

HOOFDSTUK 2

STRUCTUREN

Een structuur, in een binnen de wiskundige logica gangbare betekenis van het woord, is een verzameling met relaties en operaties erover. Als er geen operaties zijn, hebben we te maken met een *relationeel stelsel*; als er alleen totale operaties zijn, met een *algebra*. Omdat we er niet van uitgaan dat operaties totaal zijn, en omdat we nulplaatsige relaties buiten beschouwing laten, kunnen we relaties en operaties onder één noemer brengen. Preciezer gezegd: we zullen relaties beschouwen als een bijzonder soort van operaties.

In een structuur die waarheidswaarden bevat, zeg *waar* en *onwaar*, kunnen we K -plaatsige relaties voorstellen als K -plaatsige operaties die een waarheidswaarde opleveren: $R(x) = \text{waar}$ als de familie x tot de relatie R behoort, en anders $R(x) = \text{onwaar}$. Deze oplossing is echter niet algemeen toepasbaar. Er zijn nu eenmaal structuren zonder voor de hand liggende waarheidswaarden.

Een oplossing die altijd werkt, en die we daarom aan zullen houden, is als volgt. In een structuur wordt een K -plaatsige relatie R gerepresenteerd door een K -plaatsige operatie Q_R waarvan alleen het domein van belang is. Als de familie x tot R behoort, dan bestaat $Q_R(x)$; en omdat $Q_R(x)$ iets moet zijn, en we er niet van uit mogen gaan dat er een geschikte waarheidswaarde bestaat, of zelfs dat er iets bestaat buiten $\text{Im } x$, veronderstellen we dat een index k^* is gespecificeerd zo dat voor elke K -geïndexeerde familie z ,

$$z \in R \Leftrightarrow Q_R(z) = z_{k^*}.$$

Als $z \notin R$, dan *bestaat* $Q_R(z)$ *niet*.¹

Formeel is een structuur dan een paar $\mathbf{A} = \langle A, F \rangle$ van een verzameling A (het *domein*)² en een verzameling F van operaties over A . De niet-lege elementen van F zijn de *basisoperaties* van $\mathbf{A}$. Veel van wat we willen vertellen vereist evenwel dat we gelijkplaatsige basisoperaties in verschillende structuren met elkaar vergelijken, en zo komen we tot de *benoemde* structuren die in §A worden ingevoerd. Wanneer het nodig is het onderscheid te maken, heet een structuur die bestaat uit een verzameling en een collectie van operaties daarop *onbenoemd*.

Zo nu en dan zullen we ook *bovenmaatse* structuren beschouwen, structuren $\langle A, F \rangle$ zo dat $A \cup F$ een echte klasse is.

§A Symbolen en interpretatie

We veronderstellen een onuitputtelijke klasse $\mathcal{Symb}$ van *symbolen*. Men kan zich die symbolen het beste voorstellen als primitieve objecten. Met ieder symbool Q is een vaste verzameling K_Q geassocieerd, zijn *plaatsigheid*.

¹ De vroegste verschijning in de literatuur, bij weten van de auteur, van deze reductie van relaties tot partiële operaties, is in 1968, in een boek van Pierce [P].

² Als uit de context niet het tegendeel blijkt, zullen we altijd aannemen dat het domein een *oerverzameling* is.

Benoemde structuren

Een *benoemde structuur* is een paar $\mathbf{A} = \langle A, \mathcal{I} \rangle$ bestaande uit een domein A en een operatie $\mathcal{I}$ (de *interpretatie*) die aan elk symbool Q een K_Q -plaatsige operatie over A toekent, de *interpretatie van Q* . Als Q een relatiesymbool representeert, dan geldt bovendien dat $\mathcal{I}(Q)(x) = x_{k^*}$ voor elke $x \in \text{Dom } \mathcal{I}(Q)$.

De *nomenclatuur* van een structuur $\langle A, \mathcal{I} \rangle$ is de klasse

$$\text{Nom}(A, \mathcal{I}) := \{Q \in \mathcal{Symb} \mid \mathcal{I}(Q) \neq \emptyset\}.$$

Zonder tegenbericht zullen we ervan uitgaan dat nomenclaturen verzamelingen zijn. Zulke nomenclaturen kun je beschrijven met een *functie* die de niet-lege interpretaties specificeert.

