TECHNISCHE HOGESCHOOL EINDHOVEN
Afdeling Algemene Wetenschappen
Onderafdeling der Wiskunde

INLEIDING

in de

METHODEN der WISKUNDE

Dr. S.T.M. Ackermans

Najaarssemester 1970

Onderafdeling der Wiskunde

Inleiding in de methoden der wiskunde

SYLLABUS VAN HET COLLEGE VAN DR. S.T.M. ACKERMANS

GEGEVEN IN HET NAJAARSSEMESTER 1970

TECHNISCHE HOGESCHOOL EINDHOVEN

Dict.nr.: 2.200
Prijs : f 2,--

Inleiding in de methoden der wiskunde.

Syllabus van het college van
Dr. S.T.M. Ackermans
gegeven in het najaars-
semester 1969.

Voorwoord

Het is onmogelijk zich met moderne wiskunde bezig te houden zonder vertrouwd te zijn met de begrippen en notaties die daarin overal gebruikt worden.
De thans heersende opvattingen over strengheid stellen bovendien hoge eisen aan het wiskundige taalgebruik.
We zullen ons in dit college bezig houden met de fundamentele begrippen : *verzameling*, *afbeelding* en *equivalentierelatie*; we zullen vertrouwd raken met een aantal zegswijzen en notaties die thans in de wiskunde algemeen gebruikt worden; we zullen enige voorbeelden van een abstracte wiskundige theorie bestuderen.
In deze syllabus treft men talrijke vraagstukken aan. De student zal er niet in slagen zich correct wiskundig taalgebruik eigen te maken zonder de oefening verkregen door het volledig uitwerken van opgaven.

Inhoud

Hoofdstuk I. Verzamelingen en afbeeldingen.

§ 1. Verzamelingen.

1.1. Het begrip verzameling neemt in de wiskunde een centrale plaats in. We veronderstellen het bekend.

"a is een element van A" noteert men met $a \in A$;

"a is geen element van A" met $a \notin A$.

Andere zegswijzen voor $a \in A$: a ligt in A; a behoort tot A.

Bekende voorbeelden van verzamelingen zijn de verzamelingen der natuurlijke, gehele, rationale, reële getallen, resp. aangeduid met Nt, Gh, Rt, Rl.

Verzamelingen zijn volkomen gekarakteriseerd door hun elementen en niet door hun beschrijving. Zo is er geen verschil tussen: "de verzameling der getallen 2,3,5 en 7" en "de verzameling der priemgetallen ≤ 10." Een van de methoden om verzamelingen aan te geven is alle elementen opschrijven tussen accolades.

$$\{1,2,3\} = \{3,1,2\} \; ; \; \{\{1\}\} .$$

1.2. <u>Inclusie.</u> Laat A en B verzamelingen zijn. A heet een <u>deelverzameling</u> van B (notatie $A \subset B$) indien ieder element van A ook element is van B. In het bijzonder is dus voor iedere verzameling $A : A \subset A$. Is $A \subset B$ en $A \neq B$ dan noemen we A een <u>echte deelverzameling</u> van B.

A is geen deelverzameling van B noteren we als $A \not\subset B$.

$B \supset A$ betekent hetzelfde als $A \subset B$.

Het zal blijken dat onze formules veel eenvoudiger worden als we ook beschouwen de verzameling die geen enkel element bevat; deze zg. <u>lege verzameling</u> noteren we met $\emptyset$.

1.3. Eigenschappen. (Als naar deze eigenschappen verwezen wordt, gebeurt dit met de nummers 1.3.1., 1.3.2. enz.)

1. Is $A \subset B$ en $B \subset C$, dan is ook $A \subset C$.

2. Is $A \subset B$ en $B \subset A$, dan is $A = B$. Vaak bewijst men dat twee verzamelingen A en B gelijk zijn, door te laten zien dat $A \subset B$ en $B \subset A$.

3. Voor iedere verzameling geldt $\emptyset \subset A$.

4. Is U een verzameling, $a \in U$, $A \subset U$, dan is precies één van de beweringen "$a \in A$" en "$a \notin A$" waar.

1.4. Voorbeelden.

Wezenlijk voor de verzamelingenleer is het onderscheid tussen verzameling en element. Verwar nooit $\in$ en $\subset$, a en $\{a\}$.
De voorbeelden 1, 2 en 3 illustreren dit verschil.

1. $1 \in \{1,2,3\}$ maar $\{1\} \subset \{1,2,3\}$.

2. $\emptyset \in \{\emptyset\}$, $\emptyset \subset \{\emptyset\}$

3. Als $F = \{S,T\}$, $S = \{a,b,c,d\}$, $T = \{a,c,e\}$, dan zijn de volgende beweringen juist :
$a \in S$; $\{a,c\} \subset S$; $\{a,c\} \subset T$; $\{S\} \subset F$; $S \in F$; $S \not\subset T$; $T \not\subset S$.

4. $\{1,2,3\} \subset Nt \subset Gh \subset Rt \subset Rl$ en al deze inclusies zijn echt.

5. $A = \{b,n,l\}$. Alle deelverzamelingen van A zijn :
$\emptyset$, $\{b\}$, $\{n\}$, $\{l\}$, $\{n,l\}$, $\{b,l\}$, $\{b,n\}$, A.

1.5. Opgaven. (de opgaven in deze syllabus zijn doorlopend genummerd.)

1. Welke van de volgende verzamelingen zijn aan elkaar gelijk ?

$$\emptyset \ , \ \{0\} \ , \ \{\emptyset\} \ .$$

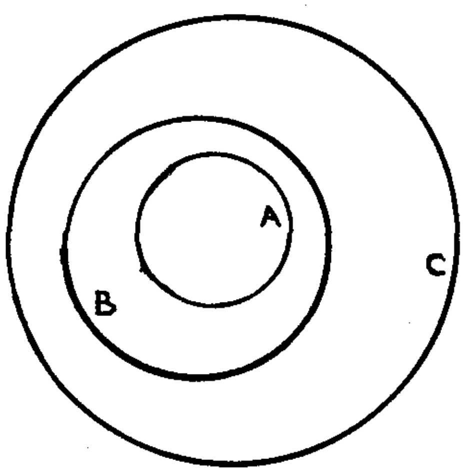
2. Heeft iedere verzameling een echte deelverzameling ?

3. $V = \{0, \{1,2\}\}$. Bepaal alle deelverzamelingen van V; deze vormen een verzameling W, bepaal alle deelverzamelingen van W.

4. Hoeveel verschillende deelverzamelingen heeft een verzameling met n elementen ?

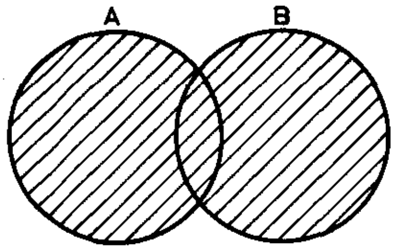
1.6. Venn-diagrammen. Men illustreert verzamelingstheoretische beweringen vaak met zg. Venn-diagrammen. Dit is een voorstellingswijze waarbij men er van uitgaat dat de optredende verzamelingen deelverzamelingen zijn van het blad papier. Venn-diagrammen zijn geen bewijzen; men kan ze wel gebruiken als tegenvoorbeelden.

Bij eigenschap 1.3.1. zou dan het nevenstaande prentje als illustratie kunnen dienen.



1.7. Vereniging. Laat A en B verzamelingen zijn. De vereniging van A en B is per definitie de verzameling bestaande uit de elementen van A en de elementen van B.

In het onderstaande Venn-diagram, geeft de arcering de vereniging aan.



De <u>vereniging</u> van A en B noteert men met $A \cup B$.

De bewering : "$c \in A \cup B$" betekent dus : "$c \in A$ of $c \in B$". "Of" is hier gebruikt in niet uitsluitende zin : het kan zijn dat c element van A is en tevens element van B. In de omgangstaal gebruikt men "of" zowel in uitsluitende zin ("het kan vriezen of dooien") als in niet uitsluitende zin ("als het regent of stormt kom ik niet met de fiets").

<u>Voorbeelden.</u>

1. $Gh \cup Nt = Gh$;
2. $\{1,2,3,4,5\} \cup \{2,4,6\} = \{1,2,3,4,5,6\}$;

<u>Eigenschappen</u> (teken Venn-diagrammen die deze eigenschappen illustreren).

1. Voor alle verzamelingen A en B geldt : $A \subset (A \cup B)$; $B \subset (A \cup B)$.

2. Als $A \subset B$ dan is $A \cup B = B$; in het bijzonder is voor alle verzamelingen A : $A \cup A = A$.

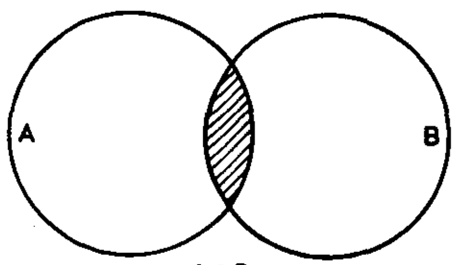
3. Omdat een verzameling volkomen vastligt door de elementen die hij bevat, geldt voor alle A en B : $A \cup B = B \cup A$ (commutativiteit).

4. $A \cup \emptyset = A$.

5. Voor alle verzamelingen A, B en C geldt : $(A \cup B) \cup C = A \cup (B \cup C)$ (associativiteit; men mag schrijven $A \cup B \cup C$).

1.8. Doorsnede. De doorsnede van de verzamelingen A en B (notatie $A \cap B$) is per definitie de verzameling bestaande uit die elementen die zowel element van A zijn als element van B.

Venn-diagram



$A \cap B$

De bewering "$c \in A \cap B$" betekent dus "$c \in A$ en $c \in B$".

Voorbeelden.

1. $Gh \cap Nt = Nt$.
2. $\{1,2,3,4,5\} \cap \{2,4,6\} = \{2,4\}$.

Eigenschappen. (teken Venn-diagrammen)

1. Voor alle verzamelingen A en B geldt : $(A \cap B) \subset A$; $(A \cap B) \subset B$.

2. Als $A \subset B$, dan is $A \cap B = A$; in het bijzonder is voor alle A: $A \cap A = A$.

3. Voor alle A en B geldt : $A \cap B = B \cap A$.

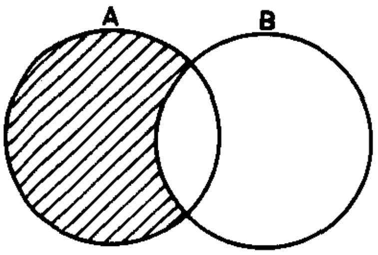
4. $A \cap \emptyset = \emptyset$.

5. Voor alle verzamelingen A, B en C geldt : $(A \cap B) \cap C = A \cap (B \cap C)$.

Definitie. Als $A \cap B = \emptyset$, dan zegt men dat A en B disjunct zijn.

1.9. Verschil. Het verschil van de verzamelingen A en B (notatie $A \setminus B$) is de verzameling van alle elementen van A die niet tevens element van B zijn.

Venn-diagram



De bewering "$c \in A \setminus B$" betekent dus "$c \in A$ en $c \notin B$".

Voorbeelden.

1. $Gh \setminus Nt$ = de verzameling bestaande uit 0 en alle negatieve gehele getallen. $Nt \setminus Gh = \emptyset$.
2. $\{1,2,3,4,5\} \setminus \{2,4,6\} = \{1,3,5\}$.

Eigenschappen. (teken Venn-diagrammen)

1. Voor alle verzamelingen A en B geldt : $(A \setminus B) \subset A$; $A \setminus B$ en B zijn disjunct.
2. Als $A \supset B$ dan is $B \setminus A = \emptyset$; in het bijzonder is voor alle A : $A \setminus A = \emptyset$.
3. $A \setminus \emptyset = A$.

Opmerking. Verschilvorming is niet associatief, d.w.z. de verzamelingen $(A \setminus B) \setminus C$ en $A \setminus (B \setminus C)$ zijn niet steeds gelijk. Als voorbeeld nemen we :
$A = \{0,1,2\}$; $B = \{-2,-1,0\}$; $C = \{-1,0,1\}$.
Dan is : $A \setminus B = \{1,2\}$; $(A \setminus B) \setminus C = \{2\}$;
$B \setminus C = \{-2\}$; $A \setminus (B \setminus C) = A$.

1.10. Eigenschappen. (teken Venn-diagrammen)

Voor alle verzamelingen A, B en C geldt :

$$\left.\begin{array}{ll} 1. & (A \cup B) \cap C = (A \cap C) \cup (B \cap C); \\ 2. & (A \cap B) \cup C = (A \cup C) \cap (B \cup C); \end{array}\right\} \text{(distributiviteitseigenschappen)}$$

3. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
4. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

De bewijzen van vorenstaande en andere eigenschappen bevatten slechts toepassingen van de definities. We spreken alleen over het bewijs van 1.10.1.

Het bewijzen van de gelijkheid van twee verzamelingen doet men vaak in twee stappen (1.3.2). In dit geval zou men kunnen laten zien :

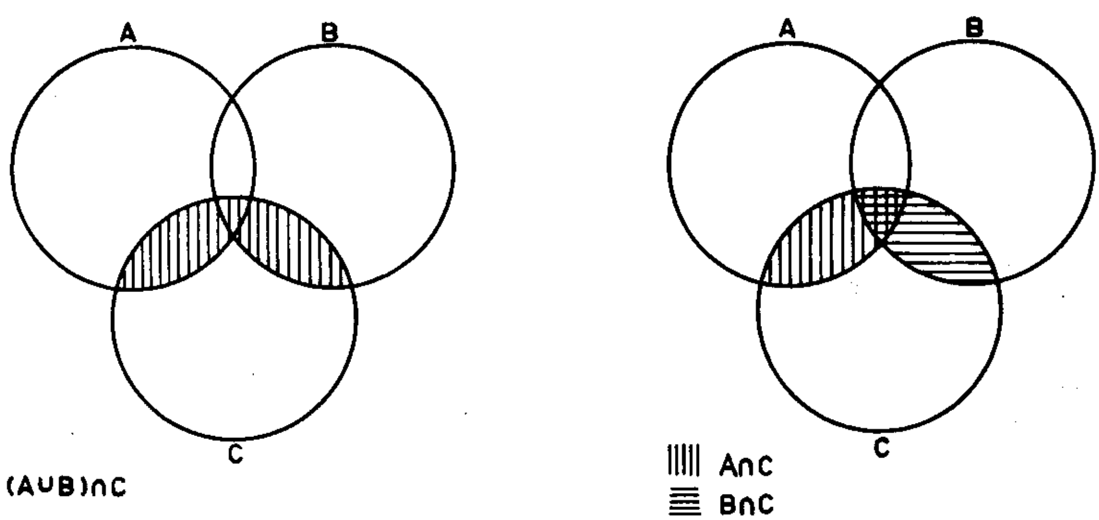
$$(*)\ (A \cup B) \cap C \subset (A \cap C) \cup (B \cap C);$$

$$(**)\ (A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C.$$

Bewijs van (*). We moeten laten zien dat ieder element uit $(A \cup B) \cap C$ ook element is van $(A \cap C) \cup (B \cap C)$. Zij $a \in (A \cup B) \cap C$, dan is $a \in (A \cup B)$ en $a \in C$. Omdat $a \in A \cup B$ geldt $a \in A$ of $a \in B$ eventueel $a \in A$ en $a \in B$. Omdat $a \in C$ is $a \in A \cap C$ als $a \in A$, en $a \in B \cap C$ als $a \in B$. Omdat zeker een van de beide beweringen $a \in A$ of $a \in B$ waar is, is dus zeker een van de beweringen $a \in A \cap C$ of $a \in B \cap C$ waar en dus is $a \in (A \cap C) \cup (B \cap C)$. Aangezien het bovenstaande geldt voor alle elementen uit $(A \cup B) \cap C$ is (*) bewezen.

Het bewijs van (**) kan op soortgelijke manier gegeven worden.

Met Venn-diagrammen kan men 1.10.1 aldus illustreren.



1.11. Zijn in een beschouwing alle voorkomende verzamelingen deelverzameling van een vaste verzameling U dan noemt men het verschil $U\setminus A$ ook wel : <u>complement van A</u> t.o.v. U. U noemt men wel universum. Vaak gebruikt men de notatie A^* voor $U\setminus A$. Met deze notatie kan men de eigenschappen 1.10.3 en 1.10.4 voor het geval dat $A = U$ herschrijven als :

$$(B \cup C)^* = B^* \cap C^* \;;$$

$$(B \cap C)^* = B^* \cup C^* \;.$$

1.12. <u>Opgaven.</u>

5. Zijn de volgende beweringen waar voor ieder drietal verzamelingen A, B, C; zo neen geef een tegenvoorbeeld.

(a) $A \subset ((A \cap B) \cup C)$.

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

(c) $(A\setminus B) \cap C = (A \cap C)\setminus(B \cap C)$.

6. Bewijs de volgende eigenschappen (teken Venn-diagrammen).

(a) Als $A \subset B$ dan is $(A \cup C) \subset (B \cup C)$ en $(A \cap C) \subset (B \cap C)$.

(b) Als $A \subset C$ en $B \subset C$, dan is $(A \cup B) \subset C$.

(c) Als $C \subset A$ en $C \subset B$ dan is $C \subset (A \cap B)$.

7. Bewijs dat voor ieder tweetal verzamelingen geldt :

(a) Als $A \cup B = B$, dan is $A \subset B$.

(b) Als $A \cap B = A$, dan is $A \subset B$.

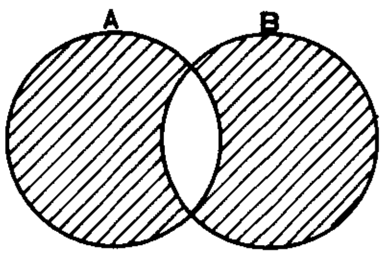
(c) $A\setminus(B\setminus A) = A$.

(d) $A\setminus(A\setminus B) = A \cap B$.

(e) $A \cup B = (A\setminus B) \cup (A \cap B) \cup (B\setminus A)$.

(f) $(A \cup B)\setminus(A \cap B) = (A\setminus B) \cup (B\setminus A)$.

(De verzameling $(A \setminus B) \cup (B \setminus A)$
noteert men als $A \dotdiv B$; het symmetrische
verschil van A en B).



$A \dotdiv B$

§ 2. Het aangeven van verzamelingen; enkele notaties.

2.1. De in § 1 besproken methode om een verzameling aan te geven door middel van een opsomming van de elementen tussen accolades is natuurlijk alleen bruikbaar bij verzamelingen met een gering aantal elementen. Wil men bijv. de verzameling van alle reële getallen die groter dan 1 en kleiner dan 2 zijn aangeven dan lukt die opsomming in het geheel niet. Men neemt in zulke situaties zijn toevlucht tot het gebruik van een veranderlijke en zegt dan bijv. : de verzameling van alle reële x die voldoen aan $1 < x < 2$.
Bekijkt men de zin : $1 < x < 2$ dan is dat geen bewering (je kunt niet zeggen : "ja, dat is waar", of "nee, dat is onwaar") omdat de letter x zelf geen betekenis heeft. Als we voor x een reëel getal invullen (substitueren) dan gaat de zin $1 < x < 2$ over in een bewering, bijv. in "$1 < \frac{1}{2}\pi < 2$" (hetgeen waar is)of "$1 < 3 < 2$" (hetgeen onwaar is).
Zinnen die een veranderlijke bevatten en die overgaan in beweringen indien men voor die veranderlijke iets substitueert noemen we <u>beweringsvormen</u>.
We duiden ze vaak aan met $P(x)$, $Q(x)$, $R(x)$, ... Als men voor x iets invult dan ontstaat er een bewering, die al of niet waar is. We zullen ons bij het substitueren beperken tot de elementen van een bepaalde verzameling : de <u>individuenverzameling</u>. Zo is : "x is een positief getal" een beweringsvorm met Rl als individuenverzameling. "x is een priemgetal" is een beweringsvorm met Nt als individuenverzameling; "7 is een priemgetal" is een juiste bewering; "9 is een priemgetal" is een onjuiste bewering. Als door substitutie van a in $P(x)$ een ware bewering ontstaat dan zeggen we dat a aan de beweringsvorm $P(x)$ voldoet.
Zij $P(x)$ een beweringsvorm met individuenverzameling U, dan geeft men de deelverzameling van U bestaande uit de elementen die aan $P(x)$ voldoen aan met:

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

We zeggen dat $P(x)$ een <u>definiërende beweringsvorm</u> is van de verzameling $P := \{x \mid P(x)\}$.

