Voorwoord

De wiskundige vorming die in de wiskundig sterke richtingen van het Vlaamse secundair onderwijs wordt aangeboden, vormt een zeer degelijke basis voor hogere studies in wetenschappelijke, technologische en wiskundige richtingen.

Toch blijkt de aansluiting tussen het secundair onderwijs (SO) en het hoger onderwijs (HO) niet eenvoudig, zeker als het op wiskunde aankomt. Enerzijds hebben in de leerplannen bepaalde onderwerpen (denk aan deelbaarheid, determinanten, verzamelingenleer, projectieve meetkunde ...) plaats geruimd voor nieuwe inhouden (probleemoplossende vaardigheden, onderzoekscompetenties, kansrekenen, statistiek ...). Anderzijds worden er tussen het secundair en het hoger onderwijs ook grote vormelijke verschillen vastgesteld, verschillen in de manier van wiskunde aanbrengen, opbouwen, presenteren. Vandaar dat vaak over de SOHO-*problematiek* wordt gesproken.

Vanuit beide onderwijsniveaus worden steeds meer constructieve inspanningen geleverd om de SOHO-uitdaging aan te gaan. Leerkrachten maken dankbaar gebruik van de vrije ruimte om in richtingen met zeven of acht lesuren wiskunde extra onderwerpen aan te bieden en een meer rigoureuze opbouw te hanteren dan in een gemiddelde zesuursklas gebruikelijk is. Ook in het hoger onderwijs werden al heel wat initiatieven in het leven geroepen, zowel voor laatstejaarsleerlingen als voor eerstejaarsstudenten.

Met de reeks SOHO Wiskunde Plantyn hopen we hierin ook een rol te spelen. We willen leerlingen van de derde graad met minstens zes lesuren wiskunde kennis laten maken met zowel inhoudelijke als vormelijke aspecten van wiskunde die in het hoger academisch onderwijs meer aandacht krijgen dan in het secundair. Ook voor studenten van een professionele bachelor wiskunde kan deze reeks een interessante kennismaking met meer academische wiskunde vormen.

SOHO Wiskunde Plantyn biedt een kant-en-klaar geheel aan, dat zowel als lessenreeks als voor begeleide zelfstudie gebruikt kan worden.

De boekjes uit deze reeks worden geschreven door veranderlijke teams, waarin leerkrachten SO met wiskundigen van een universiteit samenwerken. Daardoor kunnen we een academische stijl en inhoud combineren met een correct instapniveau, met aandacht voor de voorkennis van leerlingen en de nodige duiding.

Met elke titel binnen SOHO Wiskunde Plantyn willen we leerlingen, studenten, leerkrachten en docenten een excursie in de wondere wereld van de wiskunde aanreiken, wellicht langs nieuwe paden, soms over steile heuvels, maar telkens met nieuwe ervaringen en mooie vergezichten. Deze kennismakingen vinden hun vervolg in menige academische cursus, in opleidingen wiskunde en daarbuiten.

We wensen iedereen een leerrijke ervaring met dit boekje.

Inleiding

De groepentheorie, een belangrijk domein binnen de zuivere wiskunde, speelt niet alleen een belangrijke rol binnen de wiskunde zelf, maar kent ook veel toepassingen in andere exacte wetenschappen zoals fysica, chemie en informatica.

In de wiskundige beschrijving van heel diverse theorieën blijken bepaalde gelijkaardige eigenschappen en structuren geregeld op te duiken, zoals bij ogenschijnlijk sterk verschillende diersoorten op een meer fundamenteel niveau gelijkaardige lichaamskenmerken of skeletstructuren aanwezig zijn. Een van die wiskundige structuren is de *groepsstructuur*. Deze structuur kan teruggebracht worden tot drie fundamentele kenmerken, die we de *groepsaxioma's* noemen en die als het ware het DNA vormen van de groepentheorie. In deze drie axioma's zitten talloze eigenschappen besloten en een doel van de groepentheorie bestaat erin deze eigenschappen te ontrafelen. In die domeinen van de wiskunde, fysica, chemie of informatica waar de groepsstructuur blijkt op te duiken, kunnen de groepseigenschappen gebruikt worden om meer inzicht te krijgen in de bijbehorende fenomenen. Net zoals de bevindingen van de geneticus de basis vormen voor toepassingen binnen de geneeskunde, de biotechnologie of het milieubeheer, kan de abstracte groepentheorie aangewend worden binnen zowel de zuivere wiskunde zelf, als in diverse toegepaste domeinen.

