

1 Basisbegrippen

1.1 Verzamelingen. De getallen waarmee we op school hebben leren werken, zijn de *reële getallen*. De verzameling van alle reële getallen wordt aangeduid met $\mathbb{R}$. Belangrijke deelverzamelingen van $\mathbb{R}$ zijn $\mathbb{N}$, $\mathbb{Z}$ en $\mathbb{Q}$.

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is de verzameling van de *natuurlijke getallen*,

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ bevat de *gehele getallen* en

$\mathbb{Q} = \{x \in \mathbb{R} \mid x = m/n \text{ voor zekere gehele getallen } m \text{ en } n \text{ met } n \neq 0\}$ bevat de *rationale getallen*.

Een *verzameling* definiëren we door te omschrijven welke elementen tot de verzameling behoren. Zo'n omschrijving kan bijvoorbeeld bestaan uit een opsomming van de elementen. Opsommen kan alleen als er een eindig aantal elementen is of als er een zekere regelmaat in de opsomming zit en men de welwillende lezer door puntjes kan suggereren hoe de opsomming verder gaat. $V = \{0, 2, 4, 6, \dots\}$ bevat de even natuurlijke getallen en $W = \{0, 2, 4, 6, \dots, 82\}$ bevat de even natuurlijke getallen tot en met 82. Dat 8 tot V behoort, geven we aan met $8 \in V$, lees *8 is een element van V*. Dat 84 niet tot W behoort, geven we aan met $84 \notin W$, lees *'84 is niet een element van W'*. Verzameling W is een *deelverzameling* van V , notatie $W \subset V$. Ook $\mathbb{N} \subset \mathbb{Z}$ en $\mathbb{Z} \subset \mathbb{Q}$ en $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Twee verzamelingen V en W zijn *gelijk*, als V en W dezelfde elementen hebben. Dus als $V = \{x \in \mathbb{R} \mid x^2 = 4\}$ en $W = \{-2, 2\}$ dan $V = W$, ondanks de verschillende omschrijving. Noteren we een verzameling met een eindig aantal elementen d.m.v. opsomming, dan doet de volgorde er niet toe. Dus $\{1, 2, 3\}$ is dezelfde verzameling als $\{2, 3, 1\}$. Als een element meerdere keren genoemd wordt, doet het toch maar één keer mee. Dus $\{1, 1, 2\} = \{1, 2\}$.

Is V een verzameling, dan kunnen we een deelverzameling W van V definiëren d.m.v. $W = \{x \in V \mid \dots x \dots\}$ waarin achter de streep een eigenschap staat die een element x van V moet hebben om tot W te behoren. Zo kunnen we de verzameling van de positieve reële getallen $\mathbb{R}^+$ definiëren d.m.v. $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ en $\mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\}$ bevat de niet-negatieve reële getallen. Algemener definiëren we, als V een verzameling reële getallen is, de verzamelingen $V^+ = \{x \in V \mid x > 0\}$ en $V_0^+ = \{x \in V \mid x \geq 0\}$. Evenzo $V^- = \{x \in V \mid x < 0\}$ en $V_0^- = \{x \in V \mid x \leq 0\}$. $\langle a, b \rangle$ is het *open interval* $\{x \in \mathbb{R} \mid a < x < b\}$, $[a, b]$ is het *gesloten interval* $\{x \in \mathbb{R} \mid a \leq x \leq b\}$ en analoog de intervallen $\langle a, b]$ (*links open, rechts gesloten*) en $[a, b)$ (*links gesloten, rechts open*).

Nog een andere manier om een deelverzameling van $\mathbb{R}$ te beschrijven zien we in het volgende voorbeeld: $V = \{2x + 3 \mid x \in \langle 1, 6 \rangle\}$. Dit is een afkorting van

$V = \{y \in \mathbb{R} \mid y = 2x + 3 \text{ voor zekere } x \in \langle 1, 6 \rangle\}$. V is dus het interval $\langle 5, 15 \rangle$.

Als f een functie is en W een verzameling, dan definieert $V = \{f(x) \mid x \in W\}$ de verzameling functiewaarden die je krijgt als x de verzameling W doorloopt. (We nemen hierbij aan dat $f(x)$ bestaat voor iedere $x \in W$. Over functies straks meer.) ‘ $a \in V$, $b \in V$ en $c \in V$ ’ wordt afgekort tot ‘ $a, b, c \in V$ ’.

$\mathbb{Q} = \{x \in \mathbb{R} \mid x = k/m \text{ voor zekere gehele getallen } k \text{ en } m \text{ met } m \neq 0\}$ kunnen we korter schrijven als $\mathbb{Q} = \{k/m \mid k, m \in \mathbb{Z}, m \neq 0\}$ en $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ noteren we ook als $\mathbb{Z} = \{k - m \mid k, m \in \mathbb{N}\}$.

Als V en W verzamelingen zijn, dan is $V \cap W = \{x \mid x \in V \text{ en } x \in W\}$ de verzameling van de elementen, die zowel tot V als tot W behoren. $V \cap W$ heet de *doorsnede* van V en W . De *vereniging* $V \cup W = \{x \mid x \in V \text{ of } x \in W\}$ van V en W bevat de elementen die tot V of tot W (of tot beide) behoren.

$V \setminus W = \{x \mid x \in V \text{ en } x \notin W\}$ bevat de elementen van V die niet tot W behoren. Lees $V \setminus W$ als *V met daaruit weggelaten W*. $\mathbb{R} \setminus \{0, 3, 7\}$ bestaat bijvoorbeeld uit alle reële getallen behalve 0, 3 en 7. $\mathbb{R} \setminus \mathbb{Q}$ is de verzameling van de *irrationale* getallen met bijv. $\sqrt{3}$, π en e .

Als we willen dat $V \cap W$ altijd een verzameling oplevert, ook als V en W verzamelingen zijn die geen gemeenschappelijke elementen hebben, dan moeten we toelaten dat er een verzameling bestaat die geen elementen heeft. Deze *lege verzameling* wordt aangeduid met $\emptyset$. Als V en W geen gemeenschappelijke elementen hebben dan noemen we V en W *disjunct* en schrijven $V \cap W = \emptyset$. De lege verzameling wordt beschouwd als een deelverzameling van iedere verzameling, immers als V een willekeurige verzameling is dan is $\{x \in V \mid x \neq x\}$ een deelverzameling van V en $\{x \in V \mid x \neq x\} = \emptyset$.

Hier is nog een reden waarom de lege verzameling deelverzameling van V is:

$W \subset V$ betekent ‘ieder element van W zit ook in V ’ of, anders gezegd ‘er is geen element van W dat niet in V zit.’. Uit de laatste formulering blijkt dat $\emptyset \subset V$, want $\emptyset$ bevat geen enkel element en dus zeker geen element dat niet in V zit.

