrische probleem. Dit probleem dat reeds door de Grieken is gesteld, behelst het volgende: Bewijs, dat onder alle gesloten krommen die een gegeven oppervlakte insluiten, de cirkel met die oppervlakte degene is die de kleinste omtrek heeft. We zien op het ogenblik door de vingers, dat de woorden "kromme", "oppervlakte" en "lengte" nog zeer veel toelichting behoeven.

Steiner meende het isoperimetrische probleem te hebben opgelost, doordat hij het volgende had bewezen:

(1) Als een gesloten kromme geen cirkel is, dan is er een andere gesloten kromme te vinden met dezelfde oppervlakte en met kleinere omtrek.

Stilzwijgend had hij dus ondersteld, dat in de verzameling van de omtrekslengten van alle krommen die de gegeven oppervlakte hebben, een kleinste getal voorkomt. Dit laatste is wel waar, maar het is niet door Steiner bewezen.

Een analoge drogreden, die echter tot een foutief resultaat leidt, is de volgende: Het getal 1 is het grootste natuurlijke getal. Want de transformatie $x \to x^2$ voert elk natuurlijk getal in een groter over, behalve juist het getal 1.

-.-.-.-