(<u>Opmerking</u>: Als we = gebruiken in een definitie plaatsen we : aan de kant van de nieuw gedefinieerde grootheid.)

2.2. <u>Voorbeelden.</u>

1. De verzameling van alle reële x die voldoen aan $1 < x < 2$ noteert men als :

$$\{x \mid x \in \mathrm{Rl} \text{ en } 1 < x < 2\} \quad \text{of} \quad \{x \mid x \in \mathrm{Rl},\ 1 < x < 2\} .$$

2. De middelloodlijn van het segment AB in het platte vlak wordt met deze notatie :

$$\{P \mid P \text{ is een punt, } PA = PB\} .$$

Een verzameling van punten die aan een beweringsvorm voldoen heet(te) in de meetkunde vaak : meetkundige plaats.

(Dreigt er geen verwarring dan laat men aanduidingen als P is een punt, $x \in \mathrm{Rl}$ enz. gewoonlijk weg. Men schrijft ook wel $\{x \in \mathrm{Rl} \mid 1 < x < 2\}$.)

3. In de analytische meetkunde geeft men de cirkel met straal 1 om de oorsprong aan met

$$\{(x,y) \mid x^2 + y^2 = 1\} .$$

4. Is A een verzameling, dan is $x \in A$ een beweringsvorm en $A = \{x \mid x \in A\}$.

5. $\mathrm{Nt} = \{x \mid x \in \mathrm{Gh},\ x > 0\}$.

2.3. We kunnen dus een verzameling aangeven door opsomming van zijn elementen, en met behulp van een definiërende beweringsvorm. Er is nog een derde manier in gebruik die een variant is van de tweede. Deze illustreren we aan enige voorbeelden.

1. De verzameling Q van alle kwadraten van natuurlijke getallen kan met behulp van een definiërende beweringsvorm aangegeven worden als :

$$\{y \mid \text{er is een natuurlijk getal } x \text{ met } y = x^2\} .$$

We gebruiken vaak de notatie : $Q := \{x^2 \mid x \in Nt\}$.

2. Volgens dit gebruik kan men de cirkel met straal 1 om de oorsprong in het analytisch-meetkundige vlak beschrijven als :

$$\{(\cos\varphi,\ \sin\varphi) \mid 0 \leqslant \varphi < 2\pi\} .$$

3. Zo is $\{(a + r\cos\varphi,\ b + r\sin\varphi) \mid 0 \leqslant \varphi < 2\pi\}$ de cirkel met straal $|r|$ en middelpunt (a,b).

4. $\{\{(a + r\cos\varphi,\ b+r\sin\varphi) \mid 0 \leqslant \varphi < 2\pi\} \mid a \in Rl,\ b \in Rl,\ r \in Rl,\ r \geqslant 0\}$ is de verzameling van alle cirkels in het platte vlak.

2.4. Opgaven.

8. Welke van de volgende deelverzamelingen van Rl zijn leeg :

(a) $\{x \mid x^2 = 9 \text{ en } 2x = 4\}$;

(b) $\{x \mid x \neq x\}$;

(c) $\{x \mid x + 8 = 8\}$;

(d) $\{x \mid x^2 = 3 \text{ of } x^2 = 1\}$;

(e) $\{x \mid x^2 \geqslant -1\}$.

9. Geef de volgende verzamelingen weer met behulp van een definiërende beweringsvorm

(a) de even getallen;

(b) de cirkels in R_2 (het coördinatenvlak uit de analytische meetkunde) met straal 2;

(c) de rijen reële getallen die naar 2 convergeren;

(d) de functies die in de oorsprong continu zijn.

2.5. Nodige en voldoende voorwaarden. Laat $P(x)$ en $Q(x)$ beweringsvormen zijn met individuenverzameling U. $P := \{x \mid P(x)\}$; $Q := \{x \mid Q(x)\}$.
We zeggen dat $P(x)$ een nodige voorwaarde is voor $Q(x)$ als $Q \subset P$,
$P(x)$ heet een voldoende voorwaarde voor $Q(x)$ indien $P \subset Q$.
Als $P = Q$ dan zeggen we dat $P(x)$ een nodige en voldoende voorwaarde voor $Q(x)$ is; of ook wel dat $P(x)$ en $Q(x)$ gelijkwaardig zijn. Andere zegswijzen die uitdrukken dat $P = Q$: $P(x)$ geldt dan en slechts dan als $Q(x)$; $P(x)$ dan en dan alleen als $Q(x)$.
Als $P(x)$ een nodige voorwaarde voor $Q(x)$ is dan betekent dit dus dat elk individu dat aan $Q(x)$ voldoet ook aan $P(x)$ voldoet. Is a zo'n individu, d.w.z. dat $Q(a)$ waar is, dan is ook $P(a)$ waar. Evenzo; als $P(x)$ een voldoende voorwaarde voor $Q(x)$ is, en als $P(a)$ waar is, dan is $Q(a)$ waar.

Voorbeelden. (Als individuenverzameling treedt Rl op.)

1. $x > 0$ is een nodige voorwaarde voor $x > 1$.

2. $x > 1$ is een voldoende voorwaarde voor $x > 0$.

3. Opdat $x \neq 0$ is nodig en voldoende dat $x^2 > 0$.

Opgave.

10. Ga van de volgende paren beweringsvormen na, of de eerste een nodige en/of voldoende voorwaarde voor de tweede is (de individuenverzameling waar de veranderlijken betrekking op hebben wordt steeds het eerste genoemd).
    (a) Nt; n is een priemgetal; n is deelbaar door 7 .
    (b) Nt; n is deelbaar door 25; n is deelbaar door 5.
    V is de verzameling van alle rijen van reële getallen.

(c) V; $\lim_{n\to\infty} a_n = 0$; $\lim_{n\to\infty} |a_n| = 0$.

(d) V; $\lim_{n\to\infty} a_n = 1$; $\lim_{n\to\infty} |a_n| = 1$.

(e) V; $\lim_{n\to\infty} a_n = -3$; de rij $(a_1, a_2, \ldots)$ is convergent.

(f) V; de rij $(a_1, a_2, \ldots)$ is convergent; de rij $(a_1, a_2, \ldots)$ is begrensd.

(g) V; $\lim_{n\to\infty} a_n = \pi$; $\lim_{n\to\infty} (a_n + \frac{1}{n}) = \pi$.

2.6. En, of, niet.

1. Uit twee beweringen kan men een nieuwe bewering maken door ze te verbinden met het woordje "en". Uit de beweringen: "Eindhoven ligt in Brabant" en "Eindhoven is een stad" ontstaat de bewering : "Eindhoven ligt in Brabant en Eindhoven is een stad". Stelt a een bewering voor en stelt b een bewering voor dat noteert men de bewering "a en b" als $a \wedge b$. Deze laatste bewering is alleen dan waar als a en b beide waar zijn.

2. Evenzo maakt men uit de beweringen a en b de bewering : "a of b", waarbij "of" in niet uitsluitende zin gebruikt is (zie 1.7). We noteren dit als $a \vee b$. $a \vee b$ is waar in de volgende drie gevallen : a waar en b onwaar; a onwaar en b waar; a waar en b waar.

3. De ontkenning van een bewering, a, noteert men als : $\neg a$. $\neg a$ is dus een bewering die alleen waar is als a onwaar is.

Voorbeelden.

$\neg (a \wedge b)$ is dan en slechts dan waar als $(\neg a) \vee (\neg b)$ waar is.

$\neg (a \vee b)$ is dan en slechts dan waar als $(\neg a) \wedge (\neg b)$ waar is.

$\neg \neg a$ is dan en slechts dan waar als a waar is.

4. De notaties $\wedge$ $\vee$ en $\neg$ gebruikt men ook bij beweringsvormen.

Zijn $P(x)$ en $Q(x)$ beweringsvormen, en is U de individuenverzameling voor x dan zijn $P(x) \wedge Q(x)$; $P(x) \vee Q(x)$ en $\neg P(x)$ eveneens beweringsvormen. Een element $a \in U$ voldoet aan $P(x) \wedge Q(x)$ als $P(a) \wedge Q(a)$ waar is; a voldoet aan $P(x) \vee Q(x)$ als $P(a) \vee Q(a)$ waar is; a voldoet aan $\neg P(x)$ als $P(a)$ onwaar is.

Is $P := \{x \mid P(x)\}$; $Q := \{x \mid Q(x)\}$ dan is

$$\{x \mid P(x) \wedge Q(x)\} = \{x \mid P(x),\ Q(x)\} = P \cap Q$$

$$\{x \mid P(x) \vee Q(x)\} = P \cup Q$$

$$\{x \mid \neg P(x)\} = U \setminus P.$$

Opmerking : Let op afwijkende notaties zoals $x \geqslant 0$ voor $(x > 0) \vee (x=0)$; $x \neq 1$ voor $\neg(x = 1)$; $x \notin A$ voor $\neg(x \in A)$; $0 < x < 1$ voor $(x > 0) \wedge (x < 1)$; enz.

5. Opgaven.

11. p is een afkorting voor de bewering : $2 \times 2 = 5$;

q is een afkorting voor de bewering : Eindhoven ligt in Brabant;

r is een afkorting voor de bewering : bier is vloeibaar.

Ga na welke van de volgende beweringen waar zijn, welke onwaar :

(a) $p \vee (q \wedge r)$;

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

(c) $(\neg(p \wedge r)) \wedge (q \vee (\neg r))$;

(d) $(r \vee p) \wedge (\neg p)$;

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

12. A, B en C zijn deelverzamelingen van U. Druk de volgende verzamelingen uit met behulp van U, A, B, C en de symbolen $\cap$, $\cup$ en $\setminus$. Teken Venn-diagrammen.

(a) $\{x \mid ((x \in A) \wedge (x \in B)) \vee (x \in C)\}$;

(b) $\{x \mid (x \in A) \wedge ((x \in B) \vee (x \in C))\}$;

(c) $\{x \mid (x \notin A) \vee (x \notin B)\}$;

(d) $\{x \mid (x \notin A) \wedge ((x \in B) \vee (x \notin C))\}$.

13. Schrijf de volgende verzamelingen met behulp van een definiërende beweringsvorm opgebouwd uit $x \in A$, $x \in B$, $x \in C$ en de symbolen $\wedge$, $\vee$ en $\neg$. Teken Venn-diagrammen.

(a) $(A \setminus B) \cap C$;

(b) $(A \cup B) \cap C$;

(c) $(A \setminus C) \cup (B \cap C)$;

(d) $(A \cup B) \setminus (A \cap B)$.

14. Schets in R_2 de volgende verzamelingen :

(a) $\{(x,y) \mid (x \geqslant 1) \vee (y \leqslant -1)\}$;

(b) $\{(x,y) \mid (x^2 + y^2 \leqslant 1) \wedge (x + y \geqslant 1)\}$;

(c) $\{(x,y) \mid \neg (1 < x^2 + y^2 < 2)\}$;

(d) $\{(x,y) \mid \neg [(x \geqslant 3) \vee (x + y \leqslant 1)]\}$.

2.7. <u>Implicatie</u>. Opgebouwd uit twee beweringen a en b is ook de bewering : "als a, dan b". Notatie hiervoor is : $a \Rightarrow b$. De betekenis van de implicatie wordt vastgelegd door de afspraak dat "$a \Rightarrow b$" waar is in de volgende drie gevallen : a waar en b waar; a onwaar en b waar; a onwaar en b onwaar. "$\neg(a \Rightarrow b)$" is dus alleen waar als a waar is en b onwaar. Dit is misschien niet in overeenstemming met hetgeen men zich in het dagelijks spraakgebruik voorstelt bij als .... dan .... . We zullen echter zien dat het voor de opbouw van de wiskunde een verstandige afspraak is.

Laat $P(x)$ en $Q(x)$ beweringsvormen zijn met individuenverzameling U; men kan nu ook de beweringsvorm $P(x) \Rightarrow Q(x)$ vormen. We hebben: $\{x \mid P(x) \Rightarrow Q(x)\} = (U \setminus P) \cup Q$, waarbij $P = \{x \mid P(x)\}$, $Q = \{x \mid Q(x)\}$. Als gevolg van de afspraak omtrent de waarheid van de implicatie hebben we dat $P \subset Q$ betekent dat $(a \in P) \Rightarrow (a \in Q)$ waar is voor elke $a \in U$.

Opmerking. Vaak gebruikt men de notatie $a \Leftrightarrow b$ voor $(a \Rightarrow b) \wedge (b \Rightarrow a)$. Indien $\Leftrightarrow$ gebruikt wordt in definities dan plaatst men : aan de kant van de te definiëren beweringsvorm (vergelijk § 2.1.). "$a \Leftrightarrow b$" leest men als: "a dan en slechts dan als b".

Opgave.

15. p is een afkorting van : $2 \times 2 = 4$;

q is een afkorting van : $2 \times 2 = 5$.

Ga na welke van de volgende beweringen waar zijn, welke onwaar.

(a) $p \Rightarrow (p \Rightarrow q)$;

(b) $p \Rightarrow (q \Rightarrow p)$;

(c) $q \Rightarrow (q \Rightarrow p)$;

(d) $q \Rightarrow (p \Rightarrow q)$;

(e) $(p \Rightarrow q) \Rightarrow p$;

(f) $(p \Rightarrow q) \Rightarrow q$;

(g) $(q \Rightarrow p) \Rightarrow p$;

(h) $(q \Rightarrow p) \Rightarrow q$.

§ 3. Het gebruik van veranderlijken; quantoren.

3.1. In § 2 zagen we : een beweringsvorm is een zin die een veranderlijke bevat. Deze zin gaat over in een (al dan niet ware) bewering als we de veranderlijke door een element uit een zekere verzameling (de individuenverzameling) vervangen.

Bekijk nu de uitdrukking : "het getal $x^2 + 7$". Dit is geen beweringsvorm (als we voor x iets substitueren dan ontstaat er geen bewering). Vervangen we x door een element uit de verzameling der reële getallen dan ontstaat er een object (een grootheid): "het getal $2^2 + 7$". Dergelijke uitdrukkingen noemen we objectsvormen. Evenals in het geval van beweringsvormen beperken we ons bij het substitueren in een objectsvorm tot de elementen van een bepaalde verzameling, de individuenverzameling.

Als we van een uitdrukking met een veranderlijke willen uitmaken of het een beweringsvorm dan wel een objectsvorm is, dan substitueren we een individu voor de veranderlijke en we kijken of wat er door deze substitutie ontstaat een bewering (je kunt er van zeggen of hij waar is of onwaar) is dan wel een object (getal, verzameling, o.i.d.). Ook grammaticaal zijn beweringsvormen en objectsvormen te onderscheiden. Beweringsvormen zijn zinnen; zij bevatten dus (soms verstopt, bijv. in = of $\geqslant$) een werkwoord. Objectsvormen daarentegen zijn geen zinnen.

Opgave.

16. De individuenverzameling voor de veranderlijke x in elk van de volgende uitdrukkingen is Nt. Ga na welke uitdrukkingen beweringsvormen zijn en welke objectsvormen zijn.

(a) x is deelbaar door 7;

(b) de verzameling van de delers van x;

(c) de priemgetallen die $\leqslant$ x zijn;

(d) x is het kwadraat van een natuurlijk getal;

(e) het kleinste kwadraat dat $\geq x$ is;

(f) 100 is het kleinste kwadraat dat $\geq x$ is.

(g) 101 is het kleinste kwadraat dat $\geq x$ is.

3.2. Meer veranderlijken. In de tot nu toe beschouwde gevallen trad slechts één veranderlijke op. (In voorbeeld 2.2.3 was dat het veranderlijke punt (x,y)). We zullen ook objectsvormen en beweringsvormen beschouwen met meer veranderlijken. Steeds moeten we bij de veranderlijken de individuenverzamelingen aangeven. Zo is voor reële veranderlijken x en y: "$x \geq y$" een beweringsvorm met twee veranderlijken; "$7 \geq y$" is een beweringsvorm met één veranderlijke; "$7 \geq 4$" is een bewering. Evenzo is "$x + y$" een objectsvorm met twee veranderlijken; "$7 + y$" is een objectsvorm met één veranderlijke; $7 + 4$ is een grootheid.

N.B. Indien in een uitdrukking meer veranderlijken voorkomen dan mogen de individuenverzamelingen van de verschillende veranderlijken verschillen; bijv. "punt x ligt op lijn y" is een beweringsvorm met de veranderlijken x en y waarbij de individuenverzameling van x die van de punten, de individuenverzameling van y die van de lijnen is.

Beweringsvormen met twee veranderlijken noemt men ook wel relaties. Vaak laat men de veranderlijken uit de aanduiding weg. Zo spreekt men van de relatie $\geq$ i.p.v. $x \geq y$.

Opgave.

17. De individuenverzameling van de veranderlijken x, y en z in elk van de volgende uitdrukkingen is Nt. Ga na welke uitdrukkingen beweringsvormen zijn en welke objectsvormen.

(a) $x^2 + y^2 = z^2$;

(b) $x^2 + y^2 - z^2$;

(c) $x + 3 < y + 4$;

(d) de delers van xy;

(e) de verzameling van de delers van xy is een deelverzameling van de delers van z.

3.3. Vrije en gebonden veranderlijken. Naast de veranderlijken in beweringsvormen en objectsvormen, komen in de wiskunde ook veranderlijken voor, waarvoor in het geheel niets gesubstitueerd kan worden. Zo is $\int_0^1 x^2 dx = \frac{1}{3}$ een bewering, hoewel er een veranderlijke x in voorkomt; $\{x \mid x \in Gh \text{ en } x > 0\}$ is een object (nl. de verzameling Nt) ongeacht het voorkomen van de letter x. Dergelijke veranderlijken noemt men gebonden veranderlijken. Gebonden betekent hier dat de betekenis van de uitdrukking vastligt zonder dat voor de veranderlijke iets gesubstitueerd behoeft te worden. "$x \in Gh$ en $x > 0$" is wel een beweringsvorm, doch in de uitdrukking $\{x \mid x \in Gh \text{ en } x > 0\}$ is de veranderlijke gebonden.