Als $V \cap W = \emptyset$ en $V \cup W = U$, dan zijn V en W elkaars *complement* binnen U .

De elementen van een verzameling hoeven niet beslist getallen te zijn, het kunnen ook personen of dingen zijn. Hier zullen we echter alleen maar verzamelingen beschouwen waarvan de elementen wiskundige objecten zijn. De elementen van een verzameling kunnen zelf op hun beurt ook weer verzamelingen zijn. Zo kunnen we bijvoorbeeld spreken over de verzameling van alle eindige deelverzamelingen van $\mathbb{N}$. Om de uitdrukking ‘verzameling van verzamelingen’ te vermijden spreken we in zo’n geval ook van een ‘*collectie* verzamelingen’. Voor een collectie verzamelingen gebruikt men graag een meer gekruld lettertype als $\mathcal{A}, \mathcal{B}$ of $\mathcal{C}$.

De collectie van alle deelverzamelingen van een verzameling V wordt de *machtsverzameling* van V genoemd en aangeduid met $\mathcal{P}(V)$. De $\mathcal{P}$ staat voor ‘powerset’ (Engels) of “Potenzmenge” (Duits).

Overigens wordt niet alles wat wij op één hoop wensen te vegen daarmee automatisch tot een verzameling, zoals de *paradox van Russell* aantoonst. Stel wij definiëren de ‘Russell-verzameling’ $\mathcal{R}$ als volgt: $\mathcal{R}$ is de verzameling die precies die verzamelingen bevat die zichzelf niet tot element hebben. Voor iedere verzameling X geldt dan: $X \in \mathcal{R}$ precies dan wanneer $X \notin X$. De vraag is nu: is $\mathcal{R}$ een element van zichzelf? Indien ja, dan zou dat volgens de definitie van $\mathcal{R}$ betekenen dat $\mathcal{R}$ niet een element van zichzelf is. Indien nee, dan zou volgens de definitie $\mathcal{R}$ juist wel een element van zichzelf zijn. Een tegenspraak. De aanname dat er een verzameling $\mathcal{R}$ bestaat die aan bovenstaande definitie voldoet leidt tot een tegenspraak. De conclusie is dan ook dat zo’n verzameling niet kan bestaan.

De begrippen doorsnede en vereniging zijn niet beperkt tot een eindig aantal verzamelingen. We kunnen ook de doorsnede en vereniging van een oneindig aantal verzamelingen nemen. Stel $\mathcal{C}$ is een niet lege collectie verzamelingen. Dan nemen we aan dat de vereniging van de verzamelingen in $\mathcal{C}$ weer een nieuwe verzameling V oplevert, ook als $\mathcal{C}$ oneindig veel verzamelingen bevat. Er geldt dan: $x \in V$ precies dan wanneer x tot minstens één verzameling $W \in \mathcal{C}$ behoort. Evenzo levert de doorsnede van de verzamelingen in $\mathcal{C}$ een nieuwe verzameling D op. Er geldt: $x \in D$ precies dan wanneer x tot iedere verzameling $W \in \mathcal{C}$ behoort. Als $\mathcal{C}$ slechts twee verzamelingen A en B bevat, dus als $\mathcal{C} = \{A, B\}$, dan komt deze definitie overeen met de eerder gegeven definitie van vereniging resp. doorsnede.

Voorbeeld. Stel $\mathcal{C} = \left\{ \left[\frac{1}{n+1}, \frac{1}{n} \right] \mid n = 1, 2, 3, \dots \right\} = \left\{ \left[\frac{1}{2}, 1 \right], \left[\frac{1}{3}, \frac{1}{2} \right], \left[\frac{1}{4}, \frac{1}{3} \right], \left[\frac{1}{5}, \frac{1}{4} \right], \dots \right\}$.

De vereniging van $\mathcal{C}$ is het interval $V = \langle 0, 1 \rangle$. Iedere $x \in \langle 0, 1 \rangle$ behoort tot minstens één interval uit $\mathcal{C}$ en omgekeerd: als x tot een interval in $\mathcal{C}$ behoort dan behoort x tot $\langle 0, 1 \rangle$. De doorsnede D van $\mathcal{C}$ daarentegen is de lege verzameling $\emptyset$, want geen enkel getal behoort tot ieder interval uit $\mathcal{C}$.

De vereniging van een collectie $\mathcal{C}$ van verzamelingen kunnen we noteren als $\bigcup \mathcal{C}$. (Spreek uit: ‘de vereniging van $\mathcal{C}$ ’). De doorsnede van een collectie $\mathcal{C}$ van verzamelingen kunnen we noteren als $\bigcap \mathcal{C}$ (spreek uit: ‘de doorsnede van $\mathcal{C}$ ’).

Als $\mathcal{C}$ een eindig aantal elementen heeft, bijvoorbeeld $\mathcal{C} = \{V_1, \dots, V_n\}$, dan:

$$\bigcup \mathcal{C} = \bigcup \{V_1, \dots, V_n\} = V_1 \cup \dots \cup V_n$$

en

$$\bigcap \mathcal{C} = \bigcap \{V_1, \dots, V_n\} = V_1 \cap \dots \cap V_n.$$

Belangrijke beweringen in de wiskunde worden geponeerd als *stellingen*. Het is de bedoeling dat we een stelling *bewijzen*. Bij een bewijs doen we een beroep op eerder bewezen stellingen. Het is duidelijk dat we niet tot in het oneindige terug kunnen gaan. Bepaalde beweringen zullen we zonder bewijs moeten accepteren. Deze beweringen noemen we de *axioma's*. Het is niet zo dat bepaalde beweringen van nature axioma's zijn. Een axioma in het ene systeem kan in het andere systeem een bewijsbare stelling zijn. Het is in elk geval een goede zaak om te proberen de basisveronderstellingen zo veel mogelijk expliciet te formuleren, al hoeft dat niet direct in het begin van een boek te gebeuren. Het is didactisch beter een min of meer verkennende start te maken. Analoge opmerkingen gelden m.b.t. definities. We kunnen niet alles definiëren, er blijven altijd ongedefinieerde begrippen. Zo'n begrip is bijv. het begrip 'verzameling'. We doen geen poging het begrip verzameling te definiëren.