Een structuur $\mathbf{A}$ is van type $\mathcal{T}$, of een $\mathcal{T}$ -structuur ($\mathcal{T} \subseteq \mathcal{Symb}$), als $\text{Nom } \mathbf{A} \subseteq \mathcal{T}$. Structuren $\mathbf{A}$ en $\mathbf{B}$ heten *gelijknamig* als $\text{Nom } \mathbf{A} = \text{Nom } \mathbf{B}$.

In plaats van $\mathcal{I}(Q)$, bij een structuur $\mathbf{A} = \langle A, \mathcal{I} \rangle$, zullen we meestal $Q^{\mathbf{A}}$ schrijven. De niet-lege operaties $Q^{\mathbf{A}}$ zijn de basisoperaties van $\mathbf{A}$.

Zij $\mathcal{T}$ een type, en $\mathbf{A}$ een structuur. Dan is het $\mathcal{T}$ -reduct van $\mathbf{A}$ de structuur

$$\mathbf{A} \upharpoonright \mathcal{T} := \langle A, \mathcal{J} \rangle$$

waarin $\mathcal{J}$ gedefinieerd is, voor $Q \in \mathcal{Symb}$, door

$$\mathcal{J}(Q) = Q^{\mathbf{A}} \triangleleft Q \in \mathcal{T} \triangleright \emptyset.$$

Een structuur $\mathbf{B}$ is een *reduct* van een structuur $\mathbf{A}$, en $\mathbf{A}$ een *expansie* van $\mathbf{B}$, als $\mathbf{B} = \mathbf{A} \upharpoonright \text{Nom } \mathbf{B}$. Een structuur is altijd een reduct en een expansie van zichzelf.

Een verzameling kan worden beschouwd als een structuur van het lege type.

Bestaan en waarheid

Als Q een operatie is, dan benoemen we met $Q(x)$ de waarde die Q aan x toekent als die bestaat. Als Q aan x geen waarde toekent, dan beschouwen we elke bewering dat $Q(x)$ gelijk is aan iets, of in een logisch primitieve relatie staat tot bepaalde dingen, bestaand of niet, als *onwaar*. Evenzo is elke uitgebreidere expressie M die is opgebouwd uit operatiesymbolen en benamingen van elementen van het domein en de expressie $Q(x)$ bevat ongedefinieerd, en leidt ze tot onware beweringen. In het bijzonder is voor zo'n expressie M de bewering ' $M = M$ ' onwaar. Omdat $M = M$ triviaal waar is als M bestaat, is ' $M = M$ ' dus equivalent met $M \downarrow$.

De qualificatie 'logisch primitief' in de vorige alinea is wezenlijk. Bijvoorbeeld, *Frankrijk* is een land en *de koning van* is een operatie die aan sommige landen een persoon toekent; maar aan Frankrijk niet, want Frankrijk is een republiek. Onder aanname dat kaalheid logisch primitief is, is

$$\text{De koning van Frankrijk is kaal}$$

onwaar. *Dus* volgt uit de waarheidstafel voor implicatie dat de bewering

Als de koning van Frankrijk kaal is, eten we vanavond stokbrood
waar is.

We besluiten met twee relaties die *niet* logisch primitief zijn en die we vaak zullen gebruiken. De eerste is *gerichte gelijkheid* $\asymp$. Met $M \asymp N$ drukken we uit dat M alleen dan gedefinieerd is als N gedefinieerd is, en dat $M = N$ als M gedefinieerd is. De definitie van gerichte gelijkheid in termen van identiteit is

$$M \asymp N \text{ dan en slechts dan als: } M = M \Rightarrow M = N.$$

De conjunctie $M \asymp N \ \& \ N \asymp M$ werd door Kleene *volledige gelijkheid* genoemd, en genoteerd met $\simeq$; $M \simeq N$ betekent dat M gedefinieerd is dan en slechts dan als

N gedefinieerd is, en dat $M = N$ als M en N gedefinieerd zijn. De definitie in termen van identiteit is

$$M \simeq N \text{ dan en slechts dan als: } M = M \wp N = N \Rightarrow M = N.$$

Voorbeelden

i. Een structuur die iedereen kent van de lagere school³ is die van de natuurlijke getallen met tweeplaatsige optelling en aftrekking,

$$\mathbf{N} = \langle \mathbb{N}, \{+, -\} \rangle,$$

waarin in het bijzonder $x - y$ gedefinieerd is dan en slechts dan als $x \geq y$, en wel als het unieke getal z zo dat $x = y + z$.