Gebonden veranderlijken kan men door andere symbolen vervangen zonder dat de betekenis van de uitdrukking waarin ze voorkomen verandert. Aan deze eigenschap kan men gebonden veranderlijken herkennen. "$\int_0^1 x^2 dx = \frac{1}{3}$" en "$\int_0^1 y^2 dy = \frac{1}{3}$" is dezelfde bewering; $\{x^2 \mid x^2 = 4\}$, $\{z^2 \mid z^2 = 4\}$ en $\{\S \mid \S^2 = 4\}$is hetzelfde object. Men moet bij het vervangen van gebonden veranderlijken door andere symbolen wel symbolen nemen die binnen de uitdrukking geen betekenis hebben. Dus niet : $\{4 \mid 4^2 = 4\}$ of $\{\{ \mid \{^2 = 4\}$ of $\{= \mid =^2 = 4\}$.

In tegenstelling tot gebonden veranderlijken noemt men de echte veranderlijken, waarvoor wel gesubstitueerd kan worden vrije veranderlijken. In een bewering komen geen vrije veranderlijken voor.

Voorbeelden. (De individuenverzameling van alle veranderlijken is Rl.)

1. In "$\int_0^x t^2 dt$" is t een gebonden veranderlijke, x een vrije veranderlijke; $\int_0^x t^2 dt$ en $\int_0^x y^2 dy$ zijn dezelfde objectsvormen.

2. In de beweringsvorm "$x > y$" zijn x en y vrije veranderlijken; in de objectsvorm $\{x \mid x > y\}$ is x een gebonden, y een vrije veranderlijke.

Opgave.

18. Onderscheid vrije en gebonden veranderlijken in de volgende uitdrukkingen. Van alle veranderlijken is Rl de individuenverzameling. Onderscheid tevens beweringen, objecten, beweringsvormen, objectsvormen.

(a) $\int_0^t x\,dx > 1$;

(b) $\{t \mid \int_0^t x\,dx > y\}$;

(c) De wortels van de vergelijking $x^2 + 6x + 8 = 0$;

(d) De vergelijking $x^2 + 1 = 0$ heeft geen wortels.

3.4. Quantoren. We zullen thans een zeer belangrijke manier leren kennen om veranderlijken in een beweringsvorm te binden. Beschouw de volgende bewering: "Voor alle reële getallen x is $x^2 \geqslant 0$". Deze (ware) bewering is opgebouwd uit twee delen: een beweringsvorm "$x^2 \geqslant 0$", met als individuenverzameling Rl, en de aanduiding: "voor alle reële getallen x". We kunnen uit een beweringsvorm P(x) een bewering maken door er voor te zetten : "voor alle x uit de verzameling V geldt". Deze V moet dan een deelverzameling van de individuenverzameling van de veranderlijke x uit P(x) zijn. We noteren de zo gevormde bewering aldus:

$$\forall x \in V\ [P(x)] \ ; \ \forall x \in \mathrm{Rl}\ [x^2 \geqslant 0] \ .$$

In deze beweringen is x een gebonden veranderlijke. Het symbool $\forall x \in V$ heet al-quantor. De bewering "$\forall x \in V\ [P(x)]$" kan waar zijn of onwaar. De beweringen "$\forall x \in \mathrm{Nt}\ [x > 0]$" en "$\forall x \in \mathrm{Rl}\ [(x+1)^2 = x^2 + 2x + 1]$" zijn waar, de beweringen "$\forall x \in \mathrm{Gh}\ [x > 0]$" en "$\forall x \in \mathrm{Rt}\ [x^2 > 0]$" zijn onwaar.

Als de verzameling V maar uit eindig veel elementen bestaat, bijv. $V = \{a,b\}$ dan is de bewering "$\forall x \in V\ [P(x)]$" dezelfde als "$P(a) \wedge P(b)$".

Is $P := \{x \mid P(x)\}$ dan is de bewering "$\forall x \in A\ [P(x)]$" dezelfde als "$A \subset P$".

Daarom kan men "$A \subset B$" ook schrijven als "$\forall x \in A\ [x \in B]$".

Ook in beweringsvormen met meer veranderlijken kan men een of meer van de veranderlijken met al-quantoren binden. Zo is "$\forall x \in Rl\ [x > y]$" een beweringsvorm met één veranderlijke (nl. y). "$\forall y \in Rl\ [\forall x \in Rl\ [x > y]]$" is een (onware) bewering.

Beschouw de bewering : "Er is een reëel getal x waarvoor $x^2 = 1$". Deze bewering bestaat uit een beweringsvorm "$x^2 = 1$" en de aanduiding "er is een reëel getal x waarvoor". In symbolen schrijven we :

$$\exists x \in Rl\ [x^2 = 1]\ ;\ \exists x \in V\ [P(x)]\ .$$

$\exists x \in V$ heet <u>existentiële quantor</u>. Beweringen van de vorm $\exists x \in V\ [P(x)]$ kunnen waar zijn zoals "$\exists x \in Rl\ [x^2 \geq 0]$" en "$\exists x \in Nt\ [x^2 = 1]$" of onwaar zoals "$\exists x \in Rl\ [x^2 < 0]$" of "$\exists x \in Nt\ [x^2 = 2]$".

Is $V := \{a,b\}$ dan is de bewering "$\exists x \in V\ [P(x)]$" dezelfde als "$P(a) \vee P(b)$".

Zij U de individuenverzameling van x en zij $P := \{x \mid P(x)\}$, dan is "$\exists x \in U\ [P(x)]$" dezelfde bewering als "$P \neq \emptyset$". De mededeling "$A \neq \emptyset$" kan men dus ook geven in de vorm "$\exists x \in A\ [x \in A]$".

"$\exists x \in Rl\ [x > y]$" is een beweringsvorm met één veranderlijke.

"$\exists y \in Rl [\exists x \in Rl\ [x > y]]$" is een bewering.

"$\forall y \in Rl [\exists x \in Rl\ [x > y]]$" is eveneens een bewering.

<u>Opmerkingen over de notatie.</u>

1. Gebruikt men meerderequantoren dan schrijft men deze achter elkaar zonder haken. Zo schrijft men $\forall y \in Rl\ \ \exists x \in Rl\ [x > y]$ in plaats van $\forall y \in Rl [\exists x \in Rl\ [x > y]]$; $\forall x \in Rl\ \exists y \in Rl\ \forall z \in Rl\ [x^2 + y^2 + z^2 = t^2]$ moet gelezen worden als : $\forall x \in Rl\ [\exists y \in Rl\ [\forall z \in Rl\ [x^2 + y^2 + z^2 = t^2]]]$, (het is een beweringsvorm met één veranderlijke, nl. t).
2. Indien in een stuk tekst slechts één verzameling als individuenverzameling optreedt dan vermeldt men deze soms niet in de quantoren. Hebben bijv.

alle veranderlijken Rl als individuenverameling, en hebben alle quantoren ook betrekking op Rl, dan kan men rustig schrijven :

$\forall x \exists y \forall z [x^2 + y^2 + z^2 = t^2]$.

3. Soms gebruikt men beweringsvormen in de quantoren. Bijvoorbeeld :

$$\forall x \geq 0 [|x| = x] .$$

4. Het is een slechte doch waarschijnlijk onuitroeibare gewoonte van wiskundigen om al-quantoren weg te laten. Zo spreekt men in de middelbare school-algebra over de stelling : "$(a+b)^2 = a^2 + 2ab + b^2$", terwijl men bedoelt dat "$\forall a \in Rl \ \forall b \in Rl \ [(a+b)^2 = a^2 + 2\,ab + b^2]$", waar is.

Een wel correcte notatie die men vaak ziet is :

$P(x) \quad (x \in V) \quad$ i.p.v. $\forall x \in V \ [P(x)]$.

Voorbeeld. De volgorde van de quantoren is van wezenlijk belang voor de betekenis van een uitdrukking.

"$\forall x \in Rl \ \exists y \in Rl \ [x > y]$" is een ware bewering.

"$\exists y \in Rl \ \forall x \in Rl \ [x > y]$" is een onware bewering.

Opgaven.

19. Ga van de volgende beweringen na of ze waar zijn. (De individuenverzameling is steeds Rl.)

(a) $\forall x \in Rl \ [x \in \{1,2,3\}]$;

(b) $\exists x \in Rl \ [x \in \{1,2,3\}]$;

(c) $\exists x \in Rl \ [x \in Nt]$;

(d) $\forall x \in Rl \ [x \in Rt]$;

(e) $\forall x \in Nt \ [\frac{1}{2} x \in Rt]$;

(f) $\forall x \in Nt \ [x + 4 > 3]$;

(g) $\forall x \in Rt \ [-1 < \sin x < 1]$.

20. Ga na welke van de volgende beweringen waar zijn :

(a) $\forall x \in Rl\ \exists y \in Rl\ [x^2 > y]$;

(b) $\exists x \in Rl\ \forall y \in Rl\ [x^2 > y]$;

(c) $\forall y \in Rl\ \exists x \in Rl\ [x^2 > y]$;

(d) $\exists y \in Rl\ \forall x \in Rl\ [x^2 > y]$.

21. Door plaatsing van één der beide symbolen $\forall x \in Nt$, $\exists x \in Nt$ en één der beide symbolen $\forall y \in Nt$, $\exists y \in Nt$ voor de beweringsvorm $xy = 1$ maakt men een bewering. Welke van de acht zo te vormen beweringen zijn waar ?

22. $R(x,y)$ is een relatie; X en Y zijn de individuenverzamelingen van x en y.

(a) Als $\forall x \in X\ \forall y \in Y\ [R(x,y)]$ waar is, wat weet U dan van $\forall y \in Y\ \forall x \in X\ [R(x,y)]$?

(b) Als $\exists x \in X\ \exists y \in Y\ [R(x,y)]$ waar is, wat weet U dan van $\exists y \in Y\ \exists x \in X\ [R(x,y)]$?

(c) Als $\exists x \in X\ \forall y \in Y\ [R(x,y)]$ waar is, wat weet U dan van $\forall y \in Y\ \exists x \in X\ [R(x,y)]$?

<u>3.5. De ontkenning van uitdrukkingen met quantoren.</u> De ontkenning van "$\forall x \in V\ [P(x)]$" kan op twee manieren geschreven worden, nl. als "$\neg \forall x \in V\ [P(x)]$" en als "$\exists x \in V\ [\neg P(x)]$". Evenzo betekenen "$\neg \exists x \in V\ [P(x)]$" en "$\forall x \in V\ [\neg P(x)]$" hetzelfde. Op deze eigenschap berust de mogelijkheid tot "mechanische ontkenning" van uitdrukkingen met veel quantoren.

<u>Voorbeeld.</u> Met behulp van quantoren geeft men de definitie van convergentie van een rij reële getallen (zie Wiskunde I) weer als volgt. De rij $a_1, a_2, a_3, \ldots$ is convergent, dan en dan alleen indien :

$\exists\, a \in \mathrm{Rl}\, \forall \varepsilon > 0\ \exists N \in \mathrm{Nt}\ \forall n > N\ (|a_n - a| < \varepsilon)$.

Gevolg : de rij $a_1, a_2, a_3, \ldots$ is niet convergent, dan en dan alleen indien :

$\forall a \in \mathrm{Rl}\, \exists \varepsilon > 0\ \forall N \in \mathrm{Nt}\ \exists n > N\ (|a_n - a| \geq \varepsilon)$.

Opgaven.

23. Geef met behulp van quantoren de definitie van :

(a) de functie f is continu in x_0;

(b) de functie f is niet continu in elk punt.

24. (a) Toon aan dat de bewering in opgave 23 a waar is voor $f(x) = x$, $x_0 = 1$.

(b) Toon aan dat de bewering in opgave 23 b waar is voor

$$f(x) = \begin{cases} 1 \text{ als } x \geq 0, \\ 0 \text{ als } x < 0. \end{cases}$$

25. Gegeven is de rij functies $f_1, f_2, \ldots\ldots\ldots$, gedefiniëerd voor alle reële x. Schrijf met behulp van quantoren :

(a) alle functies uit de rij zijn continu in elk punt ;

(b) voor elke reële x geldt : $\lim_{n\to\infty} f_n(x) = x^2$.

Ga na welke volgorden van quantoren toegestaan zijn.

3.6. Meer quantoren. Natuurlijk komen er meer quantoren voor dan alleen alquantoren en existentiële quantoren. We noemen een aantal voorbeelden :

(a) Voor precies één individu;

(b) Voor tenminste twee individuen;

(c) Voor hoogstens één individu.

Hiervan is alleen het voorbeeld(a) zo belangrijk dat we er een aparte notatie voor invoeren, nl. $\exists!$

Voorbeeld.

" $\exists!\ x \in Rl\ [x^2 = 1]$ " is onwaar.

" $\exists!\ x \in Rl\ [(x^2 = 1) \wedge (x > 0)]$ " is waar.

Opmerking. Men kan de onder (a), (b) en (c) genoemde quantoren (evenals andere niet genoemde) uitdrukken m.b.v. $\forall$, $\exists$ en de symbolen $\wedge$, $\vee$, $\Rightarrow$, $\neg$, en $=$ (en uiteraard velerlei haken).

(a) " $\exists!\ x \in U\ [P(x)]$ " betekent hetzelfde als :

$$\exists\ x \in U\ [P(x) \wedge (\forall\ y \in U\ [P(y) \Rightarrow (x = y)\,]\,)\,].$$

(b) "Voor tenminste twee $x \in U$ geldt $P(x)$" kan men bijv. weergeven als

$$\exists\ x \in U\ \exists\ y \in U\ [P(x) \wedge P(y) \wedge (x \neq y)]$$

(c) "Voor hoogstens één $x \in U$ geldt $P(x)$" kan men bijv. weergeven als

$$\forall\ x \in U\ \forall\ y \in U\ [(P(x) \wedge P(y)) \Rightarrow (x = y)]\ .$$

Opgaven.

26. $V \subset Rl$. Schrijf $\neg(\exists!\ x \in Nt\ [x \in V]\ )$ op een andere manier. Geef een voorbeeld van een verzameling V waarvoor deze bewering waar is.

27. Gegeven is een beweringsvorm $P(x)$; de individuen zijn de natuurlijke getallen. Geef de volgende beweringen in symbolen weer.
   (a) hoogstens twee natuurlijke getallen voldoen aan $P(x)$;
   (b) precies twee natuurlijke getallen voldoen aan $P(x)$;
   (c) minstens drie natuurlijke getallen voldoen aan $P(x)$.

3.7. Een toepassing. Vereniging en doorsnede van een willekeurige collectie verzamelingen.

Definitie: Is I een verzameling en is aan ieder element $i \in I$ een verzameling A_i toegevoegd dan definiëert men $\bigcup_{i \in I} A_i$ en $\bigcap_{i \in I} A_i$ door :

$$\bigcup_{i \in I} A_i := \{x \mid \exists i \in I \; [x \in A_i]\}$$

$$\bigcap_{i \in I} A_i := \{x \mid \forall i \in I \; [x \in A_i]\}$$

Opmerkingen.

(a) Is I een verzameling met eindig veel elementen dan komen deze definities overeen met die van 1.7 en 1.8.

(b) In $\bigcup_{i \in I} A_i$ en $\bigcap_{i \in I} A_i$ is i een gebonden veranderlijke :

$$\bigcap_{i \in I} A_i = \bigcap_{k \in I} A_k.$$

(c) Is I een verzameling van natuurlijke getallen van de vorm $\{k, k+1, k+2, \ldots, m\}$ of $\{k, k+1, k+2, \ldots\}$ dan schrijft met i.p.v. $\bigcup_{i \in I} A_i$: $\bigcup_{i=k}^{m} A_i$ resp. $\bigcup_{i=k}^{\infty} A_i$ en evenzo in plaats van $\bigcap_{i \in I} A_i$: $\bigcap_{i=k}^{m} A_i$ resp. $\bigcap_{i=k}^{\infty} A_i$.

Opgaven.

28. $S := \{s \in Rl \mid s \geq 0\}$; voor $s \in S$, definiëren we :

$$C_s = \{(x,y) \mid (x,y) \in R_2 \; , \; x^2 + y^2 = s\}.$$

Laat zien dat :

(a) $\bigcup_{s \in S} C_s = R_2$;

(b) $\bigcap_{s \in S} C_s = \emptyset$.

29. $\forall i \in I \, (A_i \subset W)$. Bewijs de volgende beweringen (* duidt complementvorming t.o.v. W aan).

(a) $(\bigcup_{i \in I} A_i)^* = \bigcap_{i \in I} A_i^*$.

(b) $(\bigcap_{i \in I} A_i)^* = \bigcup_{i \in I} A_i^*$.

30. I = Nt, $A_1, A_2, \ldots$ is een rij verzamelingen. Laat zien dat :

$\bigcup_{m=1}^{\infty} \bigcap_{k=m}^{\infty} A_k = \{x \mid x \notin A_i$ voor slechts eindig veel waarden van i$\}$

$\bigcap_{m=1}^{\infty} \bigcup_{k=m}^{\infty} A_k = \{x \mid x \in A_i$ voor oneindig veel waarden van i$\}$.

§ 4. Afbeeldingen.

4.1. Cartesische producten. Van nu af zullen we gebruiken het begrip geordend paar. Zijn a en b elementen van een zekere verzameling dan noteren we het geordende paar van a en b als (a,b). In het algemeen is $(a,b) \neq (b,a)$; $(a,b) = (b,a)$ dan en slechts dan als $a = b$.

Definitie. Laat A en B verzamelingen zijn dan verstaat men onder het Cartesische product van A en B (notatie $A \times B$) de collectie van alle geordende paren (a,b), waarbij $a \in A$, $b \in B$. Met een notatie afgesproken in § 2 kunnen we dus schrijven

$$A \times B = \{(a,b) \mid a \in A,\ b \in B\}.$$

De naam Cartesischproduct wijst op de analogie met Cartesische coördinaten in het platte vlak, dat daarom ook opgevat kan worden als $Rl \times Rl$.

Eigenschappen.

1. $\emptyset \times A = \emptyset$.
2. $U \times (V \cap W) = (U \times V) \cap (U \times W)$,
3. $(V \cap W) \times U = (V \times U) \cap (W \times U)$,
4. $(V \cap W) \times (U \cap T) = (V \times U) \cap (V \times T) \cap (W \times U) \cap (W \times T) =$
   $= (V \times U) \cap (V \times T) \cap (W \times U)$.

Geheel analoog definiëert men $A \times B \times C$ als een verzameling waarvan de elementen tripels zijn :

$$A \times B \times C = \{(a,b,c) \mid a \in A,\ b \in B,\ c \in C\}.$$

Opmerkingen.

1. Let op het verschil tussen $A \times B \times C$; $A \times (B \times C)$ en $(A \times B) \times C$.
2. $Rl \times Rl$ noemt men vaak R_2, $Rl \times Rl \times Rl$: R_3 enz.

Opgaven.

31. A is een verzameling met m elementen, B is een verzameling met n elementen.

(a) Hoeveel elementen heeft $A \times B$?

(b) Hoeveel deelverzamelingen heeft $A \times B$? (zie opg. 4.)

(c) Hoeveel deelverzamelingen van $A \times B$ zijn van de vorm $A_0 \times B_0$, waarin $A_0 \subset A$ en $B_0 \subset B$?

32. U, V en W zijn verzamelingen; $U = V \cap W$. Welke van de volgende beweringen zijn waar ?

(a) $U \times U = (V \times V) \cap (W \times W)$;

(b) $U \times U = (V \times W) \cap (W \times V)$.

4.2. Afbeelding, beeld, volledig origineel. In de geest waarin in Wiskunde I functies ingevoerd zijn kan men zeggen : "onder een afbeelding van een verzameling A in een verzameling B verstaat men een voorschrift waardoor aan elk element van A één element van B wordt toegevoegd". Dit is echter geen correcte definitie, omdat de betekenis van het woord "voorschrift" niet precies vastligt. Dat voorschrift niet hetzelfde is als formule weten we al. M.b.v. het Cartesische product kan men nu afbeeldingen correct definiëren.