Een toepassing binnen de zuivere wiskunde die we uitvoerig bespreken, ligt in de getaltheorie, de studie van de natuurlijke getallen. We bespreken een algoritme om (heel) snel te beslissen of een gegeven (heel groot) natuurlijk getal al dan niet een priemgetal is. Dit kent op zijn beurt veel toepassingen binnen het beveiligen van digitaal dataverkeer, waarvan onze maatschappij steeds meer afhankelijk is.

De wiskundige voorkennis die je nodig hebt om met dit boek aan de slag te gaan, is beperkt. We zullen de theorie van groepen namelijk stap voor stap opbouwen, vertrekkende van drie elementaire axioma's die eenvoudig te begrijpen zijn. Onderweg leer je de taal kennen om over groepen te praten – de taal van de zuivere wiskunde. Bewijstechnieken die in de bewijzen aan bod komen, zetten we extra in de verf om je meer vertrouwd te maken met klassieke redeneringen binnen de wiskunde. De oefeningen op het einde van elk hoofdstuk laten je de geziene leerstof grondig verwerken en zetten je aan tot creatief en probleemoplossend denken. Je wordt bovendien gestimuleerd om precies en nauwkeurig je gevonden resultaten neer te schrijven.

In het eerste hoofdstuk voeren we enkele elementaire wiskundige begrippen in. Deze zijn nodig om de groepsaxioma's nauwkeurig te formuleren. Het is mogelijk dat deze begrippen door de lezer reeds gekend zijn, maar het is toch belangrijk van dezelfde basis te vertrekken en dus enkele algemene afspraken te maken en notaties in te voeren.

Groepen worden formeel ingevoerd in het tweede hoofdstuk, gevolgd door een ruim aantal voorbeelden uit ver uiteenlopende domeinen binnen de wiskunde. We onderzoeken de eerste en meest elementaire eigenschappen en zetten meteen de toon van heel het boek door ze zorgvuldig te bewijzen. Verder zoomen we in op drie belangrijke voorbeelden van eindige groepen die in de verdere hoofdstukken een belangrijke rol zullen spelen.

In het derde hoofdstuk leren we we hoe we nieuwe groepen kunnen construeren. We vertrekken van bestaande groepen en knippen ze uiteen of plakken ze samen om zo tot

nieuwe groepen te komen. Veel van deze nieuwe groepen zullen echter niet essentieel verschillen van groepen die we reeds kenden. Daarom ontwikkelen we technieken om na te gaan in welke mate twee groepen al dan niet wezenlijk verschillend zijn.

In het laatste hoofdstuk leggen we de verzamelde puzzelstukjes samen en bewijzen we de eerste stelling die echt een fundamenteel nieuw inzicht toevoegt aan de groepentheorie: de stelling van Lagrange. Deze stelling is prachtig in haar eenvoud, maar ook bijzonder nuttig in toepassingen. Als toepassing ontwikkelen we een algoritme om na te gaan of een natuurlijk getal al dan niet een priemgetal is – een priemtest dus. Als we deze priemtest vergelijken met een meer elementair algoritme dat geen gebruik maakt van groepentheorie, dan zien we dat het elementaire algoritme voor heel grote getallen miljarden jaren moet rekenen, terwijl onze priemtest klaar is na minder dan een seconde.

De auteurs willen graag hun dankbaarheid uiten aan Wouter Castryck, Filip Cools en Bert Seghers voor de inspirerende gesprekken en suggesties, aan alle betrokkenen bij uitgeverij Plantyn voor hun steun en vertrouwen en tenslotte, maar niet in het minst, aan Pedro Tytgat voor het fantastische initiatief, de vlotte samenwerking en de uitstekende eindredactie.

Tristan Kuijpers
Claudine Lybaert
december 2013

Inhoudsopgave

Lijst van bewijstechnieken

Hoofdstuk 1

Inleidende begrippen en definities

In dit hoofdstuk definiëren we enkele belangrijke begrippen en leggen we de notatie en terminologie vast die zullen gelden in de rest van dit boek. Deze zullen op een aantal punten mogelijk verschillen van wat gangbaar is in het secundair onderwijs. Het is in het algemeen niet ongebruikelijk dat in verschillende deelgebieden van de wiskunde, in verschillende landen of periodes ook verschillende notaties worden gebruikt. Dit is geen probleem zolang in het begin van de tekst alle definities en notaties maar duidelijk worden vermeld.