ii (Burmeister). Een *Mealymachine* wordt gewoonlijk gegeven als een zestal

$$\langle S, s_0, \Sigma, \Lambda, t, \lambda \rangle,$$

waarin S een eindige verzameling is, de verzameling der *toestanden*; s_0 een benoemd element van S , de *begintoestand*; Σ en Λ eindige verzamelingen, het *invoeralfabet* en het *uitvoeralfabet*; $t: S \times \Sigma \rightarrow S$ de *transitiefunctie*, die de volgende toestand specificeert op basis van een gegeven toestand en een invoersymbool; en $\lambda: S \times \Sigma \rightarrow \Lambda$ de *uitvoerfunctie*. De corresponderende structuur is

$$\mathbf{M} = \langle S \cup \Sigma \cup \Lambda, \{Q_S, Q_\Sigma, Q_\Lambda, s_0, t, \lambda\} \rangle;$$

daarin zijn Q_S , Q_Σ en Q_Λ eenplaatsige operaties, zo dat $Q_S(x) \downarrow$ dan en slechts dan als $x \in S$, en in dat geval $Q_S(x) = x$, enzovoort. De binaire operaties t en λ voldoen aan de voorwaarden

$$(t) \quad \text{als } Q_S(x) \downarrow \text{ en } Q_\Sigma(y) \downarrow, \text{ dan } Q_S(t(x, y)) \downarrow,$$

$$(\lambda) \quad \text{als } Q_S(x) \downarrow \text{ en } Q_\Sigma(y) \downarrow, \text{ dan } Q_\Lambda(\lambda(x, y)) \downarrow.$$

Als S , Σ en Λ paarsgewijs disjunct zijn, is $\mathbf{M}$ een *gesorteerde algebra*: het domein M bestaat uit drie *soorten* van elementen, S , Σ , en Λ , het definitiegebied van elk van de operaties is een cartesisch product van soorten, en het beeld is bevat in een enkele soort. Definitiegebied en bestemmingssoort vormen het *type* van de operatie. In $\mathbf{M}$ is s_0 van type S , t van type $S \leftarrow S \times \Sigma$, en λ van type $\Lambda \leftarrow S \times \Sigma$.

Gesorteerde algebra's belichamen een strenge vorm van partialiteit, waarin de sortering volledig bepaalt waar een operatie gedefinieerd is. Zelfs in de informatica is niet alle partialiteit zo fraai gereguleerd, zoals blijkt uit het volgende voorbeeld.

iii (Burmeister). *Stapels* zijn een eenvoudige vorm van datastructuren. De ingrediënten zijn:

- *Items* om te stapelen, de elementen van een verzameling D .
- De stapels, die een verzameling S vormen.
- Een *lege* stapel $e \in S$.
- Een item d kan men *pousseren* op een stapel s ; het resultaat is een verhoogde stapel $P(d, s)$.
- Van een stapel s kun je het *top*-item *plukken*. Dat item is $T(s)$, de overblijvende stapel is $p(s)$.

Samen vormen deze ingrediënten een structuur

³ — die sinds een matig doordachte poging tot integratie met het kleuteronderwijs *basisschool* heet.

$$\mathbf{A} = \langle S \cup D, \{Q_S, Q_D, e, P, T, p\} \rangle.$$

De geïntendeerde typering is $e: S, P: S \leftarrow D \times S, T: D \leftarrow S$, and $p: S \leftarrow S$. Expliciet, (P) als $Q_S(x) \downarrow$ en $Q_D(y) \downarrow$, dan $Q_S(P(x, y)) \downarrow$,

enzovoort.

Helaas is de beschrijving van de situatie geen sluitende rechtvaardiging van deze typering. We hebben een duidelijke voorstelling van de stapel die we krijgen door item d te pousseren op stapel s ; en we weten wat de *top* is van $P(d, s)$, en welke stapel resulteert als we die plukken. Maar hoe zit het met $p(e)$ en $T(e)$? De ervaring laat een breed gedragen voorkeur zien voor $p(e) = e$; het item $T(e)$, daarentegen, zou alleen bijzonder zijn doordat het $T(e)$ is — voorzover we weten. Bovendien kan in de praktijk het plukken van de lege stapel tot een impasse leiden, of tot een *uitzonderlijk volle* stapel. Zodat als we willen dat $\mathbf{A}$ zoiets belichaamt als de *minimumeisen* voor stapels, $p(e)$ en $T(e)$ ongedefinieerd moeten blijven.