Definitie 1. Een afbeelding van een verzameling A in een verzameling B is een deelverzameling F van $A \times B$ met de eigenschap :

$$\forall a \in A \ \exists ! \ b \in B \ [(a,b) \in F].$$

Afbeeldingen van een verzameling A in Rl heten reële functies op A. (Voor reële functies van een reële veranderlijke, dat zijn afbeeldingen van Rl in Rl, betekent deze definitie dat we het onderscheid tussen de functie en zijn grafiek laten vallen.)

<u>Definitie 2.</u> Is F een afbeelding van A in B, en is $(a,b) \in F$ dan heet b het <u>beeld</u> van a; notatie $b = F(a)$ (soms ook $b = Fa$).
Is $A_0 \subset A$ dan heet $F(A_0) := \{F(a) \mid a \in A_0\}$ het <u>beeld</u> van A_0.
Gevolg van definitie 2 is : $F(\emptyset) = \emptyset$. Naast $F(A_0)$ zou $F(\{a\})$ i.p.v. $F(a)$ consequent zijn.

<u>Definitie 3.</u> Is F een afbeelding van A in B, en is $b \in B$ dan heet $F^{\leftarrow}(b) := \{a \in A \mid F(a) = b\}$ het volledig <u>origineel</u> van b.
Is $B_0 \subset B$ dan heet $F^{\leftarrow}(B_0) := \{a \in A \mid F(a) \in B_0\} = \cup_{b \in B_0} F^{\leftarrow}(b)$ het volledig origineel van B_0.
Ook hier is er een inconsequentie in het naast elkaar gebruiken van de notaties : $F^{\leftarrow}(B_0)$ en $F^{\leftarrow}(b)$.

<u>Opmerking over de notatie.</u> Voor afbeeldingen gebruikt men meestal de letters $F,G,H,\ldots$ $f,g,h,\ldots$ $\varphi,\chi,\psi,\ldots$. Een handige notatie om aan te geven dat F een afbeelding van A in B is de volgende: $F : A \to B$. Hierbij moet het volgende opgemerkt worden.

1. We gebruiken de symbolen $F : A \to B$ in twee betekenissen:
   a. Als aanduiding van:"F is een afbeelding van A in B."
   b. Als aanduiding: "F, die een afbeelding van A en B is, ...".
2. Als B deelverzameling van C is, dan is $A \times B$ het van $A \times C$.
   Iedere deelverzameling van $A \times B$ is dan ook deelverzameling van $A \times C$.
   Bij iedere afbeelding van A in B bestaat er dus een afbeelding van A in C die uit dezelfde paren bestaat. Tenzij $B = C$ zijn dit verschillende afbeeldingen.

4.3. Eigenschappen.

Als $F : A \to B$; $A_1 \subset A$, $A_2 \subset A$, $B_1 \subset B$, $B_2 \subset B$, dan geldt :

1. $F(A_1 \cup A_2) = F(A_1) \cup F(A_2)$;
2. $F(A_1 \cap A_2) \subset F(A_1) \cap F(A_2)$;
3. $F^{\leftarrow}(B_1 \cup B_2) = F^{\leftarrow}(B_1) \cup F^{\leftarrow}(B_2)$;
4. $F^{\leftarrow}(B_1 \cap B_2) = F^{\leftarrow}(B_1) \cap F^{\leftarrow}(B_2)$.

4.4. Opgaven.

33. $A = \{1,2,3,4\}$; $B = \{1,2,3\}$;

$F = \{(1,1), (2,1), (3,2), (4,2)\}$.

(a) Bewijs dat F een afbeelding van A in B is.

(b) Bepaal $F(A)$.

(c) Bepaal $F^{\leftarrow}(B)$ en $F^{\leftarrow}(1)$.

34. A is een verzameling met m elementen, B is een verzameling met n elementen.

Hoeveel verschillende afbeeldingen van A in B zijn er ?

35. $F : A \to B$, $A_1 \subset A$, $A_2 \subset A$, $B_1 \subset B$, $B_2 \subset B$.

(a) Geef een voorbeeld waarvoor de inclusie in eigenschap 4.3.2. een echte inclusie is.

(b) Bewijs :

$$F(A_1 \setminus A_2) \supset F(A_1) \setminus F(A_2)$$

$$F^{\leftarrow}(B_1 \setminus B_2) = F^{\leftarrow}(B_1) \setminus F^{\leftarrow}(B_2).$$

(c) Geef een voorbeeld waarvoor de inclusie in (b) echt is.

36. Is $F : A \to B$, $A_1 \subset A$, $B_1 \subset B$ dan is

$$F^{\leftarrow}(F(A_1)) \supset A_1 \; ; \quad F(F^{\leftarrow}(B_1)) \subset B_1 .$$

Bewijs dit, en geef voorbeelden waarvoor de inclusies echt zijn.

4.5. Afbeeldingen op, een-eenduidigheid, inversen.

Definitie 1. $F : A \to B$ heet een afbeelding van A op B indien $F(A) = B$, d.w.z. ieder element van B is beeld van een element van A.

Definitie 2. $F : A \to B$ heet 1-1 duidig indien :

$$\forall b \in F(A) \quad \exists!\, a \in A\ [F(a) = b].$$

Men kan ook zeggen : $F : A \to B$ heet 1-1 duidig indien :

$$\forall a_1 \in A \quad \forall a_2 \in A\ [(F(a_1) = F(a_2)) \Rightarrow (a_1 = a_2)] ;$$

of: $$\forall a_1 \in A \quad \forall a_2 \in A\ [(a_1 \neq a_2) \Rightarrow F(a_1) \neq F(a_2)] .$$

Stelling 1. Is $F : A \to B$ een 1-1 duidige afbeelding van A op B en is $G := \{(b,a) \mid (a,b) \in F\}$ dan is G een afbeelding van B in A.

Bewijs. Er geldt $\forall b \in B\ \exists!\, a \in A\ [F(a) = b]$, d.w.z. $\forall b \in B\ \exists!\, a \in A((b,a) \in G)$, dus $G : B \to A$.

Opgave.

37. Bewijs dat onder de voorwaarden van stelling 4.5.1 $G : B \to A$ een 1-1 duidige afbeelding van B op A is.

Definitie 3. De afbeelding G heet de inverse van F; notatie F^{-1}.

Eigenschappen.

1. Is $G = F^{-1}$ en $F(a) = b$ dan is $G(b) = a$.
2. Is $G = F^{-1}$ dan is $F = G^{-1}$.

Is $A = B = Rl$ dan betekent de overgang van (a,b) op (b,a) juist spiegeling aan de diagonaal $:= \{(x,x) \mid x \in Rl\}$. De definitie van inverse afbeelding bevat dus de in wiskunde I gegeven definitie van inverse functies.

Definitie 4. Is A een verzameling dan heet $I_A := \{(a,a) \mid a \in A\}$ de identieke afbeelding van A op zichzelf. Dit is een 1-1 duidige afbeelding van A op A. Er geldt : $\forall a \in A\ (I_A(a) = a)$.

4.6. Opgaven.

38. A is een verzameling van m elementen. Hoeveel verschillende afbeeldingen van A op A bestaan er ?

39. $B = \{0,1\}$. Wat zijn alle afbeeldingen van B in B ?
Welke van deze afbeeldingen zijn 1-1 duidig en op ?

40. $A = \{x \mid x \in Rl,\ 0 \leq x \leq 1\}$.
$F : A \to A$ is gedefiniëerd door : $\forall x \in A\,[\,F(x) := \sqrt{1 - x^2}\,]$.
(a) Is F een afbeelding van A op A?
(b) Heeft F een inverse?

41. $Rl^+ := \{x \in Rl \mid x \geq 0\}$
$Rt^+ := \{x \in Rt \mid x \geq 0\}$.
(a) $f : Rl^+ \to Rl^+$ is gedefiniëerd door $f(x) := x^2$ $(x \in Rl^+)$.
Is f op, 1-1 duidig ?
(b) $g : Rt^+ \to Rt^+$ is gedefiniëerd door $g(x) := x^2$ $(x \in Rt^+)$.
Is g op, 1-1 duidig ?

42. $f : R_2 \to R_2$ is gedefiniëerd door $f((x,y)) := (x,0)$ $((x,y) \in R_2)$.
(a) Hoe zoudt U deze afbeelding noemen ?
(b) Is f op, 1-1 duidig ?
(c) Wat is $f^{\leftarrow}((1,0))$?

43. Voor elke $a \in Rl$ wordt een afbeelding $f_a : Rl \to Rl$ gedefiniëerd door : $\forall x \in Rl\,[f_a(x) := a + x]$.
(a) Bewijs dat voor elke $a \in Rl$ f_a 1-1 duidig en op is.
(b) Bepaal $f_7\,(f_3^{-1}(8))$.

44. Geef een 1-1 afbeelding van de verzameling der natuurlijke getallen op de verzameling der even natuurlijke getallen.

45. Geef een <u>1-1</u> afbeelding van de verzameling V <u>op</u> Rl indien

$$V := \{x \in Rl \mid 1 < x < 2\}.$$

46. V is de verzameling van alle afbeeldingen van R_1 in R_1.

$\varphi : V \to R_2$ is gedefiniëerd als volgt : $\forall f \in V\ [\varphi(f) := (f(1), f(2))]$

(a) Is φ 1-1 duidig, <u>op</u> ?

(b) Wat is het volledig origineel van (0,0) ?

47. $f : X \to Y$. Bewijs dat.

$\forall A \subset X \ \ \forall B \subset X\ [f(A \cap B) = f(A) \cap f(B)]$ dan en slechts dan als

f 1-1 duidig is.

<u>4.7. Samengestelde afbeeldingen.</u>

<u>Definitie.</u> Is $F : A \to B$; $G : B \to C$ dan is

$$G \circ F := \{(a, G(b)) \mid a \in A,\ b = F(a)\} ;$$

de afbeelding $G \circ F$ van A in C heet de <u>samengestelde afbeelding</u> van G en F.

<u>Eigenschappen.</u> $F : A \to B$, $G : B \to C$, $H : C \to D$.

1. $\forall a \in A\ [G \circ F(a) = G(F(a))]$
2. Is F 1-1 duidig en is G 1-1 duidig dan is $G \circ F$ 1-1 duidig
3. Is F <u>op</u> en is G <u>op</u> dan is $G \circ F$ <u>op</u>.
4. Is F 1-1 duidig en <u>op</u> en is G 1-1 duidig en <u>op</u> dan is

   $(G \circ F)^{-1} = F^{-1} \circ G^{-1}$
5. Is $C_0 \subset C$ dan is $(G \circ F)^{\leftarrow}(C_0) = F^{\leftarrow}(G^{\leftarrow}(C_0))$.
6. Afbeeldingssamenstelling is associatief: $H \circ (G \circ F) = (H \circ G) \circ F$.

<u>Opgaven.</u>

48. F is een 1-1 duidige afbeelding van A <u>op</u> B.

Bewijs dat $F^{-1} \circ F = I_A$; $F \circ F^{-1} = I_B$.

49. Gegeven zijn $f : X \to X$ en een deelverzameling $A \subset X$ waarvoor $f(A) \supset A$.

(a) Bewijs dat $f^{n+1}(A) \supset f^n(A)$ voor elke $n \in \mathbb{N}$;
($f^{n+1} := f \circ f^n$ voor alle $n \in \mathbb{N}$).

(b) $V := \bigcup_{n=1}^{\infty} f^n(A)$, bewijs dat $f(V) = V$.

(c) (Voorbeeld) $X := \mathbb{R}$, $f(x) := x^2$ $(x \in \mathbb{R})$.

Bereken V voor : $A := \{x \mid 0 \leq x \leq 1\}$.

$A := \{x \mid 0 \leq x \leq 2\}$.

4.8. Karakteristieke functies. We beschouwen een vaste verzameling U; $W := \{0,1\}$. Aan iedere deelverzameling $A \subset U$ voegen we toe de afbeelding $\chi_A : U \to W$ gedefinieerd door :

$$\chi_A(x) := \begin{cases} 1 \text{ als } x \in A \\ 0 \text{ als } x \in U \setminus A. \end{cases}$$

$\chi_A(x)$ heet de karakteristieke functie van A. Uit $\overleftarrow{\chi_A}(1) = A$ volgt dat een deelverzameling van U door zijn karakteristieke functie volledig bepaald is.

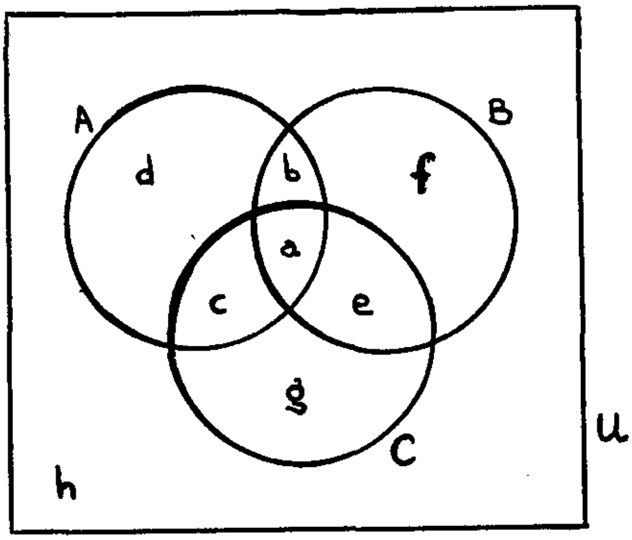
Eigenschappen. Voor alle deelverzamelingen A, B van U geldt :

1. $\chi_{A*}(x) = 1 - \chi_A(x)$
2. $\chi_{A \cap B}(x) = \chi_A(x)\, \chi_B(x) = \min\, (\chi_A(x), \chi_B(x))$
3. $\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\, \chi_B(x) = \max\,(\chi_A(x), \chi_B(x))$
4. $\chi_{A \setminus B}(x) = \chi_A(x) - \chi_A(x)\, \chi_B(x)$.

Onderstaande tabel geeft de waarden van de karakteristieke functies van de verzamelingen $A \cap B$, $A \cup B$, $A \setminus B$.

$\chi_A(x)$	$\chi_B(x)$	$\chi_{A \cap B}(x)$	$\chi_{A \cup B}(x)$	$\chi_{A \setminus B}(x)$
1	1	1	1	0
1	0	0	1	1
0	1	0	1	0
0	0	0	0	0

Als voorbeeld van het gebruik van karakteristieke functies geven we een ander bewijs van eigenschap 1.10.1.



Laat A, B, C deelverzamelingen van U zijn.

De karakteristieke functies kunnen de volgende waarden hebben :

*)	χ_A	χ_B	χ_C	$\chi_{A \cup B}$	$\chi_{(A \cup B) \cap C}$	$\chi_{A \cap C}$	$\chi_{B \cap C}$	$\chi_{(A \cap C) \cup (B \cap C)}$
a	1	1	1	1	1	1	1	1
b	1	1	0	1	0	0	0	0
c	1	0	1	1	1	1	0	1
d	1	0	0	1	0	0	0	0
e	0	1	1	1	1	0	1	1
f	0	1	0	1	0	0	0	0
g	0	0	1	0	0	0	0	0
h	0	0	0	0	0	0	0	0

*)letters corresponderen met het bovenstaande Venn-diagram.

We zien dat $\chi_{(A \cup B) \cap C}(x) = \chi_{(A \cap C) \cup (B \cap C)}(x)$ voor alle $x \in U$
en dus $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.-

Opgave.

50. Maak de opgaven van § 1.12 met behulp van karakteristieke functies.

Hoofdstuk II. Equivalentierelaties.

§ 5. Equivalentierelaties.

5.1. Partities.

Definitie. Een partitie van een verzameling V is een verzameling $W := \{V_i \mid i \in I\}$ van verzamelingen met de volgende eigenschappen.

1. $V_i \neq \emptyset \quad (i \in I)$;
2. $\bigcup_{i \in I} V_i = V$;
3. $(V_i \cap V_j \neq \emptyset) \Rightarrow (V_i = V_j) \quad (i \in I,\ j \in I)$.

Uit eigenschap 2 volgt dat $V_i \subset V \quad (i \in I)$.
Eigenschap 3 kan men ook formuleren als :

$$\forall i \in I \ \forall j \in I\, [(V_i = V_j) \vee (V_i \cap V_j = \emptyset)].$$

Populair gezegd : Een partitie van V is een opdeling van V in niet lege disjuncte delen.

Voorbeelden.

1. Als $N_1 := \{2,4,6,8,\ldots\}$ en $N_2 := \{1,3,5,7,\ldots\}$ dan is $\{N_1, N_2\}$ een partitie van Nt.
2. Is V een verzameling dan is $W := \{\{v\} \mid v \in V\}$ een partitie van V.
3. Als $V_\alpha := \{(x,y) \mid (x,y) \in R_2 ,\ x > 0,\ y = \alpha x\}$ dan is $\{V_\alpha \mid \alpha \in Rl\}$ een partitie van $V := \{(x,y) \mid (x,y) \in R_2 ,\ x > 0\}$.

Opgaven.

51. Is $V_0 \subset V$ en is $W = \{V_i \mid i \in I\}$ een partitie van V, dan is $W_0 := \{V_i \cap V_0 \mid i \in I;\ V_i \cap V_0 \neq \emptyset\}$ een partitie van V_0.

52. Is $W = \{V_i \mid i \in I\}$ een partitie van V, dan definiëert $\forall V_i \in W\ \forall x \in V\, [(f(x) = V_i) :\Longleftrightarrow (x \in V_i)]$ een afbeelding f van V op W.
(N.B. Men moet laten zien dat inderdaad een afbeelding gedefiniëerd is, en dat deze afbeelding op is.)

53. Beschrijf een partitie $N := \{N_i \mid i \in I\}$ van Nt met de eigenschap

$$\forall N_i \in N \ \forall N_j \in N\,[(N_i = N_j) \vee \{\forall x \in N_i \ \forall y \in N_j \ \ (g.g.d.(x,y) = 1)\}].$$

(*g.g.d.* (x,y) is de *grootste gemene deler van* x *en* y).

5.2. Relaties die reflexief, symmetrisch of transitief zijn. Herinner: een relatie is een beweringsvorm met twee veranderlijken. In hoofdstuk II zullen we slechts relaties beschouwen waarvoor de individuenverzameling van beide veranderlijken dezelfde verzameling V is. Is $R(x,y)$ zo'n relatie dan behoort daarbij de verzameling $R := \{(x,y) \mid x \in V,\ y \in V,\ \ R(x,y)\}$ die een deelverzameling van $V \times V$ is. (Vat men $R(x,y)$ op als beweringsvorm met *één* veranderlijke (x,y) en individuenverzameling $V \times V$ dan is R de verzameling met definiërende beweringsvorm $R(x,y)$).

Definitie 1. De relatie $R(x,y)$ heet reflexief dan en dan alleen indien

$$\forall\ x \in V(R(x,x)).$$

Reflexiviteit betekent dus dat $I_V \subset R$.

Definitie 2. De relatie $R(x,y)$ heet symmetrisch dan en dan alleen indien

$$\forall x \in V \ \ \forall y \in V \ \ (R(x,y) \Rightarrow R(y,x)).$$

Symmetrie betekent dus dat $(a,b) \in R$ dan en slechts dan als $(b,a) \in R$.