In de eerste paragraaf leggen we de notatie vast van enkele gekende verzamelingen. We voeren ook de *productverzameling* in, wat een manier is om nieuwe verzamelingen te maken uit reeds bestaande verzamelingen. In de tweede paragraaf komt het begrip *relatie* aan bod. Relaties zullen een belangrijke rol spelen in hoofdstuk 4. In de derde en laatste paragraaf geven we de definitie van een afbeelding en bekijken we enkele belangrijke eigenschappen ervan.

Al deze begrippen zullen het gereedschap vormen waarmee we de wiskunde rond groepentheorie zullen opbouwen.

1.1 Verzamelingen

Definitie 1.1. De verzameling van de natuurlijke getallen is $\{0, 1, 2, 3, \ldots\}$ en wordt genoteerd met $\mathbb{N}$. We noteren de verzameling $\{1, 2, 3, \ldots\}$ met $\mathbb{N}_0$. De verzameling van gehele getallen is $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ en wordt genoteerd met $\mathbb{Z}$. Verder hebben we de verzameling van rationale getallen, namelijk $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z} \text{ en } b \in \mathbb{N}_0\}$. We duiden met $\mathbb{R}$ de verzameling van reële getallen aan en met $\mathbb{C}$ de verzameling van complexe getallen, namelijk $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$.

Opmerking. In dit boek zullen in sommige voorbeelden de complexe getallen opduiken. Indien de lezer niet vertrouwd is met deze getallen, kan hij deze voorbeelden gewoon overslaan.

Definitie 1.2. Zij A en B verzamelingen. Dan zeggen we dat A een *deelverzameling* is van B, genoteerd met $A \subset B$, indien elk element van A ook een element is van B. We zeggen dat $A = B$ als $A \subset B$ en $B \subset A$.

Definitie 1.3. Af en toe zullen we in dit boek de symbolen $\exists$ en $\forall$ gebruiken. We lezen $\exists$ als *er bestaat* en $\forall$ als *voor alle*. Bijvoorbeeld $\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : x < y$ lezen we als *voor elk reëel getal x bestaat er een reëel getal y zodat x strikt kleiner is dan y*. Verder gebruiken we de symbolen $\Rightarrow$ voor *daaruit volgt*, en $\iff$ voor *als en slechts als*.

In een Nederlandse volzin zullen we deze vier symbolen nooit gebruiken, maar telkens voluit schrijven. Enkel in redeneringen in symbolen zullen we ze aanwenden.

Definitie 1.4. Zij A en B twee verzamelingen. De *productverzameling* van A en B is de verzameling die bestaat uit alle koppels (x, y), waarbij x een element is van A en y een element is van B. We noteren de productverzameling van A en B met $A \times B$ en in symbolen is

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

Voorbeeld 1.5. Zij $A = \{1, 2, 3\}$ en $B = \{\alpha, \beta\}$, dan is

$$A \times B = \{(1, \alpha), (2, \alpha), (3, \alpha), (1, \beta), (2, \beta), (3, \beta)\}.$$

Voorbeeld 1.6. We kunnen ook het product nemen van een verzameling met zichzelf. Zo is $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$. We noteren dikwijls $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

1.2 Relaties

Je bent al vertrouwd met het concept *relatie*. Bijvoorbeeld, indien we in een school de verzameling van leerlingen aanduiden met X en die van leerkrachten met Y, dan is "krijgt les van" een *relatie* tussen X en Y. In plaats van te spreken van een relatie tussen X en Y, kunnen we meer wiskundig ook spreken van een relatie op de productverzameling $X \times Y$. De relatie "krijgt les van" bepaalt dan een deelverzameling van koppels (x, y) van $X \times Y$ waarvoor geldt "x krijgt les van y".

In een wiskundige context verbinden relaties meestal elementen uit eenzelfde verzameling X. In plaats van te spreken over relaties op $X \times X$ spreken we meestal gewoon over relaties op X.

Voorbeeld 1.7. Zo is $<$ een relatie op $\mathbb{R}$: twee elementen $x, y \in \mathbb{R}$ voldoen aan de relatie $<$ als en slechts als x strikt kleiner is dan y en we noteren dit met $x < y$. De relatie $<$ bepaalt een deelverzameling van koppels $(x, y) \in \mathbb{R}^2$ waarvoor geldt dat $x < y$.