In het vervolg zullen we het onderscheid tussen de relatie R en de vertegenwoordigende operatie Q_R verwaarlozen: R is een operatie die aan $x \in R$ de waarde x_{k^*} toekent.

Het is gebruik om een benoemde structuur waarin bekende symbolen worden geïnterpreteerd als bekend veronderstelde operaties te beschrijven door het domein en de operatiesymbolen, liefst in een vaste volgorde, op te sommen. In Voorbeeld (i) zouden we $\mathbf{N} = \langle \mathbb{N}, +, - \rangle$ kunnen schrijven. Bij gesorteerde structuren kan men de naam van het domein vervangen door een opsomming van de soorten, die we dan van de operaties scheiden door een puntkomma; in Voorbeeld (ii) kan dat resulteren in $\mathbf{M} = \langle S, \Sigma, \Lambda; s_0, t, \lambda \rangle$; in Voorbeeld (iii) in $\mathbf{A} = \langle S, D; e, P, T, p \rangle$.

Onvolledige Hoare-notatie

We kunnen volledige gelijkheid gebruiken in definities met enkelvoudige gevalsonderscheiding:

$$F(x) \simeq M(x) \triangleleft A(x) \triangleright N(x)$$

staat voor: $F(x)$ is $M(x)$ als $M(x)$ bestaat en $A(x)$, $N(x)$ als $N(x)$ bestaat en $\sim A(x)$, en anders ongedefinieerd. Houden we eenmaal rekening met ongedefinieerdheid, dan kunnen we ook *onvolledige* Hoare-notatie gebruiken:

$$F(x) \simeq M(x) \triangleleft A(x)$$

betekent: $F(x)$ is $M(x)$ als $A(x)$ en $M(x)$ bestaat, en anders ongedefinieerd.

Ook in de onvolledige notatie kunnen we verborgen parameters inbouwen. Een definitie

$$F(x) \simeq M(x, y) \triangleleft A(x, y)$$

staat voor

$$F(x) \begin{cases} = M(x, y) \text{ als } A(x, y) \text{ geldt en } M(x, y) \downarrow, \\ \text{is ongedefinieerd als er geen } y \text{ is zo dat } A(x, y) \text{ geldt en } M(x, y) \downarrow; \end{cases}$$

mits natuurlijk algemeen geldt dat

$$A(x, y_1) \ \& \ A(x, y_2) \ \& \ M(x, y_1) \downarrow \ \& \ M(x, y_2) \downarrow \Rightarrow M(x, y_1) = M(x, y_2).$$

§B Substructuren

Zij $\mathbf{A}$ een structuur. Een *subdomein* van $\mathbf{A}$ is een verzameling $X \subseteq A$ die *gesloten* is onder de basisoperaties van $\mathbf{A}$: voor alle $Q \in \mathcal{Symb}$,

$$\text{als } x \in (\text{Dom } Q^{\mathbf{A}})|_X \text{ dan } Q^{\mathbf{A}}(x) \in X.$$

We duiden de collectie van alle subdomeinen van $\mathbf{A}$ aan met $\text{Sub } \mathbf{A}$.

Vanzelfsprekend geldt dat $A \in \text{Sub } \mathbf{A}$. Een subdomein $B \neq A$ heet een *echt* subdomein van $\mathbf{A}$. Een structuur is *minimaal* als ze geen echte subdomeinen heeft.

Voorbeelden

i. Laat t en f twee dingen zijn die niet tot $\mathbb{N}$ behoren, en $A = \mathbb{N} \cup \{t, f\}$. Definieer een interpretatie $\mathcal{I}$ in A van drie nulplaatsige operatiesymbolen t , f en 0 , drie eenplaatsige operatiesymbolen N , B en S , en een binair operatiesymbool Eq , door

$$\mathcal{I}(N) = 1_{\mathbb{N}}, \mathcal{I}(B) = 1_{\{t, f\}};$$

$$\mathcal{I}(t) = t, \mathcal{I}(f) = f, \mathcal{I}(0) = 0;$$

$$\mathcal{I}(S) = \{\langle n+1, n \rangle \mid n \in \mathbb{N}\};$$

$$\mathcal{I}(Eq) = (\{t\} \times \Delta_{\mathbb{N}}) \cup (\{f\} \times (\nabla_{\mathbb{N}} \setminus \Delta_{\mathbb{N}})).$$

(Bij verstek zijn de andere interpretaties leeg.) Zij $\mathbf{A} = \langle A, \mathcal{I} \rangle$.