Definitie 3. De relatie $R(x,y)$ heet transitief dan en dan alleen indien

$$\forall x \in V \ \ \forall y \in V \ \ \forall z \in V\,(((R(x,y) \wedge R(y,z)) \Rightarrow R(x,z)).$$

Voorbeeld. Neem $V = Rl$.

Als $R(x,y)$ is	dan is $R(x,y)$.
$x = y + 1$	niet reflexief; niet symmetrisch; niet transitief.
$x > y$	niet reflexief; niet symmetrisch; transitief.
$x \neq y$	niet reflexief; symmetrisch; niet transitief.
$x \leq y < x + 2$	reflexief; niet symmetrisch; niet transitief.

$xy > 0$	niet reflexief; symmetrisch; transitief.
$x \geqslant y$	reflexief; niet symmetrisch; transitief.
$\lvert x-y \rvert < 1$	reflexief; symmetrisch; niet transitief.
$x = y$	reflexief; symmetrisch; transitief.

Opgaven.

54. Schets van de relaties in het bovenstaande voorbeeld de bijbehorende verzamelingen in het cartesiche vlak.

55. Ga van de volgende relaties na of ze reflexief, symmetrisch, transitief zijn; individuen zijn de gehele getallen.
   (a) $x-y$ is oneven;
   (b) de grootste gemene deler van x en y is gelijk aan 2;
   (c) $xy \leqslant 0$.

5.3. Equivalentierelaties.

Definitie. Een equivalentierelatie is een relatie die zowel reflexief als symmetrisch als transitief is.
(Men gebruikt voor equivalentierelaties vaak de notatie $x \sim y$; men zegt als $a \sim b$ waar is: "a is equivalent met b".)

Voorbeelden van equivalentierelaties.

1. V : willekeurige verzameling; $x = y$.
2. V : alle rechten in het platte vlak; $(x \,//\, y) \vee (x = y)$.
3. V : alle driehoeken in het platte vlak; x congruent y.
4. V : de gehele getallen; $x - y$ is een 5-voud.
5. Is V een verzameling en is $W := \{V_i \mid i \in I\}$ een partitie van V dan is $\exists\, V_i \in W\ [(x \in V_i) \wedge (y \in V_i)]$ een equivalentierelatie op V.

Het laatste voorbeeld is heel belangrijk; omdat elke equivalentierelatie op deze wijze gegeven kan worden. Dit blijkt uit de volgende stelling.

Stelling. Is $R(x,y)$ een equivalentierelatie op V, dan bestaat er een partitie $W = \{V_i \mid i \in I\}$ van V met de eigenschap dat

$$\forall x \in V \quad \forall y \in V \; [R(x,y) \Longleftrightarrow \exists V_i \in W \; [(x \in V_i) \wedge (y \in V_i)]]$$

De elementen van W heten de equivalentieklassen. Twee elementen uit dezelfde klasse zijn dus steeds equivalent; twee elementen uit verschillende klassen zijn nooit equivalent. Ieder element uit een equivalentieklasse heet een representant van die klasse.

Bewijs. Voor iedere element $a \in V$ definiëren we de verzameling

$$V(a) := \{y \mid y \in V,\ R(a,y)\} .$$

a. We laten zien dat $\{V(x) \mid x \in V\}$ een partitie van V is.

Per definitie is $V(x) \subset V \quad (x \in V)$.

1. Wegens de reflexiviteit is $x \in V(x)$ dus $V(x) \neq \emptyset \quad (x \in V)$.
2. We hebben $\bigcup_{x \in V} V(x) \subset V$;
   wegens 1 is $V \subset \bigcup_{x \in V} V(x)$ dus $\bigcup_{x \in V} V(x) = V$.
3. Zij $V(a) \cap V(b) \neq \emptyset$, d.w.z. er is een $c \in V(a) \cap V(b)$.

Zij x een willekeurig element van $V(a)$. We hebben dan $R(a,x)$; $R(a,c)$; $R(b,c)$.

Wegens de symmetrie is nu $R(c,a)$ waar. Wegens de transitiviteit volgt uit het waar zijn van $R(c,a)$ en $R(a,x)$ dat $R(c,x)$ waar is. Wederom wegens de transitiviteit -nu toegepast voor $R(b,c)$ en $R(c,x)$- volgt dat $R(b,x)$ waar is. Dus $x \in V(b)$; dus $V(a) \subset V(b)$. Analoog: $V(b) \subset V(a)$; zodat $V(a) = V(b)$.

b. We laten zien dat de partitie $\{V(x) \mid x \in V\}$ de gewenste eigenschap heeft. Is $R(a,b)$ waar, dan is $a \in V(a)$, $b \in V(a)$. Is omgekeerd $a \in V(c)$, $b \in V(c)$ dan zijn $R(c,a)$ en $R(c,b)$ waar. Op grond van de symmetrie is dan $R(a,c)$

waar, en dan is op grond van de transiviteit $R(a,b)$ waar.

Q.E.D.

Meer voorbeelden.

6. Is V een willekeurige verzameling; is $x = y$ de equivalentierelatie, dan zijn alle deelverzamelingen van V met *één element precies* alle equivalentie-klassen.

7. $V := Rl \times Rl$. De relatie $\sim$ is gedefiniëerd door :

$$\forall (x,y) \in V \; \forall (u,v) \in V \; [((x,y) \sim (u,v)) :\Leftrightarrow (x^2 + y^2 = y^2 + v^2)].$$

De equivalentieklassen zijn $\{(0,0)\}$ en alle cirkels om de oorsprong.

8. $V := Gh$; $\forall x \in V \; \forall y \in V \; [(x \sim y) :\Leftrightarrow (x - y \text{ is even})]$. Er zijn twee equivalentieklassen: één bestaande uit alle even, één bestaande uit alle oneven getallen.

9. Zij U een verzameling; $A \subset U$. V : de collectie van alle deelverzamelingen van U.

$$\forall X \in V \quad \forall Y \in V \; ((X \sim Y) :\Leftrightarrow (X \cap A = Y \cap A)).$$

Bij iedere deelverzameling A van A hoort één equivalentieklasse: $\{X \mid X \cap A = A_1\}$.

10. Is $F : V \rightarrow W$ een afbeelding van V op W.

$$\forall x \in V \quad \forall y \in V \; [(x \sim y) :\Leftrightarrow (F(x) = F(y))].$$

Bij iedere element w van W behoort een equivalentieklasse nl. : $F^{\leftarrow}(w)$.

11. De equivalentieklassen van een equivalentierelatie kunnen in "grootte" zeer verschillen.

$$V := Rl; \quad \forall x \in Rl \quad \forall y \in Rl \; [(x \sim y) :\Leftrightarrow \exists \, a \neq 0 \; (ax = y)].$$

Er zijn twee equivalentieklassen: $\{0\}$ en $Rl \setminus \{0\}$.

12. Om alle equivalentierelaties op een verzameling V te beschouwen, is het voldoende alle partities van V te bekijken. (Ga dit na.)

Opgaven.

56. E stelt het platte vlak voor. O is een vast punt in E. Is de relatie $R(P_1,P_2)$: "er is een rechte door O, P_1 en P_2" een equivalentierelatie op E ? Op $E \setminus \{O\}$?

57. $V := \{1,2, \ldots, 1000\}$.
$P(V) := \{A \mid A \subset V\}$.
$\forall A \in P(V) \quad \forall B \in P(V) [(A \sim B) :\Leftrightarrow$ (A bevat evenveel elementen als B)].
Laat zien dat de relatie $\sim$ een equivalentierelatie is op $P(V)$.
Geef de equivalentieklassen aan.

58. U is een niet lege verzameling.
Ga na of de volgende relatie, gedefiniëerd voor de verzameling van de niet lege deelverzamelingen van U, een equivalentierelatie is :
$[(A \sim B) :\Leftrightarrow A \cap B \neq \emptyset]$. $(A \subset U,\ B \subset U)$.

59. Zij $f : Rl \to Rl$. We definiëren een relatie op de reële getallen door :
$\forall x \in Rl \ \ \forall y \in Rl \ (R(x,y) :\Leftrightarrow (f(x) = f(y)))$.
Bewijs dat dit een equivalentierelatie is. Beschrijf de equivalentieklassen.

60. $I := \{x \in Rl \mid 0 \leqslant x \leqslant 1\}$; F is de verzameling van alle reële functies op I; we definiëren :
$\forall f \in F \ \ \forall g \in F [(f \sim g) :\Leftrightarrow$ ($f-g$ is continu op I)].
Bewijs :
(a) De relatie $\sim$ is een equivalentierelatie;
(b) de continue functies vormen juist één equivalentieklasse.

61. Is $\approx$ een relatie, met individuenverzameling V die voldoet aan :

$\forall x \in V \ \exists y \in V \ (x \sim y)$

$\forall x \in V \ \forall y \in V \ ((x \sim y) \Rightarrow (y \sim x))$

$\forall x \in V \ \forall y \in V \ \forall z \in V(((x \sim y) \wedge (y \sim z)) \Rightarrow (x \sim z))$,

dan is $\sim$ een equivalentierelatie.

§ 6. Definitie door abstractie.

6.1. Het komt in de wiskunde zeer veel voor dat men nieuwe begrippen vormt door in een bekende verzameling een equivalentierelatie te definiëren en vervolgens de equivalentieklassen als nieuwe objecten te beschouwen. Zo maakt de relatie uit voorbeeld 5.3.2 het ons mogelijk de richting van rechten te definiëren. In plaats van nu zeer onduidelijk te zeggen: "een richting is datgene wat gemeenschappelijk is aan twee evenwijdige rechten of iets dergelijks definiëert men: "een richting is een equivalentieklasse van de boven beschreven relatie". Correct in deze is de zegswijze: "l en m behoren tot dezelfde richting". Het spraakgebruik: "l en m hebben dezelfde richting", lijkt echter onuitwisbaar.

6.2. Een bekend voorbeeld van definitie door abstractie is de definitie van aantal. Individuen zijn verzamelingen van stoffelijke dingen. Men beschouwt de relatie: "x en y bestaan uit evenveel dingen", d.w.z.: "er bestaat een 1-1 afbeelding van x op y". Dit is een equivalentierelatie, $\sim$. We hebben dus: drie paarden $\sim$ drie glazen bier. Een aantal is een equivalentieklasse van deze relatie. Dit voorbeeld maakt duidelijk waarom het proces definitie door abstractie heet. "Abstractie" betekent "aftrekking". Wat afgetrokken wordt is paarden, glazen bier, ... (Bedenk dat ook aan de vorming van de begrippen: paard, glas bier enz. al een abstractie voorafgegaan is.) We zullen nu verschillende belangrijke voorbeelden van definitie door abstractie bespreken.

6.3. Gehele getallen. We nemen aan dat we over de natuurlijke getallen beschikken. We hebben behoefte aan een uitbreiding van Nt, bijv. omdat we vergelijkingen $a + x = b$ niet steeds in Nt kunnen oplossen. De gewenste uitbreiding van Nt, het systeem der gehele getallen, kan vanuit Nt gedefiniëerd worden met een definitie door abstractie. We doen dit slechts schetsmatig;

men overwege zelf alle details terdege. We "weten" dat elke geheel getal het verschil van twee elementen elementen uit Nt is (denk aan winst en verlies o.i.d.) : $-3 = 1-4 = 2-5 = \dots$, en ook $2 = 4-2 = 5-3 = \dots$. Vandaar komt men tot het idee paren van elementen uit Nt te beschouwen, waarbij (a,b) en (c,d) hetzelfde gehele getal voorstellen indien $a + d = b + c$.
Nu de exacte invoering.

Beschouw Nt $\times$ Nt; definiëer met deze verzameling als individuenverzameling de relatie $(a,b) \sim (c,d)$ door te stellen :

$$\forall\ (a,b) \in Nt \times Nt\ \ \forall\ (c,d) \in Nt \times Nt\ [\{(a,b) \sim (c,d)\} :\Leftrightarrow (a+d = b+c\ ].$$

Deze relatie is een equivalentierelatie. De equivalentieklassen (dat zijn deelverzamelingen van Nt $\times$ Nt) noemt men nu gehele getallen. Men moet nu voor de verkregen objecten arithmetrische operaties (som, product, verschil) en de $\geqslant$ relatie definiëren. We schetsen dit nu voor de som. Men zou + willen definiëren door:

$$\text{klasse}(a,b) + \text{klasse}(c,d) := \text{klasse}\ (a+c,\ b+d). \qquad (*)$$

D.w.z. men neemt een representant nl. (a,b) van de éne klasse en een representant (i.c. (c,d)) van de andere, telt deze coördinaatsgewijs op en noemt de klasse waartoe het paar (a+c, b+d) behoort de somklasse van de beide klassen. Men heeft pas het recht te stellen dat zo een optelling van klassen gedefiniëerd is, nadat men heeft laten zien dat bij de gedefinieerde optelling, - hoewel deze geformuleerd is met behulp van representanten- , de som-klasse onafhankelijk is van de keuze van de representanten. Voordat men (*) als definitie van de optelling van de gehele getallen kan geven moet men dus laten zien dat uit klasse (a,b) = klasse (a',b') en klasse (c,d) = klasse(c',d') volgt dat klasse $(a+c,\ b+d)$ = klasse $(a'+c',\ b'+d')$. Dit tonen we nu aan.
Nu betekent klasse (a,b) = klasse (a',b') dat $(a,b) \sim (a',b')$ en dus $a+b'=a'+b$. Hieruit en uit $c+d' = c'+d$ volgt inderdaad $a+b'+c+d' = b+a'+c'+d$ of $(a+c,\ b+d) \sim (a'+c',\ b'+d')$. We kunnen (*) dus als definitie van de optelling nemen.

De volgende stap is dat men laat zien dat de gedefiniëerde optelling commutatief en associatief is. Dan moet men vermenigvuldiging definiëren. Deze vermenigvuldiging zal moeten uitdrukken dat $(a-b)(c-d) = ac + bd - (ad+bc)$. Daarom definiëren we :

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

Nu te verifiëren :

1. De onafhankelijkheid van de representantkeuze.
2. De commutatieve en associatieve eigenschappen van de gedefiniëerde vermenigvuldiging.
3. De distributiviteitseigenschap van de vermenigvuldiging t.o.v. de optelling $(x(y+z) = xy + xz)$.

Een volgende definitie kan zijn :klasse $(a,b) >$ klasse (c,d) dan en slechts dan als $a+d > b+c$ waarbij dit laatste $>$ de bekende groter-relatie van de natuurlijke getallen weergeeft. Wederom moet men de onafhankelijkheid van de representantkeuze en alle eigenschappen verifiëren.

Als dit alles gedaan is, is men nog steeds niet klaar. Men wil immers het systeem van de gehele getallen beschouwen als uitbreiding van dat der natuurlijke getallen. Merk op dat de ingevoerde gehele getallen en de natuurlijke getallen dingen van totaal andere soort zijn. Als men echter aan het natuurlijk getal n toevoegt het gehele getal : klasse $(n + 1,1)$ dan corresponderen alle bewerkingen met natuurlijke getallen met de overeenkomstige bewerkingen met de gehele getallen. Zo komt $n + m$ overeen met

klasse $(n + m + 1,1) =$ klasse $(n + m + 2,2) =$

klasse $(n + 1,1) +$ klasse $(m + 1,1)$.

We maken dan ook geen onderscheid meer tussen het natuurlijk getal n en het gehele getal klasse $(n + 1,1)$. Men zegt dan dat men beide identificeert. Dit betekent dat de natuurlijke getallen zoals men die in de eerdere fase van de opbouw van het getalsysteem had, hun dienst gedaan hebben; ze worden

nu vervangen door de nieuw gedefiniëerde objecten : klasse $(n + 1,1)$.
Het enige dat men dan nog te doen heeft is de notatie voor gehele getallen te definiëren : $n := \text{klasse } (n+1,1)$; $0 := \text{klasse } (1,1)$; $-n := \text{klasse } (1, n+1)$ (n notatie van een natuurlijk getal). De eerste van deze drie regels brengt de bovenomschreven identificatie in de notatie tot uitdrukking.

6.4. Rationale getallen.

Opgave.

62. Neem aan dat we de beschikking hebben over het systeem der gehele getallen. Beschouw in Gh × Gh de deelverzamelingen W en V:

$$W := \{(g,0) \mid g \in Gh\}. \quad V := Gh \times Gh \setminus W.$$

Voor V als individuenverzameling definiëren we de relatie $(a,b) \sim (c,d)$ door

$$\forall (a,b) \in V \ \ \forall (c,d) \in V \ [\{(a,b) \sim (c,d)\} : \Leftrightarrow (ad = bc)].$$

Deze relatie stelt ons in staat om, op gelijke wijze als in 6.3. de gehele getallen ingevoerd zijn, nu de verzameling der gehele getallen uit te breiden tot die der rationale getallen. Geef een schets van deze invoering.

6.5. Gehele getallen mod m. Zij m een geheel getal. In de verzameling Gh der gehele getallen heeft men de equivalentierelatie: $a - b$ is een m-voud, d.w.z. $a - b = gm$ met $g \in Gh$. De klassen van deze equivalentierelatie heten de gehele getallen mod m (spreek uit : modulo m). Men ziet onmiddellijk dat de gehele getallen mod m en de gehele getallen mod $-m$ dezelfde zijn, men beperkt zich daarom tot natuurlijke m. (Wat zijn de gehele getallen mod 0?).
Neem bijv. $m = 4$. De gehele getallen mod 4 zijn nu de volgende vier verzamelingen :

$\{\ldots -8, -4, 0, 4, 8, 12, \ldots\}$;

$\{\ldots -7, -3, 1, 5, 9, 13, \ldots\}$;

$\{\ldots -6, -2, 2, 6, 10, 14, \ldots\}$;

$\{\ldots -5, -1, 3, 7, 11, 15, \ldots\}$.

De arithmetrische operaties definiëert men analoog aan 6.3, nl. :

klasse a + klasse b : = klasse (a + b)

klasse a • klasse b : = klasse ab.

Evenals in 6.3 moet men laten zien dat de gedefiniëerde sommen en producten onafhankelijk zijn van de keuze van de representanten. Daarna moet men de eigenschappen van commutativiteit, associativiteit en distributiviteit verifiëren. (Doe dit !)

Men noteert klasse a + klasse b = klasse c voor gehele modulo m als :
"$a + b \equiv c \bmod m$" of "$a + b \equiv c\ (m)$"; (men zegt: "a + b congruent c modulo m").
Analoog: $ab \equiv c \bmod m$. Iedere formule met de gehele getallen mod m kan men opschrijven met de representanten 0,1,2,... m-1. Historisch overgeleverd is het spraakgebruik:"met de gehele getallen rekenen mod m", alsof men slechts op een andere manier rekent met de gewone gehele getallen.

<u>Voorbeelden</u>: $2 + 3 \equiv 0\ (5)$; $2 \cdot 3 \equiv 1\ (5)$; $2 + 3 \equiv 5\ (6)$; $2 \cdot 3 \equiv 0\ (6)$.
Als p een priemgetal is, dan volgt uit $ab \equiv 0\ (p)$ dat $a \equiv 0\ (p)$ of $b \equiv 0\ (p)$.

§ 7. Aftelbare verzamelingen.

7.1. Gelijkmachtigheid.

Definitie. Twee verzamelingen V en W heten gelijkmachtig indien er een 1-1 duidige afbeelding van V op W bestaat.

Notaties : $V \sim W$: V en W zijn gelijkmachtig

$$V_n := \{1, 2, \ldots n\} \qquad (n \in \mathrm{Nt}).$$

Eigenschappen.