Voorbeeld 1.8. Beschouw de verzameling $\mathcal{L}$ van alle rechten in het vlak en als relatie "is evenwijdig met". Twee rechten a en b voldoen aan deze relatie op $\mathcal{L}$ als en slechts als ze evenwijdig zijn, wat we noteren met $a \parallel b$. De relatie $\parallel$ bepaalt een deelverzameling van koppels $(a, b) \in \mathcal{L}^2$ waarvoor geldt dat $a \parallel b$.

In het algemeen noteren we een relatie met R en wanneer twee elementen x en y voldoen aan de relatie R, noteren we dit met $x \mathrel{R} y$. Indien x en y niet voldoen aan de relatie R, zullen we dit noteren met $x \not\mathrel{R} y$.

Voorbeeld 1.9. Zij $X = \{2, 4, 6, 8, 10\}$ en zij R de relatie die uitdrukt dat een element een veelvoud is van een ander. Zo is bijvoorbeeld $10 \mathrel{R} 2$ en $8 \mathrel{R} 4$. We kunnen deze relatie voorstellen als de deelverzameling

$$R = \{(2, 2), (4, 2), (6, 2), (8, 2), (10, 2), (4, 4), (8, 4), (6, 6), (8, 8), (10, 10)\}$$

van X^2.

Uit de voorbeelden bleek al dat dat een relatie op X een deelverzameling van X^2 bepaalt. In de volgende definitie vereenzelvigen we een relatie met die deelverzameling.

Definitie 1.10. Zij X een verzameling. Dan noemen we eender welke deelverzameling $R \subset X^2$ een *relatie* op X.

Voorbeeld 1.11. Definitie 1.10 maakt duidelijk dat een relatie niet noodzakelijk moet gegeven worden door een *mooi* wiskundig verband. Zo is ook $\{(1,3),(2,4),(4,2)\} \subset \mathbb{N}^2$ een relatie op $\mathbb{N}$.

Er zijn een aantal eigenschappen die een relatie interessant maken om mee te werken en die we daarom een speciale naam geven.

Definitie 1.12. Zij X een verzameling en R een relatie op X. Dan noemen we R

(i) reflexief als $\forall x \in X : x \; R \; x$;

(ii) symmetrisch als $\forall x, y \in X : x \; R \; y \iff y \; R \; x$;

(iii) antisymmetrisch als $\forall x, y \in X : (x \neq y \text{ en } x \; R \; y) \Rightarrow y \not R \, x$;

(iv) transitief als $\forall x, y, z \in X : (x \; R \; y \text{ en } y \; R \; z) \Rightarrow x \; R \; z$.

Voorbeeld 1.13. De relatie $\parallel$ op de verzameling $\mathcal{L}$ van alle rechten in het vlak (zie Voorbeeld 1.8) is:

(i) reflexief, want elke rechte is evenwijdig met zichzelf;

(ii) symmetrisch, want als een rechte a evenwijdig is met een rechte b, dan is b ook evenwijdig met a en omgekeerd;

(iv) transitief, want als een rechte a evenwijdig is met een rechte b en b is evenwijdig met een rechte c, dan is a ook evenwijdig met c.

Voorbeeld 1.14. De relatie $<$ op $\mathbb{R}$ is niet reflexief en niet symmetrisch, maar wel antisymmetrisch en transitief. De relatie R uit Voorbeeld 1.9 is reflexief, antisymmetrisch en transitief, maar niet symmetrisch. Ga na!

> *Opdracht* 1.15. Ga ook voor de andere relaties die we reeds zagen na of ze al dan niet reflexief, symmetrisch, antisymmetrisch of transitief zijn.

> *Opdracht* 1.16. Bestaan er relaties die niet symmetrisch en ook niet antisymmetrisch zijn? Zijn er relaties die zowel symmetrisch als antisymmetrisch zijn? Indien ja, geef een voorbeeld. Indien nee, verklaar waarom het niet mogelijk is.