Stellingen hebben vaak een "als .. dan..." vorm. Als A en B beweringen zijn, dan schrijven we vaak " $A \Rightarrow B$ " i.p.v. "Als A , dan B ". Om $A \Rightarrow B$ te bewijzen gaan we vaak als volgt te werk. We zeggen "stel dat A (waar is)". Vervolgens proberen we onder deze veronderstelling aan te tonen dat B (waar is). Lukt dat, dan concluderen we $A \Rightarrow B$. Het *omgekeerde* van $A \Rightarrow B$ is $B \Rightarrow A$. Als zowel $A \Rightarrow B$ als zijn omgekeerde $B \Rightarrow A$ gelden, dan schrijven we $A \Leftrightarrow B$. Spreek uit: " A precies dan, wanneer B " of " A dan en slechts dan als B " (Engels: "if and only if", vaak afgekort tot "iff"). Een bewering $A \Rightarrow B$ is gelijkwaardig met " $\text{niet-}B \Rightarrow \text{niet-}A$ ". Dus als we weten dat B niet waar is en er geldt $A \Rightarrow B$, dan kunnen we concluderen dat A niet waar is. Dit soort regels van de logica passen we dagelijks toe en zullen we niet expliciet formuleren. We redeneren volgens "het gezond verstand". In sommige wiskundeboeken zie je de afkortingen $A \wedge B$, $A \vee B$ en $\neg B$ voor " A en B ", " A of B " resp. " $\text{niet-}A$ ". Die zullen we hier niet gebruiken, de woordjes 'en', 'of' en 'niet' hebben geen afkorting nodig.

Een uitdrukking als ' A en $B \Rightarrow C$ ' kan betekenen ' $(A \text{ en } B) \Rightarrow C$ ' of ' A en $(B \Rightarrow C)$ '. Om haakjes te sparen spreken we af dat we ' A en $B \Rightarrow C$ ' indien mogelijk, interpreteren als ' $(A \text{ en } B) \Rightarrow C$ '. Evenzo: ' A of $B \Rightarrow C$ ' betekent ' $(A \text{ of } B) \Rightarrow C$ '. Idem voor 'niet- A '. M.a.w. 'en', 'of' en 'niet' worden eerder uitgevoerd dan $\Rightarrow$ (en $\Leftrightarrow$), net zoals bij het rekenen vermenigvuldigen en delen voorrang hebben boven optellen en aftrekken.

1.2 Geordende paren. De verzamelingen $\{a, b\}$ en $\{b, a\}$ zijn gelijk, het doet er niet toe in welke volgorde we de elementen van een verzameling opnoemen. Is de volgorde wel van belang dan spreken we van een *geordend paar* en schrijven (a, b) i.p.v. $\{a, b\}$. Er geldt: $(a, b) = (p, q) \Leftrightarrow a = p \text{ en } b = q$.

Als V en W verzamelingen zijn, dan is er een verzameling, die bestaat uit alle geordende paren (x, y) met $x \in V$ en $y \in W$. Deze verzameling wordt aangeduid met $V \times W$ en wordt de *productverzameling* van V en W genoemd:

$$V \times W = \{(x, y) \mid x \in V \text{ en } y \in W\}.$$

Voorbeeld. Stel $V = \{1, 2, 3, 4\}$ en $W = \{1, 2, 3\}$. Dan bevat $V \times W$ de 12 punten $(1, 1)$, $(1, 2)$, $(1, 3)$, $(2, 1)$, $(2, 2)$, $(2, 3)$, $(3, 1)$, $(3, 2)$, $(3, 3)$, $(4, 1)$, $(4, 2)$, $(4, 3)$. Merk op dat het aantal elementen van $V \times W$ gelijk is aan het product van de aantallen elementen van V en W .

Voorbeeld. $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$ is de verzameling van alle punten in het Oxy -vlak en de verzameling $C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 9\}$ bevat alle punten op de cirkel met middelpunt O en straal 3.

Voorbeeld. $[a, b] \times [c, d] = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid a \leq x \leq b \text{ en } c \leq y \leq d\}$ bevat alle punten van een rechthoekig gebied in het Oxy -vlak, als $a < b, c < d$.

1.3 Functies, afbeeldingen. Functies worden vaak gedefinieerd d.m.v. een vergelijking als $y = x^2 - 3x$ of $f(x) = \sqrt{x^2 - 3x}$. Als we een getal voor x invullen krijgen we de bijbehorende *functiewaarde* y resp. $f(x)$. Soms mogen we niet elk getal voor x invullen: de noemer van een breuk moet ongelijk 0 zijn, wat onder het wortelteken staat moet ≥ 0 zijn, wat achter het log-teken staat moet > 0 zijn, etc. De getallen die we voor x mogen nemen vormen het *domein* van de functie, de bijbehorende functiewaarden y vormen het *bereik*. Bij het definiëren van een functie kunnen we expliciet zeggen wat we als domein nemen. Is het domein niet aangegeven, dan wordt het domein zo groot mogelijk genomen. Bij iedere x uit het domein hoort precies één functiewaarde y .

Verschillende formules kunnen dezelfde functie definiëren. Twee functies f en g zijn gelijk als ze hetzelfde domein hebben en voor iedere x uit het domein geldt: $f(x) = g(x)$. Een functie f bepaalt een verzameling getallenparen (x, y) waarvoor geldt $y = f(x)$. Als bij de functies f en g dezelfde getallenparen (x, y) horen dan gaat het om één en dezelfde functie $f = g$. Door welke formule een functie gedefinieerd wordt doet er niet toe. Voor het bestaan een functie $y = f(x)$ is het zelfs niet nodig dat er een formule bestaat die y expliciet uitdrukt in x . Functie f is in feite niets anders dan een verzameling geordende paren en $y = f(x)$ betekent gewoon dat het paar (x, y) tot de functie f behoort. I.p.v. $y = f(x)$ zouden we ook kunnen schrijven $(x, y) \in f$. Niet iedere verzameling geordende paren is een functie, bij een x uit het domein van een functie hoort precies één y . Dus als (x, y_1) en (x, y_2) beide tot f behoren dan moet gelden $y_1 = y_2$.

Afhankelijk van de context komen we functies ook onder andere namen tegen. Zo wordt een functie wel een *afbeelding* genoemd. Men zegt dan bijvoorbeeld dat de functie $y = f(x) = x^2 + 2$ het interval $\langle -2, 3 \rangle$ *afbeeldt* op het interval $[2, 11]$. In deze terminologie wordt het getal dat men voor x invult het *origineel* genoemd en de bijbehorende functiewaarde $y = f(x)$ het *beeld*. In weer andere contexten gebruikt men de term ‘*transformatie*’ voor een functie, een functie transformeert in deze zienswijze het domein van de functie naar het bereik van de functie.

Originelen en beelden van een functie, afbeelding of transformatie hoeven niet beslist getallen te zijn, het mogen ook andere wiskundige objecten zijn.