Ieder subdomein van $\mathbf{A}$ bevat t , f en 0 ; en bovendien $1 = S^{\mathbf{A}}(0)$, $2 = S^{\mathbf{A}}(1)$, en zo voort langs alle natuurlijke getallen. De structuur $\mathbf{A}$ heeft dus geen echte subdomeinen: $\mathbf{A}$ is minimaal.

ii. Een relatie is een operatie R die elke familie x in zijn definitiegebied afbeeldt naar het element x_{k^*} van $\text{Im } x$. Bijgevolg is iedere deelverzameling van het domein van een structuur gesloten onder relaties; dus in een relationeel stelsel $\mathbf{A}$, $\text{Sub } \mathbf{A} = \mathcal{P}A$.

1 DEFINITIE. Laat $\mathbf{A} = \langle A, \mathcal{I} \rangle$ en $\mathbf{B} = \langle B, \mathcal{J} \rangle$ structuren zijn zo dat $A \subseteq B$.

(a) $\mathbf{A}$ is een *zwakke substructuur* van $\mathbf{B}$, notatie $\mathbf{A} \subseteq \mathbf{B}$, en $\mathbf{B}$ een *uitbreiding* van $\mathbf{A}$, als $\mathcal{I}(Q) \subseteq \mathcal{J}(Q)$ voor elk symbool $Q \in \mathcal{Symb}$.

(b) $\mathbf{A}$ is een *relatieve substructuur* van $\mathbf{B}$, notatie $\mathbf{A} \subseteq \mathbf{B}$, en $\mathbf{B}$ een *uitwendige uitbreiding* van $\mathbf{A}$, als $\mathcal{I}(Q) = \mathcal{J}(Q)|_A$ voor elk symbool $Q \in \mathcal{Symb}$.

(c) $\mathbf{A}$ is een *gesloten substructuur* van $\mathbf{B}$, notatie $\mathbf{A} \leq \mathbf{B}$, en $\mathbf{B}$ een *superstructuur* van $\mathbf{A}$, als $\mathbf{A} \subseteq \mathbf{B}$ en $A \in \text{Sub } \mathbf{B}$.

Met ‘substructuur’, zonder nadere bepaling, zullen we altijd ‘gesloten substructuur’ bedoelen.

In plaats van ‘ $\mathbf{A} \subseteq \mathbf{B}$ en $\mathbf{A} \neq \mathbf{B}$ ’ kunnen we $\mathbf{A} \subset \mathbf{B}$ schrijven; we zeggen dan dat $\mathbf{A}$ een *echte* zwakke substructuur is van $\mathbf{B}$. Analoog schrijven we $\mathbf{A} \subset \mathbf{B}$ en $\mathbf{A} < \mathbf{B}$, en spreken van *echte* relatieve substructuren en *echte* substructuren.

Merk op dat elke deelverzameling A van het domein van een structuur $\mathbf{B}$ een unieke relatieve substructuur van $\mathbf{B}$ bepaalt die A als domein heeft. We duiden die aan met $\mathbf{B}|_A$. Daarentegen kunnen er vele zwakke substructuren van $\mathbf{B}$ bestaan die een gegeven $A \subseteq B$ als domein hebben. In het bijzonder kunnen er echte zwakke substructuren van $\mathbf{B}$ bestaan die B als domein hebben; we noemen ze *verarmingen* van $\mathbf{B}$. Als $\mathbf{A}$ een verarming is van $\mathbf{B}$, dan is $\mathbf{B}$ een *inwendige uitbreiding* van $\mathbf{A}$.