1. Gelijkmachtigheid is een equivalentierelatie op de klasse van de verzamelingen.
2. Als $V_n \sim V_m$, dan is $n = m$.

Opgaven.

63. Bewijs dat Nt en $\{0\} \cup \mathrm{Nt}$ gelijkmachtig zijn.

64. A en B zijn verzamelingen; bewijs dat $A \times B$ en $B \times A$ gelijkmachtig zijn.

65. Laat zien dat de verzamelingen I en C_1 gelijkmachtig zijn, waarbij

$$I := \{x \in \mathrm{Rl} \mid 0 \leqslant x < 1\};$$

$$C_1 := \{(x,y) \in R_2 \mid x^2 + y^2 = 1\}.$$

7.2. Aftelbare verzamelingen.

Definities.

Een verzameling V heet eindig indien er een natuurlijk getal n bestaat met $V \sim V_n$. V heet oneindig indien V niet eindig is. V heet aftelbaar indien $V \sim \mathrm{Nt}$. Een 1-1 afbeelding van Nt op V heet aftelling van V.

De aftelbare verzamelingen spelen een belangrijke rol. Zij zijn weliswaar oneindig maar toch nog overzichtelijk op te schrijven : als f een aftelling van V is dan is V = $\{f(1), f(2), f(3), \ldots\}$. Vaak schrijft men f_1 i.p.v. f(1) enz.

Opmerking.

Oneindige verzamelingen kunnen gelijkmachtig zijn met een echte deelverzameling: zo is $x \to 2x$ een 1-1 afbeelding van Nt op de verzameling der even getallen. (Zie opgave 44.) Deze eigenschap karakteriseert de oneindige verzamelingen. We hebben : Een verzameling V is oneindig dan en slechts dan als V gelijkmachtig is met een echte deelverzameling.

Definitie. Een verzameling, die niet leeg, niet eindig en niet aftelbaar is, heet overaftelbaar.

Voorbeeld. De verzameling A van alle afbeeldingen van Nt in $\{0,1\}$ is een voorbeeld van een oneindige verzameling waarvoor het niet lukt een aftelling aan te geven. Ieder element van A is een rij nullen en enen. Stel dat A aftelbaar is dan is er een aftelling F van A, bijv. :

$$F_1 = (\underline{0}, 0, 1, 1, 0, 0, 1, 0, 1, 0, \ldots),$$
$$F_2 = (1, \underline{1}, 0, 0, 0, 0, 0, 1, 0, 1, \ldots),$$
$$F_3 = (0, 1, \underline{0}, 0, 1, 1, 1, 1, 1, 0, \ldots), \ldots\ldots\ldots$$

Zij $F_i(j)$het j^{de} cijfer uit de rij F_i. We construeren nu een element $(a_1, a_2, \ldots)$ ($a_i = 0$ of 1) van A dat niet in de aftelling voorkomt. Neem nl. $a_1 \neq F_1(1)$; $a_2 \neq F_2(2)$, $a_3 \neq F_3(3)$ ... . In ons voorbeeld zouden we dus hebben (1, 0, 1, ...). F is dus geen afbeelding van Nt op A; F is dus geen aftelling. A is overaftelbaar. De in dit voorbeeld gebruikte constructie-methode heet het diagonaalprocédé van Cantor.

Met behulp van het diagonaalprocédé van Cantor toont men aan dat de verzameling der reële getallen overaftelbaar is.

7.3. Verenigingen van aftelbare verzamelingen.

Stelling 1. De vereniging van twee aftelbare verzamelingen is aftelbaar.

Bewijs. Zij $V_1 = \{a_1, a_2, \ldots\}$; $V_2 = \{b_1, b_2, \ldots\}$, dan is $V_1 \cup V_2 = \{a_1, b_1, a_2, b_2 \ldots\}$. Schrap in de laatste rij, van links naar rechts gaande, ieder element dat men al eerder gehad heeft. Wat overblijft is een rij verschillende elementen. $V_1 \cup V_2$ is dus aftelbaar. q.e.d.

Gevolgen. 2. De vereniging van eindig veel aftelbare verzamelingen is aftelbaar.

3. De verzameling der gehele getallen is aftelbaar.

Stelling 4. De vereniging van een aftelbare collectie aftelbare verzamelingen is aftelbaar, d.w.z. is $I = \{i_1, i_2, i_3, \ldots\}$ aftelbaar en is aan iedere element uit I een aftelbare verzameling W_i toegevoegd dan is $W := \cup_{i \in I} W_i$ aftelbaar.

Bewijs. Zij

$$W_{i_1} = \{w_{11}, w_{12}, w_{13}, w_{14}, w_{15}, \ldots\}$$
$$W_{i_2} = \{w_{21}, w_{22}, w_{23}, w_{24}, w_{25}, \ldots\}$$
$$W_{i_3} = \{w_{31}, w_{32}, w_{33}, w_{34}, w_{35}, \ldots\}$$
$$\vdots$$

Nu is

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

Laat links beginnend de elementen uit deze rij weg die al eerder zijn voorgekomen. Voegt men dan aan n toe het element van W dat op de n^{de} plaats in de uitgedunde rij staat dan is dat een aftelling van W. q.e.d.

Het in dit bewijs gebruikte proces heet digonaalprocédé van Cauchy.

Gevolg 5. De verzameling der rationale getallen is aftelbaar.

Bewijs. $Rt = \bigcup_{n \in Nt} W_n$ waarbij :

$$W_1 := \{0, 1, -1, 2, -2, \ldots\}$$

$$W_2 := \{0, \tfrac{1}{2}, -\tfrac{1}{2}, \tfrac{2}{2}, -\tfrac{2}{2}, \ldots\}$$

$$W_3 := \{0, \tfrac{1}{3}, -\tfrac{1}{3}, \tfrac{2}{3}, -\tfrac{2}{3}, \ldots\}$$

$$\vdots$$

7.4. Voorbeelden en eigenschappen.

1. $\{x \mid x \in Rl,\ \tan x \in Rt\}$ is aftelbaar.

2. Is V een aftelbare verzameling, en is $W \subset V$ dan is W eindig of aftelbaar.

3. Zijn V en W aftelbaar dan is $V \times W$ aftelbaar.
Zijn $V_1, V_2, \ldots, V_k$ aftelbaar, dan is $V_1 \times V_2 \times \ldots \times V_k$ aftelbaar.

4. De vereniging van een aftelbare collectie eindige verzamelingen is eindig of aftelbaar.

5. W zij de deelverzameling van de verzameling van alle afbeeldingen van Nt in $\{0,1\}$ gedefiniëerd door :
$W := \{f \mid f : Nt \to \{0,1\}, \exists n \in Nt\ \forall m > n\ (f(m) = 0)\}$. W is aftelbaar.

6. Zij $f : A \to B$ een afbeelding van A op B, zij A aftelbaar, dan is B eindig of aftelbaar.

7.5. Opgaven.

66. Bewijs dat de verzameling van alle punten uit R_2 met uitsluitend rationale coördinaten aftelbaar is.

67. Bewijs dat de volgende verzamelingen aftelbaar zijn.
$A := \{x \in Rl \mid x^2 \in Rt\}$;
$B := \{x \in Rl \mid \sin x \in Rt\}$.

68. V is een aftelbare verzameling. Bewijs dat het n-voudige cartesische product $V \times V \times V \times \ldots \times V$ aftelbaar is.
Als men het aftelbaar-voudige cartesische product $V \times V \times V \times \ldots$ definiëert als de verzameling van alle geordende rijen $(a_1, a_2, \ldots\ldots)$ met $a_i \in V (i \in Nt)$, bewijs dan dat

$$V \times V \times V \times \ldots\ldots\ldots\ldots \text{ overaftelbaar is.}$$

69. V is een aftelbare verzameling; W is de verzameling van alle eindige deelverzamelingen van V. Bewijs dat W aftelbaar is.

Hoofdstuk III. Voorbeelden van "abstracte" wiskunde.

§ 8. Over de opbouw van een wiskundige theorie.

8.1. Definiëren en bewijzen.

Zonder ons op het terrein van het grondslagenonderzoek te begeven, willen we enige aandacht wijden aan de opbouw van een wiskundige theorie. Vooreerst moet men duidelijk twee dingen onderscheiden :

1. het verwerven van wiskundige inzichten, en
2. het vastleggen daarvan.

Over de wijze van het tot stand komen van wiskundige kennis bestaat weinig zekerheid. Zeker zullen van beoefenaar tot beoefenaar verschillen optreden. Ervaring speelt een belangrijke rol. Het onderzoek van dit totstandkomingsproces is werk voor psychologen, al zal men zich voor de didactiek der wiskunde van bepaalde aspecten ervan rekenschap moeten geven.
Het vastleggen van de wiskundige kennis heeft tot doel aan de verkregen kennis de hoogst mogelijke graad van zekerheid en duidelijkheid te waarborgen. Ideaal zou zijn de wiskundige kennis zo te beschrijven, dat elke voorkomende uitdrukking verklaard, elke bewering bewezen wordt. Enig nadenken leert echter dat dit onmogelijk is. Om een uitdrukking te verklaren heb ik andere begrippen nodig, die zelf al weer eerder verklaard hadden moeten zijn m.b.v. ,,,,, . Met de beweringen is het al net zo gesteld: een bewering wordt bewezen m .b.v. weer andere beweringen, die, ,,, .

Vragen hoe men in feite een theorie dan wel moet vastleggen; wat men de hoogst mogelijke zekerheid noemt, zijn filosofische vragen. De waarde die men aan door ervaring verkregen inzichten toekent, speelt bij de beantwoording een belangrijke rol. Wij zullen er ons niet in verdiepen.

We zullen slechts beschrijvenderwijs nagaan wat thans (1969) vrijwel algemeen aanvaarde principes bij het vastleggen van wiskundige theorieën zijn.

Men zoekt allereerst een klein aantal tot de vast te leggen theorie behorende begrippen die onmiddellijk begrijpelijk schijnen (bijv. punt, lijn, evenwijdigheid, ... in de meetkunde). Deze begrippen worden zonder verklaring gebruikt. Men noemt ze de primitieve of ongedefiniëerde begrippen van de theorie. In hoofdstuk I § 1.1 voerden we de begrippen verzameling en "element van" als primitieve begrippen in. De grondlegger van de verzamelingenleer, Georg Cantor (1845-1918), omschreef een verzameling als : "Eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die Elemente genannt werden) zu einem Ganzen". Uit deze formulering kan iemand die nog helemaal niets weet beslist niet leren wat een verzameling is, evenmin als iemand die niet weet wat een punt is veel geholpen wordt door Euclides' begripsbepaling : "een punt is datgene wat geen afmeting heeft". Ook in hoofdstuk I § 4.1 is een begrip als primitief begrip ingevoerd nl. "geordend paar". Dat is toen echter gemakshalve gebeurd. Geordende paren kunnen met behulp van de begrippen verzameling en element (maar zonder het nog onverklaarde begrip : volgorde) goed gedefiniëerd worden.
Tegelijk met het aangeven van de primitieve begrippen aanvaardt men de verplichting van elk ander begrip de betekenis vast te leggen m.b.v. de primitieve begrippen en reeds "eerder" verklaarde begrippen. De zin die de betekenis van een begrip vastlegt heet de definitie van dat begrip.

Op soortgelijke wijze gaat men te werk bij de beweringen. Een aantal evident lijkende beweringen wordt zonder bewijs als waar aangenomen. Men noemt ze axioma's of postulaten. Alle andere beweringen moeten bewezen worden m.b.v. eerder bewezen beweringen en axioma's.

Wat we tot nu gezegd hebben heeft betrekking op de opbouw van een stuk wiskunde van de grond af. We zullen echter zelden stukken wiskundige theorie ontmoeten die helemaal bij het begin aanvangen. Bij de differentiaalrekening worden bijv. de eigenschappen der reële getallen reeds aanwezig verondersteld. De meeste wiskundige theorieën berusten weer op theorieën die er aan voorafgaan. We zullen ons daarom nu niet bezig houden met axioma's.
-Men begrijpt echter wel dat men aan een axiomastelsel zekere eisen moet stellen, bijv. dat het geen tegenspraak bevat.- Evenmin spreken we over primitieve termen.

De processen die men op ieder niveau van opbouw van de wiskunde voortdurend bedrijft zijn definiëren en bewijzen. Men overwege de analogie die er tussen beide bestaat.

Het is gebruikelijk bij het wiskundeonderwijs veel aandacht te geven aan bewijzen. Iedereen weet dat bewijzen volledig dienen te zijn, en van het te bewijzene niet verkapt al gebruik mogen maken (vicieuze cirkel bij het bewijzen). Het is goed dat men zich bewust is dat dezelfde eisen voor definities gelden: De definitie moet zijn een volledige verklaring van het te definiëren begrip m.b.v. uitdrukkingen waarvan de betekenis onafhankelijk van het te definiëren begrip vastligt.
Een vicieuze cirkel bij het definiëren kan de gehele verder theorie waardeloos maken. Het is van belang dat de zinnen die een nieuw begrip definiëren als zodanig kenbaar zijn. Dit kan gebeuren door ze vooraf te laten gaan door het woord : "definitie", maar ook door het gebruik van zinswendingen als : "we zeggen dat ..."; "een ... heet ..."; "... noemen we ...".
Stel bijv. dat we de rekenkunde aan het opbouwen zijn en dat we weten wat de relatie $>$ betekent. Een correcte definitie is dan : "we zeggen dat $x \leqslant y$, (dan en dan alleen) indien het niet zo is dat $x > y$." We geven dus precies

aan welke paren getallen aan de te definiëren relatie voldoen. In heel de verdere theorie kan $x \leq y$ zonder bezwaar vervangen worden $(x > y)$. Anderzijds is de volgende formulering ontleend aan de oude versie van het wegenverkeersreglement een voorbeeld van een begripsbepaling die als definitie onaanvaardbaar is.

"Onder wegen dient men te verstaan : alle voor het openbaar verkeer openstaande wegen of paden; de in de wegen liggende bruggen en duikers alsmede de tot de wegen behorende voet- en rijwielpaden en bermen."

8.2. Abstracte wiskundige theorieën.

Bovenstaande opmerkingen over de opbouw van een wiskundige theorie gelden voor elke vorm van wiskunde. We zullen nu stilstaan bij wat men heden abstracte wiskunde noemt. Eigenlijk is de uitdrukking onzinnig; alle wiskunde is abstract. Waarin het onderscheid tussen z.g. concrete en z.g. abstracte wiskunde bestaat illustreren we aan een voorbeeld (uit Wiskunde I). Men heeft vectoren in de ruimte, voorgesteld door pijlen en uitgaande van een vast punt O (dit zijn abstracties van bijv. krachten of snelheden uit de mechanica). Men heeft ook $R1 \times R1 \times R1$. Vectoren in de ruimte kan men optellen, vermenigvuldigen met getallen. Elementen van $R1 \times R1 \times R1$ kan men optellen en vermenigvuldigen met getallen. Deze beide bewerkingen voldoen aan precies dezelfde regels. Ieder bewijs voor vectoren dat alleen gebruik maakt van deze bewerkingen geldt mutatis mutandis voor elementen uit $R1 \times R1 \times R1$. Men definiëert nu het abstracte begrip vectorruimte. Dit is een verzameling waarvan men <u>afziet</u> van de aard der elementen (vandaar abstract), en waarin bewerkingen gedefiniëerd worden, die overeenkomen met optelling en scalaire vermenigvuldiging. Elke eigenschap die men voor de abstracte vactorruimte bewezen heeft geldt in elke "concrete" realisatie (of model) ervan.

De tegenstelling tussen concrete en abstracte wiskunde wordt aldus in het leven geroepen, zodra men er toe komt verschillende theorieën in een grotere theorie samen te vatten, waarvoor het dan nodig is van specifieke eigenschappen van de objecten van de "kleinere"theorieën af te zien. De omvattende theorie heet dan abstract tegenover de concrete kleinere theorieën. Een abstracte theorie voorkomt dat men analoge redeneringen moet herhalen in verschillende gevallen; hij is echter ook steeds "armer" dan de concrete theorieën, in die zin dat over allerlei speciale eigenschappen niet meer gesproken kan worden.
Het bovenstaande maakt ook duidelijk dat het afhangt van de ontwikkelingsfase van de wiskunde wat men concreet, wat abstract noemt. Voor ons is R_3 concreet, maar het begrip vectorruimte abstract. In een volgende ontwikkelingsfase bestudeert men abstracte algebraïsche systemen waarvan de vectorruimten dan concrete realisaties zijn.

We zullen in de volgende paragrafen twee voorbeelden bespreken. In beide gevallen wordt het voorwerp van de theorie vastgelegd door twee dingen :

1. Een verzameling V, waarvan men de aard der elementen in het midden laat.
2. Een beweringsvorm met individuenverzameling V, waarvan een aantal eigenschappen als axioma's gepostuleerd worden.

Niet iedere abstracte wiskundige theorie heeft een dergelijk eenvoudig voorwerp; de theorie der vectorruimten is al ingewikkelder (waarom?).

§ 9. Geordende verzamelingen.

9.1. Partiëel geordende verzamelingen.

Definitie 1. Een (partiëel) geordende verzameling is een paar (V, R(x,y)) waarin V een verzameling is en R(x,y) een relatie met de elementen van V als individuen en met de volgende eigenschappen.

O_1 R(x,y) is transitief.

O_2 $\forall\, x \in V\, [\neg R(x,x)]$ (anti reflexief).

De relatie R(x,y) heet een (partiële) ordening of orderelatie op V. Heel vaak spreekt men slordig over de geordende verzameling V i.p.v. over (V, R(x,y)). Vaak gebruikt men voor het aangeven van orderelaties symbolen als $<$, $\measuredangle$, $\propto$, $\lessdot$. De geordende verzameling duidt men dan aan als (V, <), (V, $\measuredangle$) enz. (Zie pag.21 voor de notatie < i.p.v. x < y.)
Als $V \subset Rl$, dan duidt < steeds de "gewone" ordening der reële getallen aan. (Ga na dat deze inderdaad de eigenschappen O_1 en O_2 heeft.) "x < y" spreekt men uit als: "x kleiner (eerder) dan y"; "x gaat vooraf aan y".
Eigenschap. 1. Is (V, R(x,y)) een geordende verzameling; $a \in V$, $b \in V$, dan is hoogstens één van de drie beweringen R(a,b), R(b,a), a = b, waar.

Bewijs. Als a = b waar is, is op grond van O_2, $\neg R(a,b)$ waar dus R(a,b) = R(b,a) onwaar. Als R(a,b) waar is, dan is a = b onwaar (wegens O_2). Ook R(b,a) is onwaar, want wegens O_1 zou uit R(a,b) en R(b,a), R(a,a) volgen.

Definitie 2. Als $R(a,b) \vee R(b,a) \vee (a = b)$ waar is, dan heten a en b vergelijkbaar. Twee verschillende elementen a en b zijn dus vergelijkbaar als a voorafgaat aan b, of b voorafgaat aan a.
Voorbeelden.

1. Op de verzameling van alle mannen is de relatie :"x is een voorvader van y" een partiële ordening.

2. Op Nt is de relatie "x is een echte deler van y" een partiële ordening (echte deler betekent: $\exists n > 1 \ (y = nx)$).