Omdat een functie f een verzameling geordende paren is, kunnen we f op dezelfde manier als een verzameling definiëren. Een functie f met domein V en beelden in W definiëren we d.m.v. $f = \{(x, y) \in V \times W \mid \dots x \dots y \dots\}$, waarin $\dots x \dots y \dots$ een eigenschap voorstelt die garandeert dat bij iedere $x \in V$ precies één $y \in W$ bestaat zo dat $\dots x \dots y \dots$. Het bereik van f noteren we als $\text{Im}(f)$ ['Im' staat voor 'Image'] en het domein van f als $\text{Dom}(f)$.

Een andere manier om een functie te definiëren is de *pijljesnotatie*. Zo stelt $x \mapsto x^3 - 5x$ de functie voor die x afbeeldt op $x^3 - 5x$. Als we deze functie de naam f willen meegeven, dan noteren we dit als $f : x \mapsto x^3 - 5x$. De letters, die we gebruiken om een functie uit een algebraïsche uitdrukking te abstraheren, doen er niet toe, dezelfde functie f wordt gedefinieerd door $f : p \mapsto p^3 - 5p$. We kunnen er bij vermelden dat $\mathbb{R}$ het domein van f is, maar vaak moet het domein uit de context afgeleid worden.

Het domein van een functie kunnen we als volgt expliciet aangeven:

Met $f : V \rightarrow W$ bedoelen we een functie f met $\text{Dom}(f) = V$ en $\text{Im}(f) \subset W$.

[De pijl in $f : V \rightarrow W$ zonder dwarsstreepje.] We zeggen dan dat f de verzameling V *afbeeldt in* W . Het hoeft niet zo te zijn dat ieder element van W ook beeld is bij de afbeelding f . In $f : V \rightarrow W$ kan W iedere verzameling zijn die het bereik van f omvat. W is, in tegenstelling tot V , niet eenduidig door f bepaald.

Bovenstaande pijlnotaties kunnen we ook combineren, zoals in

$$f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^3 - 5x.$$

Als $f : V \rightarrow W$ en $A \subset V$, dan definiëren we $f(A) = \{f(x) \mid x \in A\}$. Dus $f(A)$ bevat alle beelden van de elementen van A en wordt *het beeld van A onder f* genoemd. De verzameling $f(A)$ is een deel van het bereik van f . Het bereik van f is $f(V)$.

Met nadruk moet gesteld worden dat de functie $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}$, met $f(x) = x^2$, niet dezelfde functie is als de functie $g : \mathbb{R} \rightarrow \mathbb{R}$, met $g(x) = x^2$. Twee functies zijn precies dan gelijk, als ze dezelfde geordende paren bevatten. Functie f is *de beperking* van g tot $\mathbb{R}_0^+$, omgekeerd is g *een uitbreiding* van f naar $\mathbb{R}$. Een gegeven functie kunnen we meestal op meerdere manieren uitbreiden, we spreken dus over 'de beperking' en over 'een uitbreiding'. Een uitbreiding kan wel uniek zijn, als we bepaalde eisen aan de uitbreiding stellen, bijv. continuïteit of differentieerbaarheid. Als we een functie f beperken of uitbreiden blijven we toch vaak dezelfde letter f gebruiken voor de beperking of de uitbreiding van f . We kunnen tenslotte niet steeds nieuwe symbolen blijven verzinnen en in de praktijk levert dit geen problemen op. Desnoods voegen we een extra symbooltje aan f toe, zoals in f^* , $f^\#$ of $\tilde{f}$, om f te onderscheiden van een beperking of uitbreiding. De officiële notatie voor de beperking van f tot A is $f|A$.

Als $f: V \rightarrow U$ en $g: U \rightarrow W$, dan kunnen we deze functies *samenstellen*: $x \in V$ wordt eerst door f op een element $y \in U$ afgebeeld en daarna wordt $y \in U$ weer door g op $z \in W$ afgebeeld. Dan $z = g(f(x))$.

We definiëren de *samengestelde functie* $h: V \rightarrow W$ waarvoor geldt $h(x) = g(f(x))$ voor iedere $x \in V$. We schrijven $h = g \circ f$, spreek uit als '*g na f*' of als '*f gevolgd door g*'.

We noemen $f: V \rightarrow W$ *een-op-een* of kortweg '1-1', als $f(x) = f(y) \Rightarrow x = y$ voor $x, y \in V$. Als $f(V) = W$, dan heet f een *afbeelding van V op W*.

Is $f: V \rightarrow W$ een 1-1-afbeelding, dan bestaat er een functie g die f omkeert. Bedoelde functie g met domein $\text{Im}(f)$ wordt gedefinieerd door $g(y) = x \Leftrightarrow f(x) = y$ of anders gezegd $(y, x) \in g \Leftrightarrow (x, y) \in f$. Deze functie g noemen we de *inverse* van f of de *omkeersfunctie* van f en we schrijven $g = f^{-1}$ [soms ook $g = f^{\text{inv}}$].

Is f een 1-1 afbeelding van V op W , dan is f^{-1} een 1-1-afbeelding van W op V en noemen we f ook een 1-1-*correspondentie* tussen V en W . In dat geval:

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x, \text{ voor iedere } x \in V.$$

$$(f \circ f^{-1})(y) = f(f^{-1}(y)) = y, \text{ voor iedere } y \in W.$$

De afbeelding $i: V \rightarrow V$ gedefinieerd door $i(x) = x$, noemen we de *identieke afbeelding* op V . Deze afbeelding wordt ook aangeduid met i_V of id_V . Is $f: V \rightarrow W$ een 1-1-afbeelding zo dat $f(V) = W$, dan geldt $f^{-1} \circ f = i_V$ en $f \circ f^{-1} = i_W$.

Voorbeeld. De functie $f: \mathbb{R} \rightarrow \mathbb{R}$ gedefinieerd door $f(x) = x^2$ is niet 1-1, want bijv. $y = 9$ is het beeld van zowel $x = 3$ als $x = -3$. De beperking van f tot het interval $[0, \rightarrow)$ is wel 1-1. Duiden we deze beperking van f ook aan met f (dat is in de wiskunde een gebruikelijke praktijk), dan is f wel 1-1 en de beeldverzameling is $[0, \rightarrow)$, $f^{-1}(x) = \sqrt{x}$ voor iedere x uit $[0, \rightarrow)$. Ga na dat $(f^{-1} \circ f)(x) = (f \circ f^{-1})(x) = \sqrt{x^2} = (\sqrt{x})^2 = x$, voor iedere $x \geq 0$.

Een 1-1 afbeelding f wordt ook *injectief* genoemd. Een afbeelding $f: V \rightarrow W$ met $f(V) = W$, wordt ook *surjectief* genoemd, maar daarbij moeten we wel bedenken dat de vraag of f wel of niet surjectief is niet alleen van f , maar ook van W afhangt. Eenzelfde afbeelding f kan surjectief m.b.t. W en niet surjectief m.b.t. $\tilde{W}$.