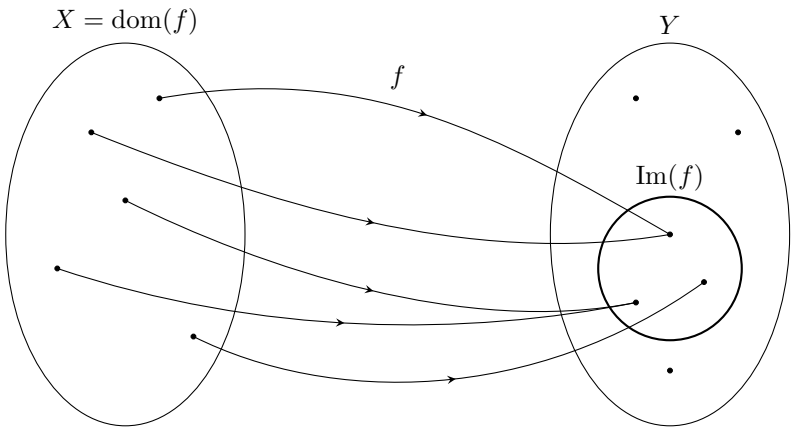
1.3 Afbeeldingen

Zij X en Y verzamelingen. Een afbeelding is een speciaal soort relatie tussen X en Y, namelijk één die met *elk* element van X *precies één* element van Y associeert.

Voorbeeld 1.17. Als we met elk element $x \in \mathbb{R}$ het kwadraat van dit element associëren, dan krijgen we de afbeelding $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$.

Definitie 1.18. Zij X en Y verzamelingen. Een *afbeelding* f van X naar Y is een relatie op $X \times Y$ zodat voor elke $x \in X$ precies één element $y \in Y$ bestaat zodat (x, y) een element is van deze relatie. Voor deze x en y noteren we $f(x) = y$.

We noemen X het *domein* van de afbeelding f, genoteerd met $\mathrm{dom}(f)$. Het is niet verplicht dat elk element van Y wordt bereikt door de afbeelding. We noteren de verzameling van de beelden als $\mathrm{Im}(f) = \{y \in Y \mid \exists x \in X : f(x) = y\}$ en noemen dit het *beeld* van de



Figuur 1.1: Schematische voorstelling van een afbeelding $f : X \to Y$

afbeelding f. Het beeld van een afbeelding f wordt ook wel met $\mathrm{bld}(f)$ genoteerd. Er geldt dus $\mathrm{Im}(f) \subset Y$ (zie Figuur 1.1).

Meer algemeen noteren we $f : X \to Y : x \mapsto f(x)$ om duidelijk te maken dat f een afbeelding is van X naar Y die elk element $x \in X$ afbeeldt op het element $f(x) \in Y$.

Definitie 1.19. We zeggen dat twee afbeeldingen $f : X \to Y$ en $g : X \to Y$ *gelijk zijn*, indien voor elke $x \in X$ geldt dat $f(x) = g(x)$.

Opmerking. Op het eerste zicht lijkt een afbeelding heel sterk op een functie. Het enige verschil is dan ook dat bij een functie $f : X \to Y$ het domein een deelverzameling is van X, terwijl bij een afbeelding $f : X \to Y$ steeds geldt dat $\mathrm{dom}(f) = X$. Met andere woorden, er hoeft bij een functie niet uit elk element van X een pijl te vertrekken en bij een afbeelding wel.

Voorbeeld 1.20. De afbeelding $f : [-1, 1] \to \mathbb{R} : x \mapsto x^2$ beeldt elk element van $[-1, 1]$ af op het kwadraat van dit element. Hier is $\mathrm{dom}(f) = [-1, 1]$ en $\mathrm{Im}(f) = [0, 1]$.

Een belangrijke klasse van afbeeldingen zijn afbeeldingen van een verzameling naar zichzelf. We geven ze daarom een speciale naam.

Definitie 1.21. Zij X een verzameling, dan noemen we een afbeelding $f : X \to X$ een *transformatie*.

De eenvoudigste transformatie is degene die elk element $x \in X$ afstuurt op zichzelf. We noemen dit de *identieke* transformatie, genoteerd met id_X. In formulevorm is dus

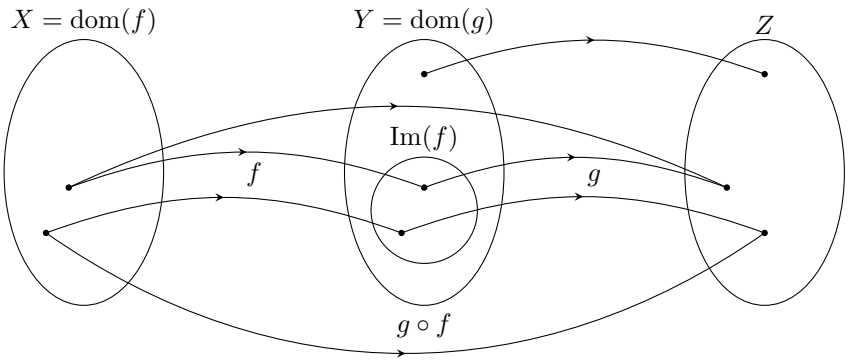
$$\mathrm{id}_X : X \to X : x \mapsto x.$$

Indien het uit de context duidelijk is over welke verzameling X het gaat, schrijven we vaak kortweg id in plaats van id_X.