3. Op iedere verzameling is de "lege" relatie d.i. de relatie waaraan geen enkel paar voldoet een partiële ordering.

4. Zij W een verzameling; V de verzameling van alle deelverzamelingen van W (notatie: $V =: P(W)$). Op V is de relatie $(X \subset Y) \wedge (X \neq Y)$ een partiële ordening. We noteren de zo ontstane partiëel geordende verzameling met $(P(W), \subset)$. Spreek $\subset$ uit als: "echt deel van").

5. Zij Φ de verzameling van alle reële functies gedefiniëerd op een verzameling W. (Dus Φ is de verzameling van alle afbeeldingen van W in Rl). Nu is $(\Phi, \prec)$ een partiëel geordende verzameling als $\prec$ gedefiniëerd is door :

$$[(f_1 \prec f_2) :\Leftrightarrow \forall x \in W \ (f_1(x) - f_2(x) < 0)] \quad (f_1 \in \Phi \ , \ f_2 \in \Phi).$$

9.2. Lineair geordende verzamelingen.

Definitie. Een partiëel geordende verzameling $(V, R(x,y))$ heet lineair (of: totaal) geordend indien ieder tweetal elementen vergelijkbaar is. De orderelatie voldoet dan dus aan :

O_3 : $\forall x \in V \ \ \forall y \in V \ [R(x,y) \vee R(y,x) \vee (x = y)]$.

Voorbeelden.

1. De relatie "$x < y$" op Rl is een lineaire ordening.

2. Van de vectorruimte R_3 maakt men een lineair geordende verzameling door invoering van de volgende relatie

$$(\underline{a} \lessdot \underline{b}) :\Leftrightarrow [(a_1 < b_1) \vee \{(a_1 = b_1) \wedge (a_2 < b_2)\} \vee$$
$$\vee \{(a_1 = b_1) \wedge (a_2 = b_2) \wedge (a_3 < b_3)\}], \ (\underline{a} = (a_1, a_2, a_3), \ \underline{b} = (b_1, b_2, b_3) \in R_3).$$

Een dergelijke ordening heet lexicografische ordening.

3. Bij iedere aftelling van een aftelbare verzameling $V = \{a_1, a_2, \ldots\}$ hoort op natuurlijke wijze een lineaire ordening; deze is gedefiniëerd door :

$$(a_n < a_m) :\Leftrightarrow (n < m). \quad (a_n, a_m \in V).$$

4. Op Nt is de relatie $\propto$ gedefinieerd door

$$(x \prec y) :\Leftrightarrow \{(x \text{ even en } y \text{ oneven}) \vee (x \text{ even, } y \text{ even, } x < y) \vee$$
$$\vee (x \text{ oneven, } y \text{ oneven, } x < y)\} \quad (x \in Nt, y \in Nt).$$

geeft op Nt een lineaire ordening waarbij alle even getallen vooraf-gaan aan de oneven getallen.

5. Op Gh is de relatie $<\cdot$ gedefiniëerd door :

$$(x <\cdot y) :\Leftrightarrow [\{|x| < |y|\} \vee \{(|x| = |y|) \wedge (x < y)\}] (x \in Gh, y \in Gh).$$

een lineaire ordening.

9.3. Kleinste elementen, minimale elementen.

Definitie 1. In iedere partiëel geordende verzameling $(V,<)$ definiëert men de relatie $\leqslant$, $>$, $\geqslant$ door :

$\forall x \in V \ \forall y \in V \ [(x \leqslant y) :\Leftrightarrow \{(x < y) \vee (x = y)\}]$;

$\forall x \in V \ \forall y \in V \ [(x > y) :\Leftrightarrow (y < x)]$;

$\forall x \in V \ \forall y \in V \ [(x \geqslant y) :\Leftrightarrow (y \leqslant x)]$.

Eigenschap 1. Is $(V, <)$ een partiëel geordende verzameling, is $a \in V$, $b \in V$, $a \leqslant b$, $b \leqslant a$, dan is $a = b$.

Definities. Steeds stelt $(V, <)$ een partiëel geordende verzameling voor.

2. $a \in V$ heet kleinste of eerste element van $(V, <)$ indien

$$\forall x \in V \ (a \leqslant x).$$

2'. $b \in V$ heet grootste of laatste element van $(V, <)$ indien

$$\forall x \in V \ (x \leqslant b).$$

Eigenschap 2. $(V, <)$ heeft hoogstens één kleinste en hoogstens één grootste element.

Bewijs. Laat $a \in V$ en $b \in V$ kleinste elementen zijn; dan is $\forall x \in V \; (a \leqslant x)$ en $\forall \, x \in V \; (b \leqslant x)$, dus in het bijzonder $a \leqslant b$ en $b \leqslant a$, dus $a = b$.

Voorbeelden. Van de voorbeelden in 9.1 en 9.2 hebben de navolgende een kleinste element, dat we tussen haakjes vermelden : 9.1.1 (Adam(?)); 9.1.2 (1) ; 9.1.4 ($\emptyset$) ; 9.2.3 (a_1) ; 9.2.4 (2) ; 9.2.5 (0).

Definities.

3. $a \in V$ heet minimaal element van $(V, <)$ indien $\forall x \in V \; [(x \leqslant a) \Rightarrow (x = a)]$.

3'. $b \in V$ heet maximaal element van $(V, <)$ indien $\forall x \in V \; [(x \geqslant a) \Rightarrow (x = a)]$.

a minimaal betekent dus: $a \leqslant x$ voor alle x die met a vergelijkbaar zijn.

Eigenschappen.

3. Als $(V, <)$ een kleinste (grootste) element heeft dan is dit het enige minimale (maximale) element. (Vergelijk deze uitspraak met voorbeeld 3.)

4. Een lineair geordende verzameling heeft hoogstens één minimaal (maximaal) element, dat tevens het kleinste (grootste) element is.

Voorbeelden:

1. Voor $Nt \setminus \{1\}$ met als ordeningsrelatie "x is een echte deler van y" zijn alle priemgetallen minimale elementen.

2. Voor $P(W) \setminus \{\emptyset\}$ en echte inclusie als ordeningsrelatie zijn alle één-puntsdeelverzamelingen van W minimale elementen.

3. Op $Gh \setminus \{0\}$ is een partiële ordeningsrelatie $\propto$ gedefiniëerd door

$$x \propto y \;:\Leftrightarrow\; ((xy > 0) \wedge (x < y)) \qquad (x \in Gh,\; y \in Gh).$$

Van $(Gh, \propto)$ is 1 het enige minimale element en $(Gh, \propto)$ heeft geen kleinste element.

9.4. Deelverzamelingen van een geordende verzameling.

Is $(V, \prec)$ een geordende verzameling, is $U \subset V$ dan is $(U, \prec)$ ook een geordende verzameling, waarbij de orderelatie in U de beperking (restrictie) tot U is van de orderelatie uit V. Deze ordening heet de door $(V, \prec)$ op U geïnduceerde ordening. Als $(V, \prec)$ minimale elementen heeft en $U \subset V$, dan hoeft $(U, \prec)$ geen minimale elementen te hebben.

Definitie 1. Zij $(V, <)$ een geordende verzameling, $U \subset V$. Een element $a \in V$ heet benedengrens (resp. bovengrens) indien $\forall x \in U\ (a \leq x)$, (resp. $\forall x \in U\ (a \geq x)$).

Eigenschappen.

1. Als a een benedengrens van U is en $a \in U$, dan is a het kleinste element van U bij de geïnduceerde ordening.

2. Als V zelf een kleinste element heeft, dan is dit benedengrens van iedere deelverzameling.

Definities.

2. Zij $(V, <)$ een geordende verzameling, $U \subset V$. Als de verzameling van benedengrenzen van U een grootste element heeft dan heet dit het infimum van U (notatie: inf U). Let op: inf U behoeft niet in U te liggen.

2'. Als de verzameling van bovengrenzen van U een kleinste element heeft dan heet dit het supremum van U (notatie: sup U).

Eigenschappen.

3. Iedere deelverzameling van een geordende verzameling heeft hoogstens één infimum en hoogstens één supremum.

4. Is $(V <)$ een geordende verzameling en $U \subset V$ dan betekent $w = \inf U$:

   1. $\forall u \in U (w \leq u)$ en
   2. $\forall v \in V\ [\{\forall u \in U (v \leq u)\} \Rightarrow (v \leq w)]$

Voorbeelden.

1. $(P(W), \subset)$; is $U := \{A_i | i \in I\}$ een deelverzameling van $P(W)$ (dus $A_i \subset W$ $(i \in I)$) dan is :

$$\inf U = \cap_{i \in I} A_i \text{ ;}$$

$$\sup U = \cup_{i \in I} A_i \text{ .}$$

2. We beschouwen R_2 met de ordeningsrelatie $\prec$ gedefiniëerd door :
$\underline{a} \prec \underline{b} :\Leftrightarrow (a_1 < b_1) \wedge (a_2 < b_2)$, $(\underline{a} = (a_1,a_2)$, $b = (b_1,b_2)$, $\underline{a},\underline{b} \in R_2)$.
Zij $U := \{(x,y) \mid x^2 + y^2 < 1\}$.
De verzameling van de benedengrenzen van U is $\{(x,y) \mid x \leq -1, y \leq -1\}$;
U heeft geen infimum.

9.5. Opgaven.

70. $N = \{x \in Nt \mid x \geq 2\}$. Is de relatie $n \prec m$ gedefiniëerd door : "het aantal priemfactoren van n is kleiner dan dat van m" een partiële (lineaire) ordening op N ? Is er een kleinste element ? Zijn er minimale elementen ? Beschouw de verzamelingen $N_1 = \{15,30\} \subset N$ en $N_2 = \{15,30,35\}$. Welke zijn de benedengrenzen van N_1, van N_2 ? Bestaan $\inf N_1$, $\inf N_2$, $\sup N_1$, $\sup N_2$?

71. Bepaal benedengrenzen, bovengrenzen, infima, suprema, grootste en kleinste elementen van de volgende deelverzamelingen van Rl met de gebruikelijke ordening.

(a) $\{x \mid 0 < x < 1\}$;

(b) $\{x \mid 0 \leq x < 1\}$;

(c) $\{x \mid x^2 \in Nt\}$.

72. V is een verzameling; $f : V \to Nt$. We definiëren
$\forall v \in V \ \forall w \in V \ [(v <^* w) :\Leftrightarrow f(v) < f(w)]$.

Is $(V, <^*)$ een partiëel geordende verzameling ? Welke zijn de minimale elementen van $(V, <^*)$?

Bewijs dat de ordening $<^*$ lineair is dan en slechts dan als f 1-1 duidig is.

73. $\forall\ (x,y) \in R_2 \quad \forall (u,v) \in R_2 \quad [((x,y) \prec (u,v)) :\Longleftrightarrow \{(x=u) \wedge (y<v)\}]$.

(a) Laat zien dat $(R_2, \prec)$ een partiëel geordende verzameling is.

$V := \{(x,y) \in R_2 \mid 0 < x \leq 1,\ 0 < y \leq 1\}$.

(b) Heeft V benedengrenzen of bovengrenzen ?

(c) Welke zijn de minimale en maximale elementen van $(V, \prec)$?

74. In de verzameling Nt der natuurlijke getallen wordt de relatie $<_\circ$ gedefiniëerd door :

$\forall n,m \in Nt$ [$n <_\circ m$ $:\Longleftrightarrow$ de grootste priemfactor van n is kleiner dan de grootste priemfactor van m]

Gevraagd :

(a) Is $(Nt, <_\circ)$ een (partiëel) geordende verzameling ?

(b) Heeft Nt een kleinste element? en een grootste ?

(c) Bedenk een aftelbare deelverzameling van Nt die een bovengrens heeft ? Heeft deze verzameling een supremum ?

75. Op de verzameling P(Nt) van alle deelverzamelingen van Nt definiëren we

$\forall\ A \subset Nt \quad \forall B \subset Nt\ [(A \blacktriangleleft B) :\Longleftrightarrow \exists a \in A \quad \forall b \in B\ (a < b)]$.

(a) Is $(P(Nt), \blacktriangleleft)$ een partiëel geordende verzameling ?

(b) Heeft $(P(Nt), \blacktriangleleft)$ een grootste element ?

(c) Heeft $(P(Nt), \blacktriangleleft)$ minimale elementen ?

§ 10. Groepen.

10.1. Productoperaties.

Definitie 1. Zij V een verzameling. Een productoperatie in V is een afbeelding $\varphi: V \times V \to V$. Aan ieder geordend paar (a,b) van elementen uit V is dus toegevoegd een element uit V : $\varphi((a,b))$.

Voorbeelden.

1.	$V = Rl$;	$\varphi((a,b)) = ab$
2.	$V = Rl$;	$\varphi((a,b)) = a + b$
3.	$V = R_2$;	$\varphi((\underline{a},\underline{b})) = \underline{a} + \underline{b}$
4.	$V = \{f \mid f : Rl \to Rl\}$;	$\varphi((f,g)) = f \circ g$ (zie § 4.7)
5.	$V = Rl$;	$\varphi((a,b)) = \frac{1}{2}(a + b)$.

Definitie 2. Een productoperatie in V heet commutatief indien

$$\forall (a,b) \in V \times V\ [\varphi((a,b)) = \varphi((b,a))].$$

De productoperaties in de voorbeelden 1, 2, 3 en 5 zijn commutatief, die in 4 is dat niet.

Men noemt $\varphi((a,b))$ het product van a en b en noteert het meestal met ab; soms ook $a \,.\, b$, $a \times b$, $a \circ b$, $a * b$, of $a + b$. Om aan te geven welke productnotatie men heeft, geven we in deze gevallen de verzameling met productoperatie aan met (V,);(V, .); (V,×); (V,∘); (V,*) of (V, +).

Definitie 3. De productoperatie in (V,) heet associatief indien :

$$\forall a \in V\ \ \forall b \in V\ \ \forall c \in V\ [(ab)c = a(bc)].$$

De productoperaties in de voorbeelden 1, 2, 3 en 4 zijn associatief, die in 5 is dat niet.

<u>Definitie 4.</u> Een element $e \in V$ heet <u>eenheidselement</u> van de verzameling met productoperatie (V,) indien :

$$\forall a \in V \; [ae = ea = a].$$

In de voorbeelden 1, 2, 3 en 4 is er een eenheidselement en wel achtereenvolgens 1, 0, $\underline{0}$, I_{R1} (zie § 4.6 def. 4). In voorbeeld 5 is er geen eenheidselement.

<u>Stelling 1.</u> Een verzameling met productoperatie (V,) heeft hoogstens één eenheidselement.

<u>Bewijs</u> (Vergelijk § 9.3 eigenschap 2). Stel dat e_1 en e_2 eenheidselementen zijn, dan is $\forall a \in V \; [ae_1 = e_1a = a]$ en $\forall a \in V \; [ae_2 = e_2a = a]$ dus in het bijzonder is $e_2e_1 = e_1e_2 = e_2$ en $e_1e_2 = e_2e_1 = e_1$ dus $e_1 = e_2$. q.e.d.

<u>Definitie 5.</u> Is a een element van een verzameling met productoperatie (V,) die een eenheidselement e heeft, en is $b \in V$ zó dat $ab = ba = e$, dan heet b een inverse van a.

In voorbeeld 1 heeft iedere $a \neq 0$ een inverse en wel $\frac{1}{a}$; in voorbeeld 2 heeft elke a een inverse: $-a$; in voorbeeld 3 heeft elke vector $\underline{a}$ een inverse: $-\underline{a}$; in voorbeeld 4 hebben alleen de functies f die 1-1 duidig en <u>op</u> zijn een inverse: f^{-1}.

<u>Stelling 2.</u> Zij (V,) een verzameling met een associatieve productoperatie en een eenheidselement. Een element $a \in V$ heeft hoogstens één inverse.

<u>Bewijs.</u> Laat b_1 en b_2 beide inversen van a zijn, d.w.z. $b_1a = ab_1 = b_2a = ab_2 = e$. Nu is $(b_1a)b_2 = eb_2 = b_2$. Bovendien is $(b_1a)b_2 = b_1(ab_2) = b_1e = b_1$. Dus $b_1 = b_2$.

Opmerking. Als b de inverse van a is, is a de inverse van b. Voor de inverse van a gebruikt men de notatie a^{-1}.

Opgaven.

76. V is een verzameling. In de verzameling van alle deelverzamelingen (P(V)) beschouwen we achtereenvolgens de productoperaties

(a) $\cap$; (b) $\cup$; (c) $\setminus$; (d) $\div$ (zie opgave 7 f).

Ga na welke van deze operaties commutatief zijn, welke associatief. Ga na in welke gevallen er een eenheidselement is, en welke elementen in deze gevallen een inverse hebben.

77. De product operatie $k : Nt \times Nt \to Nt$ voegt aan elk paar natuurlijke getallen hun kleinste gemene veelvoud toe.

(a) Is k commutatief ?

(b) Is k associatief ?

(c) Heeft (Nt,k) een eenheidselement ?

(d) Bepaal alle elementen die een inverse bezitten.

78. De productoperatie $\varphi : Rl \times Rl \to Rl$ wordt als volgt gedefiniëerd :

$$\forall (a,b) \in Rl \times Rl[\varphi((a,b)) := a + b - ab].$$

(a) Is φ commutatief ?

(b) Is φ associatief ?

(c) Zoek het eenheidselement;

(d) Geef aan welke elementen een inverse bezitten.

10.2. Groepen.

Definitie 1. Een verzameling met productoperatie heet een groep indien aan de volgende drie axioma's voldaan is :

G1. De productoperatie is associatief.

G2. Er is een eenheidselement.

G3. Ieder element heeft een inverse.

Definitie 2. Een groep (G,) met een commutatieve productoperatie heet ook abelse of commutatieve groep (N.H.Abel 1802-1829).

Voorbeelden. Een voorbeeld van een groep, (G,φ) bestaat steeds uit twee dingen : een verzameling G en een afbeelding $\varphi : G \times G \rightarrow G$ waarbij aan G1, G2 en G3 voldaan is.

1. Voorbeeld 10.1.2. Additieve groep of optelgroep der reële getallen.

2. $G = \{x \in Rl \mid x \neq 0\}$, $\varphi((a,b)) = ab$ (gewone vermenigvuldiging). Multiplicatieve groep der reële getallen $\neq 0$.

3. $G = \{x \in Rl \mid x > 0\}$; $\varphi((a,b)) = ab$.
   Multiplicatieve groep der positieve reële getallen.
   N.B. Op de verzameling der negatieve reële getallen is de gewone vermenigvuldiging geen productoperatie.

4. Analoog aan de voorbeelden 1, 2, 3 heeft men : De additieve groepen van de rationale getallen en van de gehele getallen; de multiplicatieve groepen van de rationale getallen $\neq 0$ en van de positieve rationale getallen.

5. Voorbeeld 10.1.3. De vectoren uit een vectorruimte vormen met vectoroptelling als productoperatie een groep (zie WSK I).

De groepen in de voorbeelden 1 t/m 5 zijn abels.

6. G : alle een-eenduidige afbeeldingen van Rl op Rl

$\varphi((f,g)) = f \circ g$. Deze groep is niet abels.

6'. W : niet lege verzameling. G : alle 1-1 duidige afbeeldingen van W op W (deze verzameling noteren we als S(W)).

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

$(S(W), \circ)$ heet de permutatiegroep van de elementen van W.

Opgaven.

79. Bewijs dat de groep uit voorbeeld 6' dan en slechts dan abels is als W hoogstens 2 elementen bevat.

80. V is een oneindige verzameling. $(P(V), \div)$ is een commutatieve groep (zie opgave 76). Zij $W := \{U \in P(V) \mid U \text{ eindig}\}$.
Bewijs dat $(W, \div)$ een commutatieve groep is.