Is $f: V \rightarrow W$ injectief en surjectief (m.b.t. W), dan heet f *bijjectief* (m.b.t. W).

Bij een afbeelding $f: V \rightarrow W$ wordt een deelverzameling van V afgebeeld op een deelverzameling van W . Omgekeerd hoort bij iedere deelverzameling Y van W een deelverzameling X van V die de elementen van V bevat die op een element van Y afgebeeld worden. $X = \{x \in V \mid f(x) \in Y\}$. We noemen de verzameling X het *volledig origineel* van Y en schrijven $X = f^{-1}(Y)$, ook als f niet omkeerbaar is.

Het is mogelijk dat $f^{-1}(Y) = \emptyset$, neem bijv. $f: \mathbb{R} \rightarrow \mathbb{R}: x \mapsto x^2$ en neem voor Y een deelverzameling van $\mathbb{R}$ die uitsluitend negatieve getallen bevat.

1.4 Indexnotatie, rijen. Functies hebben binnen de wiskunde vele verschijningsvormen. Notatie en terminologie kunnen per toepassinggebied aanzienlijk verschillen. Zo gebruiken we bij een afbeelding waarvan de originelen natuurlijke of gehele getallen zijn vaak de ‘*indexnotatie*’ in plaats van de ‘*haakjesnotatie*’.

Voorbeeld. Bij $a: \mathbb{N}^+ \rightarrow A$, worden de beelden van 1, 2, 3, in de indexnotatie geschreven als $a_1, a_2, a_3, \dots$ in plaats van $a(1), a(2), a(3), \dots$. Deze laatste notatie heet de haakjesnotatie.

Voor een functie in indexnotatie gebruiken we, in plaats een letter die normaliter voor functies wordt gebruikt, bijv. ‘ f ’, ‘ g ’ of ‘ h ’, (dus een letter in de buurt van ‘ f ’), graag een letter die normaliter voor de elementen van A gebruikt wordt. In dit geval de letter ‘ a ’. Waren de elementen van A bijvoorbeeld verzamelingen geweest, dan hadden we misschien de letter V gebruikt. Bij V hadden we dan de beelden van 1, 2, 3, geschreven als $V_1, V_2, V_3, \dots$.

Vanwege het feit dat ieder natuurlijk getal n een *directe opvolger* $n+1$ heeft kunnen we bij een afbeelding $x: \mathbb{N}^+ \rightarrow \mathbb{R}$ de beelden van 1, 2, 3, in de indexnotatie opschrijven als een rij $x_1, x_2, x_3, \dots$. De afbeelding hebben we met de letter ‘ x ’ aangeduid, een letter die we anders meestal voor getallen gebruiken. Dit suggereert dat de beelden $x_1, x_2, x_3, \dots$ reële getallen zijn en dat is juist de bedoeling.

Definitie. Een *oneindige rij* in V is een functie $a: \mathbb{N}^+ \rightarrow V$. We schrijven de oneindige rij $a: \mathbb{N}^+ \rightarrow V$ als $(a_1, a_2, a_3, \dots)$ en ook vaak zonder haakjes als $a_1, a_2, a_3, \dots$. We noemen het domein $\mathbb{N}^+$ de *indexverzameling* van de rij. We noemen a_1 het eerste element van de rij, a_2 het tweede element, etc. In ruimere zin spreken we ook van een oneindige rij als de indexverzameling niet $\mathbb{N}^+$, maar bijv. $\mathbb{N}$, $\{-3, -2, -1, 0, 1, 2, 3, \dots\}$ of een andere verzameling $\{x \in \mathbb{Z} \mid k \leq x\}$ is. De *beginindex* is dan 0, -3 resp. k .

Eenzelfde getal c kan meerdere keren in de rij voorkomen, d.w.z. er kunnen meerdere indices n zijn zo dat $a_n = c$. Het is best mogelijk dat het bereik $\{a_1, a_2, a_3, \dots\}$ van de oneindige rij $(a_1, a_2, a_3, \dots)$ slechts een eindig aantal elementen bevat. Zo bevat het bereik van de rij $(0, 1, 0, 1, 0, 1, \dots)$ slechts twee getallen, namelijk 0 en 1.

Definitie. Onder een *eindige rij* in V met lengte n verstaan we een functie $a: \{1, 2, 3, \dots, n\} \rightarrow V$, in indexnotatie geschreven als $(a_1, a_2, a_3, \dots, a_n)$ of zonder haakjes als $a_1, a_2, a_3, \dots, a_n$. In ruimere zin spreken we ook van een eindige rij als $\{x \in \mathbb{Z} \mid k \leq x \leq m\}$ de indexverzameling is, de lengte van zo'n rij is dan $m - k + 1$ ($k, m \in \mathbb{Z}, m \geq k$). De lengte van een eindige rij wordt gedefinieerd als het aantal elementen van zijn indexverzameling.

Een rij in $\mathbb{R}$ noemen we een rij reële getallen, een rij in $\mathbb{Q}$ noemen we een rij rationale getallen. Als de elementen van V verzamelingen of functies zijn, dan spreken we van een rij verzamelingen resp. een rij functies, etc.

Er geldt: $(a_1, \dots, a_n) = (b_1, \dots, b_n) \Leftrightarrow a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$.

Vanwege deze eigenschap gebruiken we eindige rijtjes als *geordende n -tallen*. We definiëren $\mathbb{R}^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{R}\}$, m.a.w. $\mathbb{R}^n$ is de verzameling die bestaat uit alle rijtjes reële getallen met lengte n .

Algemener: $A^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in A\}$, als A een willekeurige verzameling is.

Is $a_1, \dots, a_n$ een rij getallen dan noteren we de som van deze rij als $a_1 + \dots + a_n$ en ook korter als $\sum_{k=1}^n a_k$. Op soortgelijke wijze noteren we product van deze rij getallen als

$\prod_{k=1}^n a_k$, maar meestal gewoon als $a_1 \cdot \dots \cdot a_n$

Opmerking. In uitdrukkingen als $\sum_{k=1}^n a_k$ of $\prod_{k=1}^n a_k$ mogen we voor de *indexvariabele* k net zo goed een andere letter gebruiken mits die niet in conflict komt met andere variabelen in de formule. Zo mogen we in $\sum_{k=1}^3 x^k$ de letter k niet vervangen door de letter x , maar wel door i of j .

Voorbeeld. In $\prod_{k=1}^n a_k$ hoeft de waarde van a_k niet van k af te hangen. Als $a_k = x$ voor

iedere $k \in \{1, 2, \dots, n\}$, dan schrijven we $\prod_{k=1}^n a_k = \underbrace{x \cdot x \cdot x \cdot \dots \cdot x}_n$ als x^n .