Definitie 1.22. Zij X, Y en Z verzamelingen en $f : X \to Y$ en $g : Y \to Z$ afbeeldingen. Dan noteren we

$$g \circ f : X \to Z : x \mapsto g(f(x))$$

en noemen dit de *samenstelling* van de afbeeldingen f en g. We lezen $g \circ f$ als g *na* f (zie Figuur 1.2).



Figuur 1.2: Schematische voorstelling van de samenstelling $g \circ f : X \to Z$

Definitie 1.23. Zij X en Y verzamelingen en $f : X \to Y$ een afbeelding. We noemen f *injectief* indien verschillende elementen van X op verschillende elementen van Y worden afgebeeld. Meer formeel is f injectief als:

$$\forall x_1, x_2 \in X : f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

We noemen f *surjectief* als elk element in Y het beeld is van minstens één element in X. In dit geval is $\mathrm{Im}(f) = Y$. Meer formeel is f surjectief als:

$$\forall y \in Y : \exists x \in X : f(x) = y.$$

We noemen f *bijectief* als f zowel injectief als surjectief is.

Voorbeeld 1.24. (i) De afbeelding $f : \mathbb{Z} \to \mathbb{Q} : x \mapsto x$ is injectief omdat twee verschillende elementen $x, y \in \mathbb{Z}$ steeds een verschillend beeld hebben. De afbeelding f is echter niet surjectief omdat er bijvoorbeeld geen enkele $x \in \mathbb{Z}$ bestaat zodat $f(x) = \frac{1}{2}$.

(ii) De afbeelding $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ is noch injectief, noch surjectief. Ga zelf na waarom!

(iii) Zij $\mathbb{R}_0 = \mathbb{R} \setminus \{0\}$. De afbeelding $f : \mathbb{R}_0 \to \mathbb{R}_0 : x \mapsto 1/x$ is een bijectie. Aangezien $1/x = 1/y \Rightarrow x = y$ voor alle $x, y \in \mathbb{R}_0$, is f immers injectief en aangezien elk element $x \in \mathbb{R}_0$ het beeld is van $1/x$, is f surjectief.

(iv) De afbeelding $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} : (x, y) \mapsto x$ is surjectief omdat elk element $x \in \mathbb{R}$ het beeld is van (bijvoorbeeld) $(x, 0)$. Deze afbeelding is echter niet injectief, omdat bijvoorbeeld $f((2, -3)) = f((2, 1/2))$ terwijl $(2, -3) \neq (2, 1/2)$.

Lemma 1.25. *Zij X en Y eindige verzamelingen waartussen een bijectie $f : X \to Y$ bestaat. Dan hebben X en Y evenveel elementen.*

Bewijs. We moeten aantonen dat het niet mogelijk is dat X en Y een verschillend aantal elementen hebben. Veronderstel nu even dat dat wel zo is. Veronderstel eerst dat X minder elementen heeft dan Y. Dan heeft ook $\mathrm{Im}(f)$ minder elementen dan Y. Er bestaat dus een element van Y dat niet het beeld is van een element van X en dus kan f niet surjectief zijn. Aangezien we weten dat f een bijectie is en dus wel surjectief is, kunnen we besluiten dat X al zeker niet minder elementen kan hebben dan Y.

Dus moet Y minder elementen hebben dan X. Maar dan is er minstens één element van Y dat het beeld is van meerdere elementen van X. Dit wil zeggen dat f niet injectief is en dus ook geen bijectie kan zijn. We komen dus weeral uit bij een tegenstrijdigheid. De veronderstelling dat X en Y een verschillend aantal elementen hebben, is niet houdbaar. Dus moeten X en Y evenveel elementen hebben. □