81. Voor deelverzamelingen X en Y van Rl definiëren we :

$$X \cdot Y := \{z \in Rl \mid \exists x \in X \; \exists y \in Y \; (z = xy)\}.$$

Is $(P(Rl), \cdot)$ een groep ?

82. Ga van de volgende verzamelingen na of ze met de gegeven productoperatie een groep vormen.

(a) $\{x + y\sqrt{2} \mid x \in Rt, y \in Rt\}$; gewone optelling.

(b) $\{x + y\sqrt{2} \mid x \in Rt, y \in Rt, x \neq 0 \neq y\}$; gewone vermenigvuldiging.

(c) $\{x \mid x^2 \in Rt, x \neq 0\}$; gewone vermenigvuldiging.

83. Bewijs, dat de monotoon toenemende continue functies f op $[0,1]$ met $f(0) = 0$ en $(1) = 1$ een groep vormen met functiesamenstelling als productoperatie.

84. In R1 definiëren we een productoperatie * door :

$$a * b = \sqrt[3]{a^3 + b^3} \qquad (a,b \in R1).$$

Bewijs dat (R1 *) een commutatieve groep is.

10.3. Stellingen.

Stelling 1. In een groep (G,) zijn de vergelijkingen $ax = b$ en $xa = b$ voor alle a en b éénduidig oplosbaar.

Bewijs. Het element $a^{-1}b$ is een oplossing van $ax = b$ want $a\,a^{-1}b = eb = b$. De vergelijking is dus oplosbaar. Zij c een oplossing, dus $ac = b$, dan is $a^{-1}\,ac = a^{-1}b$;maar $a^{-1}ac = ec = c$ dus $c = a^{-1}b$. $a^{-1}b$ is dus de enige oplossing. De vergelijking $xa = b$ heeft als enige oplossing ba^{-1}. q.e.d.

Stelling 2. In een groep (G,) volgt voor alle a uit $ax = ax'$ en eveneens uit $xa = x'a$ dat $x = x'$.

Bewijs. Gevolg van stelling 1.

Men kan de axioma's G2 en G3 nagenoeg vervangen door de eisen van éénduidige oplosbaarheid van de vergelijkingen $ax = b$ en $xa = b$. Men moet dan alleen nog er bij eisen dat G niet leeg is. Dit is de inhoud van stelling 3.

Stelling 3. Is (G,) een niet lege verzameling met een associatieve productoperatie waarvoor de vergelijkingen $ax = b$ en $xa = b$ voor alle $a, b \in G$ éénduidig oplosbaar zijn, dan is (G,) een groep.

Bewijs. We laten eerst zien dat er een eenheidselement in (G,) is. G is niet leeg, dus $a \in G$, $ax = a$ heeft nu één oplossing : e_a; $xa = a$ heeft één oplossing: e'_a. Nu geldt voor alle b: $e_a b = b$, anders waren $e_a b$ en b twee verschillende oplossingen van $ax = ab$. Dus $\forall b(e_a b = b)$;

evenzo $\forall c(c\, e'_a = c)$. Door het eerste resp. tweede resultaat voor e'_a resp. e_a te specialiseren vindt men

$$e_a\, e'_a = e'_a, \quad e_a\, e'_a = e_a, \text{ dus } e_a = e'_a.$$

We weten nu tevens dat e_a het eenheidselement is en noemen het e.
Het bestaan van inversen is nu eenvoudig. Neem $c \in G$; $cx = e$ is dan éénduidig oplosbaar; noem de oplossing d. Het enige dat men dan nog moet laten zien is dat ook $dc = e$. Nu is echter

$$dcd = d(cd) = de = d = ed.$$

Uit de éénduidige oplosbaarheid van $xd = d$ volgt nu dat $dc = e$. q.e.d.

Opgave.

85. $(G, \ )$ is een verzameling met een associatieve productoperatie. Er is in $(G, \ )$ een linkereenheidselement ℓ, en een rechtereenheidselement r, d.w.z. $\forall x \in G \ (\ell x = x)$ en $\forall x \in G \ (xr = x)$. Bewijs dat $(G, \ )$ één eenheidselement heeft.

10.4. Eindige groepen.

Definitie. Een groep $(G, \ )$ waarvan G een verzameling met eindig veel elementen is heet een eindige groep. Het aantal elementen van G heet de orde van de groep.

Voorbeelden.

1. De getallen +1 en -1 met gewone vermenigvuldiging vormen een groep van de orde 2.

2. Een groep met vier elementen krijgt men aldus : beschouw de reële functies f_1, f_2, f_3, f_4 op de reële getallen $\neq 0$ gedefinieerd door :

$$f_1(x) := x; \ f_2(x) := \frac{1}{x}; \ f_3(x) := -x; \ f_4(x) := -\frac{1}{x}.$$

f_1, f_2, f_3, f_4 zijn dus afbeeldingen van de verzameling der reële getallen $\neq 0$ op zichzelf. Met de samenstelling van afbeeldingen als productoperatie (dus $f_i \circ f_j)\ (x) := f_i(f_j(x)))$ vormen ze een groep van de orde 4.

Men ziet dat f_1 het eenheidselement is, en dat $f_i^{-1} = f_i$ $(i=1,2,3,4)$.

Voor de eindige groepen kan men zg. vermenigvuldigingstafels opstellen. Dit zijn schema's waarin men van alle producten de uitkomst geeft. Van de groepen uit voorbeeld 1 en voorbeeld 2 zijn de vermenigvuldigingstafels :

linkerfactor \ rechterfactor	+ 1	- 1
+ 1	+ 1	- 1
- 1	- 1	+ 1

linkerfactor \ rechterfactor	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Men ziet aan de vermenigvuldigingstafels dat beide groepen commutatief zijn.

Stelling. In de vermenigvuldigingstafel van een eindige groep staan in elke rij en elke kolom alle elementen van de groep één keer.

Bewijs. Gevolg van 10.3. stelling 2.

We bespreken nog enige voorbeelden van eindige groepen.

3. De gehele getallen mod m met de optelling gedefiniëerd in § 6.5 vormen een groep van de orde m, de zgn.optelgroep (additieve groep) der gehele getallen modulo m.

We geven de vermenigvuldigingstafel van de optelgroep van de gehele getallen mod 4. We noemen de representanten 0,1,2,3.

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

4. Is W een verzameling met n elementen dan is de groep $(S(W), \circ)$ (zie 10.2 voorbeeld 6') een groep met n! elementen.
Aan de hand van een voorbeeld introduceren we een notatie voor elementen van de permutatiegroep van een eindige verzameling. We nemen $W = \{1,2,3,4,5\}$.
Een element f van S(W) kan dan geschreven worden als :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ f(1) & f(2) & f(3) & f(4) & f(5) \end{pmatrix}$$

Zo betekent : $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$ dat

$f(1) = 3$, $f(2) = 1$, $f(3) = 4$, $f(4) = 5$, $f(5) = 2$.

Is $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$, dan is

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}, \quad g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}.$$

We stellen de vermenigvuldigingstafel op van de permutatiegroep van $\{1,2,3\}$.
De elementen van deze groep zijn :

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix};$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

De groep is niet commutatief.

Opgaven.

86. Bewijs dat de volgende afbeeldingen van $\mathbb{R} \setminus \{0,1\}$ in zichzelf een groep vormen met de samenstelling van afbeeldingen als productoperatie:

$f_1(x) := x$; $f_2(x) := \frac{1}{x}$; $f_3(x) := 1-x$; $f_4(x) := \frac{x}{x-1}$;

$f_5(x) := \frac{1}{1-x}$; $f_6(x) := \frac{x-1}{x}$.

Stel de vermenigvuldigingstafel van deze groep op.

87. Beschouw de gehele getallen mod 12. De klassen 1,5,7,11 vormen met de in § 6.5 ingevoerde vermenigvuldiging een groep van 4 elementen. Evenzo de klassen 1,5,8,12 mod 13.

Stel van beide groepen een vermenigvuldigingstafel op.

88. Stel de vermenigvuldigingstafel op van de optelgroep van de gehele getallen modulo 5.

10.5. Isomorfie. In de abstracte algebra interesseert men er zich niet voor wat het nu eigenlijk voor dingen zijn die als elementen van een groep optreden, slechts de door de productoperatie aangebrachte structuur is van belang. Vandaar dat een van de meest belangrijke begrippen uit de theorie zal aangeven dat twee groepen in dit opzicht hetzelfde zijn.

Definitie. De groepen $(G, .)$ en $(G^*, *)$ heten isomorf (notatie : $(G,.)\sim(G^*,*)$) indien er een 1-1 duidige afbeelding ϕ van G op G^* bestaat zó dat

$$\forall a\in G \quad \forall b\in G \; [\phi(a.b) = \phi(a) * \phi(b)].$$

Een afbeelding ϕ met deze eigenschap heet een isomorfisme.

Eigenschappen.

1. Isomorfie is een equivalentierelatie op de klasse van alle groepen.

2. Is ϕ een isomorfisme van $(G,.)$ op $(G^*,*)$ dan geldt :

   (a) $\phi(e) = e^*$ als e het eenheidselement van $(G,.)$; e^* dat van $(G^*,*)$ is.

   (b) $\forall a\in G \; [\phi(a^{-1}) = (\phi(a))^{-1}]$.

Bewijs 2(a). Voor alle a uit G geldt : $\phi(a) = \phi(a \,.\, e) = \phi(a) * \phi(e)$ en $\phi(a) = \phi(e \,.\, a) = \phi(e) * \phi(a)$. Omdat ϕ een afbeelding van G op G^* is betekent dit :

$$\forall a^*\in G^* \; [a^* * \phi(e) = \phi(e) * a^* = a^*].$$

Bewijs 2(b). Analoog aan het vorige bewijs, nu met de betrekking :

$$\phi(a^{-1}) * \phi(a) = \phi(a^{-1} \,.\, a) = \phi(e) = e^* = \phi(a \,.\, a^{-1}) = \phi(a) * \phi(a^{-1}).$$

q.e.d.

Voorbeelden van isomorfie.

1. De multiplicatieve groep van de positieve reële getallen is isomorf met de additieve groep der reële getallen. Om dit te bewijzen moet men een 1-1 afbeelding ϕ van de positieve reële getallen op alle reële getallen aangeven die zo is dat : $\phi(p_1p_2) = \phi(p_1) + \phi(p_2)$. Men gaat gemakkelijk na dat $\phi(x) := \log x$ de gewenste eigenschappen heeft.

2. Zij V een willekeurige verzameling. Op P(V) definiëert men de productoperatie $\cdot|\cdot$ door:

$$A \cdot|\cdot B := (A^* \cap B^*) \cup (A \cap B) \qquad (A,B \in P(V)).$$

Nu is $(P(V), \cdot|\cdot)$ een groep die isomorf is met $(P(V), \div)$.
$\psi(A) := A^*$ is een isomorfisme van $(P(V), \cdot|\cdot)$ op $(P(V), \div)$.

3. Zij φ een 1-1 duidige afbeelding van Rl op Rl.
Zij de productoperatie $*$ gedefinieerd door :

$$\forall x \in Rl \quad \forall y \in Rl \; [x * y := \varphi^{-1}(\varphi(x) + \varphi(y)].$$

Dan is (Rl, $*$) een groep, en φ is een isomorfisme van (Rl, $*$) op de additieve groep der reële getallen (Rl, +).

4. Is er een 1-1 duidige afbeelding g van V op W, dan zijn $(S(V), \circ)$ en $(S(W), \circ)$ isomorf. Als $G : S(V) \to S(W)$ gedefiniëerd is door :
$\forall f \in S(V) \; [G(f) := g \circ f \circ g^{-1}]$ dan is G een isomorfisme van $(S(V), \circ)$ op $(S(W), \circ)$.
Gevolg: de permutatiegroep van een verzameling van n elementen is isomorf met de permutatiegroep van $\{1,2,...,n\}$. Deze laatste heet symmetrische groep van n elementen (notatie: S_n).

Opgaven.

89. Bewijs dat de groep uit opgave 84 isomorf is met de additieve groep van de reële getallen.

90. Bewijs dat de groep uit opgave 86 isomorf is met S_3 i.e. de permutatiegroep van $\{1,2,3\}$ (§10.4 voorbeeld 4).

91. Men wil van de verzameling $\{e,a,b,c\}$ een groep maken door invoering van een productoperatie. Stel alle vermenigvuldigingstafels op die $\{e,a,b,c\}$ tot een groep maken met eenheidselement e. Hoeveel onderling

niet-isomorfe groepen kunt U maken ? Bewijs dat iedere groep van de orde 4 isomorf is met hetzij de optelgroep van de gehele getallen mod 4, hetzij de groep uit § 10.4 voorbeeld 2 (Viergroep van Klein).

92. Welk van de beide groepen uit opgave 87 is isomorf met de Viergroep van Klein, welke met de optelgroep der gehele getallen mod 4.

93. Is de optelgroep van de gehele getallen mod 6 isomorf met S_3 ?

94. (De nu volgende opgave vraagt behalve begrip van § 9 en § 10.5 precieze kennis van het begrip vectorruimte uit WSK I.)
Enig nadenken leert dat in iedere abstracte theorie een isomorfie-begrip een centrale plaats moet innemen. Zo definiëert men voor geordende verzamelingen : $(V,<)$ heet <u>(ordenings)isomorf</u> met $(V^*,\prec)$ indien er een 1-1 duidige afbeelding ϕ van V <u>op</u> V* bestaat zódanig dat

$$\forall a \in V \quad \forall b \in V \quad [(a<b) \Leftrightarrow (\phi(a) \prec \phi(b))].$$

Formuleer het isomorfiebegrip voor vectorruimten. Bewijs dat iedere vectorruimte met dimensie n isomorf is met R_n.

10.6. Ondergroepen.

Bij geordende verzamelingen $(V,<)$ is het zó dat de ordening $<$ iedere deelverzameling $W \subset V$ tot een geordende verzameling $(W,<)$ maakt. Dit is met groepen niet zo. Als nl. (G,) een groep is en $H \subset G$, H niet leeg, dan is (H,) niet steeds een groep. Neem bijv. voor (G,) de multiplicatieve groep der reële getallen $\neq 0$; H : de negatieve reële getallen. De beperking van het product tot H is geen afbeelding van $H \times H$ in H, wel van $H \times H$ in G. Neemt men de verzameling Nt der natuurlijke getallen als deelverzameling van G dan is het product wel een afbeelding van $Nt \times Nt$ in Nt; toch wordt Nt geen groep want er zijn geen inversen.

Stelling 1. Zij (G, .) een groep, H een niet lege deelverzameling van G dan is (H, .) dan en slechts dan zelf een groep indien

$$\forall h_1 \in H \ \ \forall h_2 \in H \,[h_1 \, . \, h_2 \in H] \qquad (i)$$

$$\forall h \in H \,[h^{-1} \in H] \qquad (ij).$$

Bewijs. Dat de voorwaarden (i) en (ij) nodig zijn is onmiddellijk duidelijk. We laten zien dat ze ook voldoende zijn. Uit (i) volgt dat de vermenigvuldiging een afbeelding van $H \times H$ in H is. Aan de associatieve wet is zeker voldaan, want dat is in G al zo. Daar H niet leeg is, is er een $h_0 \in H$. Uit (ij) volgt nu dat voor deze h_0 ook $h_0^{-1} \in H$. Nu is ook $h_0 \, . \, h_0^{-1} = e \in H$. (H, .) voldoet dus aan G2. Aan G3 is eveneens voldaan. q.e.d.

Definitie. Is (G, .) een groep, $H \subset G$, $H \neq \emptyset$ zó dat aan (i) en (ij) voldaan is, dat heet (H, .) ondergroep van (G, .).

Voorbeelden.

1. De multiplicatieve groep der positieve reële getallen is een ondergroep van de multiplicatieve groep der reële getallen $\neq 0$.

2. De additieve groep van de gehele getallen is een ondergroep van de additieve groep van de reële getallen.

Soms kan men om te bewijzen dat iets een ondergroep is, gebruik maken van de volgende stelling :

Stelling 2. Zij (G, .) een groep, H een niet lege deelverzameling van G, dan is (H, .) dan en slechts dan een ondergroep van (G, .) indien :

$$\forall h_1 \in H \ \forall h_2 \in H \,[h_1 \, . \, h_2^{-1} \in H] \qquad (iij).$$

Bewijs. Dat (iij) nodig is, is duidelijk. We zullen bewijzen dat (iij) voldoende is door te laten zien dat (i) en (ij) uit (iij) volgen.

Zij $h_0 \in H$ $(H \neq \emptyset!)$, dan is wegens (iij) $h_0 \cdot h_0^{-1} = e \in H$. Voor iedere $h \in H$ is dus $e \cdot h^{-1} = h^{-1} \in H$ (ij). Als $h_1 \in H$, $h_2 \in H$ dan is ook $h_2^{-1} \in H$ en $h_1 \cdot (h_2^{-1})^{-1} = h_1 \cdot h_2 \in H$. (i) q.e.d.

Het aangeven van alle ondergroepen van een gegeven groep behoort tot de belangrijkste taken van de groepentheorie (zie opgave 101).

Opgaven.

95. Zoek alle ondergroepen van :

(a) de optelgroep van de gehele getallen mod 4 ;

(b) de Viergroep van Klein ;

(c) S_3.

96. Een functie φ uit S(Rl) heet monotoon stijgend indien :

$$\forall x_1 \in \mathrm{Rl}\ \forall x_2 \in \mathrm{Rl}\ [(x_1 > x_2) \Rightarrow (\varphi(x_1) > \varphi(x_2))].$$

Bewijs dat de monotoon stijgende functies een ondergroep van $(S(\mathrm{Rl}), \circ)$ vormen.

97. Als $a \in W$; $A := \{f \mid f \in S(W),\ f(a) = a\}$, dan is $(A, \circ)$ een ondergroep van $(S(W), \circ)$.

98. Als $U \subset W$; $B := \{f \mid f \in S(W),\ f(U) = U\}$, dan is $(B, \circ)$ een ondergroep van $(S(W), \circ)$.

99. $(G,\ )$ en $(R, .)$ zijn groepen.

Op $G \times R$ definiëren we een productoperatie $*$ door :

$$(a,b) * (c,d) := (ac,\ b.d) \text{ voor alle } (a,b) \in G \times R,\ \ (c,d) \in G \times R.$$

(a) Bewijs dat $(G \times R, *)$ een groep is.

(b) Als $G_1 := \{(a,e) \mid a \in G,\ e \text{ eenheidselement van } (R, .)\}$, dan is $(G_1, *)$ een ondergroep van $(G \times R, *)$ die isomorf is met $(G,\ )$.

100. F zij de verzameling van alle afbeeldingen van Rl in Rl.

We definiëren een productoperatie $\oplus$ in F :

$(f \oplus g)(x) := f(x) + g(x), \quad (f \in F,\ g \in F,\ x \in Rl).$

(a) Bewijs dat $(F, \oplus)$ een groep is.

(b) Geef enige ondergroepen van $(F, \oplus)$ aan.

101. Bewijs de stelling van Cayley (1821 - 1895).

Iedere groep (G,) is isomorf met een ondergroep van de permutatie-groep $(S(G), \circ)$.

(Aanwijzing : beschouw bij $g \in G$; $\varphi_g \in S(G)$ gedefiniëerd door :

$\varphi_g(x) := gx \ (x \in G)$).