Voorbeeld. Nemen we voor a de rij $1, 2, 3, \dots, n$, dan is het product van de rij gelijk $1 \cdot 2 \cdot 3 \cdot \dots \cdot n = n!$ (*n -faculteit*)

De indexnotatie is niet alleen bij eindige of oneindige rijen handig, hij komt ook in andere situaties van pas.

Voorbeeld. Stel $V : A \rightarrow B$ is een afbeelding, waarbij de elementen van B verzamelingen zijn. Voor V gebruiken we de indexnotatie, zodat V_x voor iedere $x \in A$ een verzameling is. Het bereik van V is dan $\{V_x \mid x \in A\}$. Het domein A van V noemen we de indexverzameling. Voor de vereniging $\bigcup \{V_x \mid x \in A\}$ schrijven we in zo'n geval ook $\bigcup_{x \in A} V_x$. Evenzo schrijven we $\bigcap_{x \in A} V_x$ voor de doorsnede $\bigcap \{V_x \mid x \in A\}$.

Als $A = \{1, 2, \dots, n\}$, dan schrijven we $\bigcup_{x \in A} V_x$ en $\bigcap_{x \in A} V_x$ behalve als $V_1 \cup V_2 \cup \dots \cup V_n$

resp. $V_1 \cap V_2 \cap \dots \cap V_n$ ook als $\bigcup_{k=1}^n V_k$ resp. $\bigcap_{k=1}^n V_k$.

Nog enkele definities: Een functie $f : V \rightarrow W$, waarbij de elementen van V en W geordend zijn van klein naar groot, heet *stijgend op V* als $x \leq y \Rightarrow f(x) \leq f(y)$, voor iedere $x, y \in V$. Anders dan op school wordt 'stijgend' hier in zwakke zin gebruikt en betekent eigenlijk 'stijgend of gelijkblijvend'. Als $x < y \Rightarrow f(x) < f(y)$, voor iedere $x, y \in V$, dan noemen we f *strikt stijgend op V* . Op analoge wijze definiëren we '*dalend op V* ' resp. '*strikt dalend op V* '. Stijgende en dalende functies vormen samen de *monotone functies*. De *identieke functie* op een verzameling V is de functie die ieder element van V op zichzelf afbeeldt. Een functie f wordt *constant op V* genoemd, als f alle elementen van V op eenzelfde element in het bereik van f afbeeldt.

Een rij $(a_1, a_2, a_3, \dots)$ noteren we ook als $(a_n \mid n \in \mathbb{N}^+)$. Een eindige rij $(a_1, a_2, \dots, a_n)$ kunnen we noteren als $(a_k \mid k = 1, 2, \dots, n)$.

Deze notatie is handig als we de rij a willen definiëren met behulp van een formule voor a_n , zoals in $a = (1/n \mid n \in \mathbb{N}^+) = (1, \frac{1}{2}, \frac{1}{3}, \dots)$. Een rij is een functie en het bereik van deze functie noteren we op de gebruikelijke wijze met accolades i.p.v. haakjes als $\{a_n \mid n \in \mathbb{N}^+\} = \{a_1, a_2, a_3, \dots\}$ resp. $\{a_k \mid k = 1, 2, \dots, n\} = \{a_1, a_2, \dots, a_n\}$.

De notatie $\{a_1, a_2, a_3, \dots\}$ of $\{a_1, a_2, \dots, a_n\}$ impliceert uiteraard niet dat $a_1, a_2, a_3, \dots$ resp. $a_1, a_2, \dots, a_n$ allemaal verschillend zijn, $\{a_1, a_2, \dots, a_n\}$ kan minder dan n elementen bevatten. We passen deze handige notatie ook toe bij andere functies dan rijen. We gebruiken bijv. $f = (x^2 \mid x \in \mathbb{R}^+)$ als handig alternatief voor $f : \mathbb{R}^+ \rightarrow \mathbb{R} : x \mapsto x^2$. In $f = (x^2 \mid x \in \mathbb{R}^+)$ wordt het domein expliciet genoemd, het bereik is $\text{Im}(f) = f(\mathbb{R}^+) = \{x^2 \mid x \in \mathbb{R}^+\}$.

Zijn $f, g : V \rightarrow \mathbb{R}$ functies met gemeenschappelijk domein V en functiewaarden in $\mathbb{R}$ en is c een reëel getal, dan definiëren we de functies $c \cdot f$, $f \pm g$, $f \cdot g$ d.m.v.

$c \cdot f = (c \cdot f(x) \mid x \in V)$, $f \pm g = (f(x) \pm g(x) \mid x \in V)$ resp.

$f \cdot g = (f(x) \cdot g(x) \mid x \in V)$. Als $g(x) \neq 0$ voor iedere $x \in V$, dan

$f / g = (f(x) / g(x) \mid x \in V)$.

Een rij is een speciaal soort functie, dus deze definities gelden i.h.b. voor rijen. Zijn a en b rijen met indexverzameling $\mathbb{N}^+$, dan is bijv. $a + b$ de rij $a_1 + b_1, a_2 + b_2, a_3 + b_3, \dots$.

In sommige contexten is met f^{-1} de functie $1/f$ bedoeld, in andere contexten is f^{-1} de omkeersfunctie van f . Een soortgelijke opmerking geldt t.a.v. f^2 . Is $f: V \rightarrow \mathbb{R}$ een functie die reële getallen als functiewaarden heeft dan kan met f^2 de functie $f \cdot f$ bedoeld zijn, zoals hierboven gedefinieerd. Vergelijk bijv. $\sin^2 x$, dit betekent $(\sin x)^2$. Maar is f een functie $f: V \rightarrow V$, dan kan f^2 ook staan voor $f \circ f$ en dan betekent $f^2(x)$ hetzelfde als $f(f(x))$. Altijd even opletten wat bedoeld is.

1.5 De lege verzameling nader bekeken.

De lege verzameling verdient onze speciale aandacht.

Een verzameling als $\{a\}$ die maar één element bevat is een ander object dan dat element a . I.h.b. bevat $\{\emptyset\}$ één element, maar $\emptyset$ bevat geen element. Merk op dat $\emptyset$ zowel element als deelverzameling van $\{\emptyset\}$ is.

$\emptyset$ is deelverzameling van iedere verzameling V . Een van de redenen is dat we $\emptyset$ kunnen definiëren als $\{x \in V \mid x \neq x\}$. Een andere reden is dat $W \subset V$ betekent: ieder element van W hoort ook tot V , dus ‘ W is niet een deelverzameling van V ’ houdt in: er is een element in W dat niet in V zit. Op grond hiervan geldt: $\emptyset \subset V$, immers er is niet een element van $\emptyset$ dat niet tot V behoort.