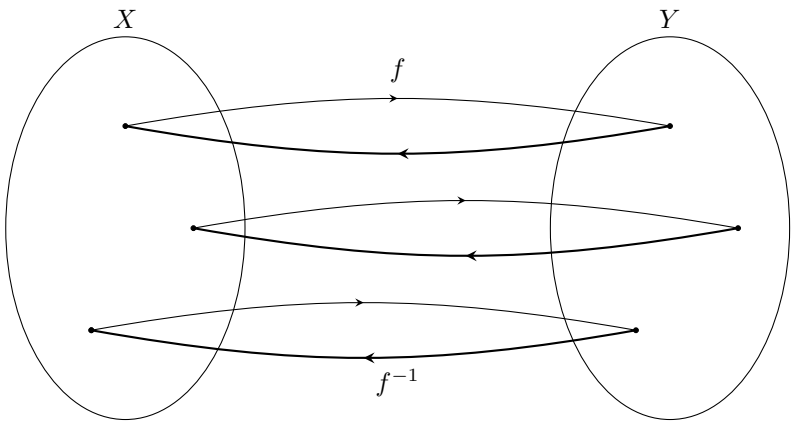
Bewijstechniek. Het voorgaande bewijs is een bewijs *uit het ongerijmde*. Het is een bewijstechniek waarbij we het tegenovergestelde aannemen van wat we willen bewijzen en dan trachten een contradictie (of tegenstrijdigheid) te verkrijgen. Aangezien tegenstrijdigheden binnen de wiskunde onmogelijk zijn, moet de tegenovergestelde aanname foutief geweest zijn en dus geldt datgene wat we wilden bewijzen.

Lemma 1.26. *Zij X en Y eindige verzamelingen met evenveel elementen. Zij $f : X \to Y$ injectief, dan is f automatisch ook surjectief en dus een bijectie.*

Bewijs. We geven opnieuw een bewijs uit het ongerijmde. Veronderstel dus dat f niet surjectief is. Dat wil zeggen dat er een element is van Y dat niet wordt bereikt door f. Het beeld van f bevat dus minder elementen dan Y. Aangezien X en Y evenveel elementen hebben, bevat het beeld van f dus ook minder elementen dan X. Dit wil zeggen dat er een element is in het beeld van f dat het beeld is van meerdere elementen van X, wat in strijd is met de injectiviteit van f. □

Lemma 1.27. *Zij $f : X \to Y$ een bijectie. Dan bestaat er een unieke afbeelding $f^{-1} : Y \to X$ zodat $f \circ f^{-1} = \mathrm{id}_Y$ en zodat $f^{-1} \circ f = \mathrm{id}_X$. Bovendien is $f^{-1} : Y \to X$ ook een bijectie en er geldt $(f^{-1})^{-1} = f$.*

Bewijs. We definiëren $f^{-1} : Y \to X$ als volgt. Zij $y \in Y$. Aangezien f een surjectie is, bestaat er een $x \in X$ zodat $f(x) = y$ en we definiëren $f^{-1}(y) = x$ (zie Figuur 1.3).



Figuur 1.3: Schematische voorstelling van een bijectie $f : X \to Y$ en van $f^{-1} : Y \to X$

Ten eerste merken we op dat $f^{-1} : Y \to X$ een goed gedefinieerde afbeelding is, aangezien f injectief is en er dus met elk element van Y precies één element van X overeen komt.

Het is duidelijk dat deze afbeelding f^{-1} voldoet aan $f \circ f^{-1} = \mathrm{id}_Y$ en $f^{-1} \circ f = \mathrm{id}_X$. Ga zelf na dat dat er maar één afbeelding kan zijn die hieraan voldoet.

Nu tonen we aan dat f^{-1} een bijectie is. Het is onmogelijk dat twee verschillende elementen van Y op hetzelfde element van X worden afgebeeld door f^{-1} omdat f een

afbeelding is en dus met elk element van X precies één element van Y associeert. Met andere woorden is f^{-1} injectief. Zij nu $x \in X$ willekeurig, dan is $f^{-1}(f(x)) = x$, dus bestaat er een element in Y dat op x wordt afgebeeld. Dit wil zeggen dat f^{-1} surjectief is. We vinden zo dat $f^{-1} : Y \to X$ een bijectie is. De formule $(f^{-1})^{-1} = f$ volgt hier automatisch uit (ga na!). □

Lemma 1.28. *Zij $f : X \to Y$ en $g : Y \to Z$ bijecties, dan is ook $g \circ f : X \to Z$ een bijectie.*

Bewijs. We tonen eerst aan dat $g \circ f$ injectief is. Zij $x_1, x_2 \in X$ en veronderstel dat $(g \circ f)(x_1) = (g \circ f)(x_2)$. We kunnen dit ook schrijven als $g(f(x_1)) = g(f(x_2))$ en aangezien g injectief is, geldt dat $f(x_1) = f(x_2)$. Maar ook f is injectief, dus vinden we dat $x_1 = x_2$ en bijgevolg is $g \circ f$ injectief.