Als we willen aantonen dat een bepaalde eigenschap _____ niet voor alle elementen van een verzameling V geldt, dan moeten we laten zien dat er een element van V is dat deze eigenschap niet heeft. Zo’n element is dan een *tegenvoorbeeld* voor de bewering “voor iedere $x \in V$ geldt _____”. Is er niet zo’n tegenvoorbeeld, dan heeft ieder element van V de bedoelde eigenschap. Omdat $\emptyset$ leeg is, is er in $\emptyset$ nooit een tegenvoorbeeld te vinden. Gevolg:

“Voor iedere $x \in \emptyset$ geldt _____” is altijd waar, wat we ook over x beweren!

“Voor iedere $x \in \emptyset$ geldt: $x \in V$ ” is waar omdat er geen tegenvoorbeeld is. Dus $\emptyset \subset V$.

Nu bekijken we de bewering “ $\emptyset$ is een functie”. Waar of niet waar? Je vermoedt het al: dat is waar! Wat is namelijk een functie? De eerste eis is dat een functie een verzameling geordende paren is. Kun je in $\emptyset$ een element aanwijzen dat niet een geordend paar is? Nee, dus $\emptyset$ is in elk geval een verzameling geordende paren. Verder moet bij een functie f gelden: $(x, y), (x, z) \in f \Rightarrow y = z$. Dit klopt bij $f = \emptyset$, wijs maar eens een tegenvoorbeeld aan! Dus $\emptyset$ is inderdaad een functie. Het domein van $\emptyset$ is $\emptyset$. Ook het beeld is leeg: $\emptyset(\emptyset) = \emptyset$. Is V een willekeurige verzameling dan $\emptyset: \emptyset \rightarrow V$. Ga na dat $\emptyset: \emptyset \rightarrow V$ zelfs injectief is.

Is $\emptyset$ een rij? We hadden een eindige rij $a_1, a_2, \dots, a_n$ in A gedefinieerd als een afbeelding $a: \{1, \dots, n\} \rightarrow A$ en we schreven de beelden $a(1), a(2), \dots, a(n)$ in indexnotatie als $a_1, a_2, \dots, a_n$. Stilzwijgend veronderstelden we hierbij dat $n \geq 1$. Het blijkt nu in het vervolg wel handig om $\{1, \dots, n\}$ te interpreteren als de lege verzameling als $n = 0$. Dit maakt vaak simpeler formuleringen mogelijk, omdat we het geval $n = 0$ dan niet meer apart hoeven te noemen. We noemen $a_1, a_2, \dots, a_n$ een rij met lengte n , waarbij n voortaan ook 0 mag zijn. Dus de rij met lengte 0 is de rij $\emptyset$, de lege rij!

Algemener interpreteren we $\{k, \dots, p\}$ als $\emptyset$, wanneer $k, p \in \mathbb{Z}$ en $p < k$.

Voorbeeld. $\mathbb{R}^n$ bestaat uit rijtjes $(x_1, x_2, \dots, x_n)$. $\mathbb{R}^0$ bevat de rijen met lengte 0. Daar is er maar één van, namelijk $\emptyset$. Dus $\mathbb{R}^0 = \{\emptyset\}$ en bevat 1 element.

Definitie. We noemen een verzameling A *eindig*, als er een rij $a_1, a_2, \dots, a_n$ is waarin ieder element van A precies één keer voorkomt. We zeggen dan dat A n elementen bevat. Het aantal elementen van A geven we aan met $\#(A)$. Hier dus $\#(A) = n$. Ga na dit ook nog klopt als $n = 0$.

Voorbeeld. Als $a_1, a_2, \dots, a_n$ een rij reële getallen is, hoe moeten we $a_1 + a_2 + \dots + a_n$ interpreteren als $n = 0$? Dit is een som met 0 termen. Tellen we $a_1 + a_2 + \dots + a_n$ en $b_1 + b_2 + \dots + b_p$ dan krijgen een som van $n + p$ termen. Als $n = 0$, dan is $a_1 + a_2 + \dots + a_n + b_1 + b_2 + \dots + b_p$ een som van $n + p = 0 + p = p$ termen. Het ligt dus voor de hand dat dan $a_1 + a_2 + \dots + a_n + b_1 + b_2 + \dots + b_p = b_1 + b_2 + \dots + b_p$, waaruit volgt dat $a_1 + a_2 + \dots + a_n = 0$. Idem voor het product $a_1 \cdot a_2 \cdot \dots \cdot a_n$. Als $n = 0$, dan is $a_1 \cdot a_2 \cdot \dots \cdot a_n \cdot b_1 \cdot b_2 \cdot \dots \cdot b_p$ een product van $n + p = 0 + p = p$ factoren, dus $a_1 \cdot a_2 \cdot \dots \cdot a_n \cdot b_1 \cdot b_2 \cdot \dots \cdot b_p = b_1 \cdot b_2 \cdot \dots \cdot b_p$ en $a_1 \cdot a_2 \cdot \dots \cdot a_n = 1$.

1.6 Bewerkingen. Optellen en vermenigvuldigen van reële getallen zijn bewerkingen in $\mathbb{R}$. Bij deze bewerkingen wordt als het ware uit twee getallen een nieuw getal geproduceerd. Wiskundig gezien zijn zulke bewerkingen niets anders dan afbeeldingen van $\mathbb{R} \times \mathbb{R}$ in $\mathbb{R}$. Algemener definiëren we een *bewerking* (op tweetallen) in A als een afbeelding $f: A \times A \rightarrow A$ en een bewerking op n -tallen in A als een afbeelding $f: A^n \rightarrow A$. A^1 wordt meestal geïdentificeerd met A en een bewerking op 1-tallen in A wordt dan ook als een afbeelding $f: A \rightarrow A$ beschouwd. [Voor de scherpslijpers onder ons: De elementen van A^1 zijn rijtjes (a) met $a \in A$ en $(a) = \{(1, a)\}$. Eigenlijk zouden we onderscheid moeten maken tussen een geordend paar (x, y) en de rij (x, y) met lengte 2. De rij (x, y) is de verzameling $\{(1, x), (2, y)\}$. Het is in de wiskunde echter gebruikelijk om het geordend paar (x, y) en de rij (x, y) te *identificeren*, d.w.z. als hetzelfde te beschouwen.] We beperken ons tot bewerkingen op tweetallen en hier volgt wat terminologie die op dit soort bewerkingen betrekking heeft.

Stel $f: A \times A \rightarrow A$ is een bewerking op A . We gebruiken voor f de *infixnotatie* en schrijven $x * y = z$ i.p.v. $f(x, y) = z$. We noemen f (of $*$) *associatief* als $x * (y * z) = (x * y) * z$ voor iedere $x, y, z \in A$ en we kunnen dan de haakjes net zo goed weglaten. De bewerking wordt *commutatief* genoemd, als de volgorde er niet toe doet: $x * y = y * x$ voor iedere $x, y \in A$.

Een element $n \in A$ wordt een *neutraal element* van f genoemd als $n * x = x * n = x$ voor iedere $x \in A$, f kan hoogstens één neutraal element hebben en we spreken dan van *het* neutrale element van f . Als n_1 en n_2 neutrale elementen van f zijn, dan $n_1 = n_1 * n_2 = n_2$. Zo is bijv. 0 het neutrale element bij het optellen en 1 het neutrale element bij het vermenigvuldigen van reële getallen.

Is n het neutrale element van bewerking f en zijn x en y elementen van A zo dat $x * y = y * x = n$, dan noemen we x en y elkaars *inverse* m.b.t. f . Zo zijn $-x$ en x elkaars inverse bij de optelling en zijn x en $\frac{1}{x}$ ($x \neq 0$) elkaars inverse bij de vermenigvuldiging van reële getallen.

Opmerking. Is f commutatief, dan hoeven we i.p.v. $n * x = x * n = x$ alleen maar $n * x = x$ te eisen opdat n neutraal element van f is. Ook volstaat dan $x * y = n$ om er voor te zorgen dat x en y elkaars inverse zijn.

In $\mathbb{R}$ treden de optelling en de vermenigvuldiging naast elkaar op en geldt $x \cdot (y + z) = x \cdot y + x \cdot z$, voor iedere $x, y, z \in \mathbb{R}$. We zeggen dat vermenigvuldigen in $\mathbb{R}$ *distributief* is over de optelling. Algemener: is $g: A \times A \rightarrow A$ een bewerking in A naast f en schrijven we $g(x, y) = z$ in de infixnotatie als $x \square y = z$, dan zeggen we dat f *distributief* is over g als voor iedere $x, y, z \in A$

$$x * (y \square z) = (x * y) \square (x * z) \quad \text{en ook} \quad (x \square y) * z = (x * z) \square (y * z).$$

(Is $*$ commutatief, dan is één van beide voorwaarden voldoende.)

Voorbeeld. Bewerkingen hoeven niet beslist betrekking te hebben op getallen. Stel P_n is de verzameling die bestaat uit alle 1-1-afbeeldingen van $V_n = \{1, \dots, n\}$ op zichzelf, de elementen van P_n zijn de *permutaties* van V_n . Een permutatie $p \in P_n$ is een eindig rijtje $p_1, \dots, p_n$ waarin ieder element van $V_n = \{1, \dots, n\}$ precies één keer voor komt. De bewerking in P_n die we beschouwen is het samenstellen van afbeeldingen. Als $p, q \in P_n$, dan ook $q \circ p \in P_n$. Deze bewerking is associatief, maar niet commutatief (geef een voorbeeld). Het neutrale element is de identieke afbeelding i , die ieder element van $\{1, \dots, n\}$ op zichzelf afbeeldt. De afbeeldingen in P_n zijn omkeerbaar: bij iedere $p \in P_n$ bestaat een $q \in P_n$ zo dat $q \circ p = p \circ q = i$. Dan $q = p^{-1}$ de inverse van p en $p = q^{-1}$ de inverse van q m.b.t. het samenstellen van afbeeldingen. Het aantal elementen van P_n is gelijk aan $n!$ (*n-faculteit*).

Definitie. Is $*$ een bewerking in A , dan noemen we een deelverzameling B van A *gesloten* m.b.t. deze bewerking als $x, y \in B \Rightarrow x * y \in B$. Zo is $\mathbb{N}$ een deelverzameling van $\mathbb{R}$ die gesloten m.b.t. optellen en vermenigvuldigen, maar niet m.b.t. aftrekken. De even gehele getallen vormen een deelverzameling van $\mathbb{Z}$, die gesloten is m.b.t. optellen, aftrekken en vermenigvuldigen. $\mathbb{Q}^+$ is gesloten m.b.t. optellen, vermenigvuldigen en delen.

1.7 Groep.

Definitie. Is A een verzameling, $*$ een associatieve bewerking in A met neutraal element n , waarin bij iedere $x \in A$ een inverse $y \in A$ bestaat, dan heet de combinatie $(A, *)$ een *groep*.

Eenzelfde verzameling A kan m.b.t. een bewerking $*$ een groep zijn en m.b.t. een andere bewerking $\square$ geen groep, bij een groep gaat het dus uitdrukkelijk om het paar $(A, *)$.

Iedere x in een groep $(A, *)$ heeft precies één inverse. Stel namelijk dat $x * y_1 = y_1 * x = n$ en ook $x * y_2 = y_2 * x = n$. Dan $y_1 * x * y_2 = y_1 * n = y_1$ en ook $y_1 * x * y_2 = n * y_2 = y_2$, dus $y_1 = y_2$. De haakjes hebben we weggelaten want $*$ is associatief. Duiden we de inverse van x aan met x^- , dan

$$\boxed{x^- * x = x^- * x = n}.$$

Is $(A, *)$ een groep en $*$ commutatief, dan noemen we $(A, *)$ een *commutatieve groep* of *abelse groep*.

In een groep $(A, *)$ gelden de ‘*schrapregels*’

$$\boxed{a * x = a * y \Rightarrow x = y} \text{ en } \boxed{x * a = y * a \Rightarrow x = y}.$$

Uit $a * x = a * y$ volgt namelijk $a^- * a * x = a^- * a * y$, dus $n * x = n * y$ ofwel $x = y$ en analoog voor de andere schrapregel.

In een groep $(A, *)$ gelden m.b.t. de inverse de regels

$$\boxed{(x^-)^- = x \text{ en } (x * y)^- = y^- * x^-}.$$

Dit tonen we aan met behulp van de schrapregels: $(x^-)^- * x^- = n_A$ en ook $x * x^- = n_A$, dus $(x^-)^- = x$. Soortgelijk: $(x * y)^- * (x * y) = n_A$ en ook $(y^- * x^-) * (x * y) = y^- * x^- * x * y = y^- * n_A * y = y^- * y = n_A$, dus $(x * y)^- = y^- * x^-$.

In $(\mathbb{R}, +)$ komen we deze regels tegen als $a + x = a + y \Rightarrow x = y$, $-(-x) = x$ en $-(x + y) = -x - y$. Dit laatste is gelijk aan $-x + -y$, omdat optellen in $(\mathbb{R}, +)$ commutatief is. Ook $(\mathbb{R} \setminus \{0\}, \cdot)$ is een commutatieve groep, dus daar krijgen we $a \cdot x = a \cdot y \Rightarrow x = y$, $(x^{-1})^{-1} = x$ en $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1} = x^{-1} \cdot y^{-1}$.