We tonen vervolgens aan dat $g \circ f$ surjectief is. Zij $z \in Z$ een willekeurig element. Aangezien g surjectief is, weten we dat er een element $y \in Y$ bestaat zodat $g(y) = z$. Omdat ook f surjectief is, bestaat er een element $x \in X$ zodat $f(x) = y$. Nu vinden we gemakkelijk dat

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

dus $g \circ f$ is surjectief. □

1.4 Oefeningen

1. (a) Zij $A = \{1, 2\}$ en $B = \{3\}$. Ga na dat
$$(A \times B) \cup (B \times A) \subset (A \cup B)^2.$$
   (b) Toon aan dat de bovenstaande formule geldt voor willekeurige verzamelingen A en B.

2. Ga voor de volgende relaties R op $\mathbb{Z}$ na of ze reflexief, symmetrisch of transitief zijn.
   (a) $a \; R \; b \iff a|b$
   (b) $a \; R \; b \iff a^2 + a = b^2 + b$
   (c) $a \; R \; b \iff 7|(a - b)$

3. Ga voor de volgende relaties R op $\mathbb{R}$ na of ze reflexief, symmetrisch of transitief zijn.
   (a) $a \; R \; b \iff a = b$
   (b) $a \; R \; b \iff a = b + 1$
   (c) $a \; R \; b \iff a \leq b$

4. Ga voor de volgende relaties R op $\mathbb{C}$ na of ze reflexief, symmetrisch of transitief zijn.
   (a) $a \; R \; b \iff a = |b|$
   (b) $a \; R \; b \iff |a| = |b|$

5. Zij $f(x) = \sqrt{x}$, $g(x) = x/8$, $h(x) = 3x - 2$. Zoek het functievoorschrift van:
   (a) $h \circ g$ (c) $g \circ h$ (e) $f \circ g$
   (b) $h \circ f$ (d) $g \circ f$ (f) $f \circ h$

6. Zij $f(x) = x-4$, $g(x) = \sqrt{x}$, $h(x) = x^3$, $j(x) = 3x$. Schrijf de volgende afbeeldingen als een samenstelling van de bovenstaande afbeeldingen:
   (a) $\sqrt{x-4}$ (e) $\sqrt{(x-4)^3}$ (i) x^9
   (b) $3\sqrt{x}$ (f) $(3x-12)^3$ (j) $x-12$
   (c) $x^{1/4}$ (g) $3x-4$ (k) $3\sqrt{x-4}$
   (d) $9x$ (h) $x^{3/2}$ (l) $\sqrt{x^3-4}$

7. Zij $f : A \to B$ en $g : B \to C$ twee afbeeldingen. Bewijs of geef een tegenvoorbeeld bij de volgende uitspraken.
   (a) Als $g \circ f$ injectief is, dan is f injectief.
   (b) Als $g \circ f$ injectief is, dan is g injectief.
   (c) Als $g \circ f$ surjectief is, dan is g surjectief.
   (d) Als $g \circ f$ surjectief is, dan is f surjectief.

8. Zij $B \subset \mathbb{R}$ en zij $f : [1, +\infty[\to B : x \mapsto \frac{1-5x}{x}$.
   (a) Bewijs dat f injectief is.
   (b) Bepaal B zodat f surjectief is.
   (c) Bepaal in dit geval f^{-1}.

9. Onderzoek of volgende afbeeldingen injectief of surjectief zijn:
   (a) $f : \mathbb{R} \to \mathbb{R}^+ : x \mapsto x^2$
   (b) $g : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$
   (c) $h : \mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto x^2$

10. Zij $A = \{0, 1, 2\}$, $B = \{0, 1\}$ en $C = \{\mathrm{id}, a, a^2, b, ab, ab^2\}$.
    Definieer $f : A \times B \to C$ als volgt:

$$\begin{aligned} f : A \times B \to C : (0,0) &\mapsto \mathrm{id} \\ (1,0) &\mapsto a \\ (2,0) &\mapsto a^2 \\ (0,1) &\mapsto b \\ (1,1) &\mapsto ab \\ (2,1) &\mapsto a^2 b. \end{aligned}$$

    Toon aan dat f een bijectie is.