Voorbeeld iii. Laat $\mathbf{Q}$ de structuur zijn der rationale getallen met optelling en aftrekking, $\mathbf{Z}$ de substructuur van $\mathbf{Q}$ die de gehele getallen als domein heeft, en $\mathbf{N}$ de relatieve substructuur met de natuurlijke getallen als domein. We noteren

$$\langle \mathbf{N}, +, - \rangle \subset \langle \mathbf{Z}, +, - \rangle < \langle \mathbf{Q}, +, - \rangle,$$

zonder ons eraan te storen dat $+$ en $-$ in de drie structuren verschillende operaties zijn. Preciezere notatie, zeg

$$\langle \mathbf{N}, +|_{\mathbf{N}}, -|_{\mathbf{N}} \rangle \subset \langle \mathbf{Z}, +|_{\mathbf{Z}}, -|_{\mathbf{Z}} \rangle < \langle \mathbf{Q}, +, - \rangle,$$

is niet alleen van storende complexiteit, maar ook arbitrair. De optelling van rationale getallen is immers niet de meest algemene, er zijn ook reële getallen, en daar weer generalisaties van.

§C Homomorfismen

Het zou geen overdrijving zijn te stellen dat homomorfismen de belangrijkste vorm van gelijkenis belichamen tussen structuren.

1 DEFINITIE. Laat $\mathbf{A}$ en $\mathbf{B}$ structuren zijn. Een afbeelding $f: A \rightarrow B$ is een *homomorfisme* van $\mathbf{A}$ naar $\mathbf{B}$ als voor ieder operatiesymbool Q , voor elke familie $a \in \text{Dom } Q^{\mathbf{A}}$, $f(Q^{\mathbf{A}}(a)) = Q^{\mathbf{B}}(f \circ a)$.

(Omdat volgens conventie ‘ $\dots = N$ ’ alleen waar kan zijn als de uitdrukking ‘ N ’ betekenis heeft, impliceert deze definitie in het bijzonder

$$\text{als } a \in \text{Dom } Q^{\mathbf{A}}, \text{ dan } f \circ a \in \text{Dom } Q^{\mathbf{B}}.)$$

De verzameling van alle homomorfismen van $\mathbf{A}$ naar $\mathbf{B}$ duiden we aan met $[\mathbf{B} \leftarrow \mathbf{A}]$. We schrijven meestal $f: \mathbf{A} \rightarrow \mathbf{B}$ in plaats van $f \in [\mathbf{B} \leftarrow \mathbf{A}]$. Voor een klasse $\mathcal{K}$ van structuren definiëren we

$$[\mathcal{K} \leftarrow \mathbf{A}] := \bigcup_{\mathbf{K} \in \mathcal{K}} [\mathbf{K} \leftarrow \mathbf{A}].$$

Als $\mathbf{A} = \mathbf{B}$, dan heet $f: \mathbf{A} \rightarrow \mathbf{B}$ een *endomorfisme* van $\mathbf{A}$. In plaats van $[\mathbf{A} \leftarrow \mathbf{A}]$ schrijven we ook $\text{End } \mathbf{A}$. Een injectief homomorfisme wordt ook een *zwakke inbedding* genoemd. Voor zwakke inbeddingen gebruiken we de notatie

$$(1) \quad f: \mathbf{A} \hookrightarrow \mathbf{B}.$$

Analoog gebruiken we $\twoheadrightarrow$ en $\hookrightarrow$ om, respectievelijk, surjectiviteit en bijectiviteit aan te geven. In het surjectieve geval spreken we van een homomorfisme *op* $\mathbf{B}$.

Voorbeelden

i. Als $\mathbf{A} \subseteq \mathbf{B}$, dan is de kanonieke inbedding $1_B^{\mathbf{A}}$ een zwakke inbedding van $\mathbf{A}$ in $\mathbf{B}$.

ii. Laat A een verzameling zijn, $\mathbf{B}$ een structuur, en $f: A \rightarrow B$. Dan is f een homomorfisme van A naar $\mathbf{B}$.

iii. Laat $\mathbf{N} = \langle \mathbf{N}, +, - \rangle$ de benoemde versie zijn van de structuur in §A Voorbeeld (i); en $\mathbf{E}$ de structuur met domein $\{0, 1\}$ waarin zowel het optellings- als het aftrekkingssymbool wordt geïnterpreteerd als optelling modulo 2. Definieer

$$f, g: \mathbf{N} \rightarrow \{0, 1\}$$

door: $f(n) = 0 \triangleleft n \text{ is even} \triangleright 1;$
 $g(n) = 1 \triangleleft n \text{ is even} \triangleright 0.$

Dan is f een homomorfisme en g niet.

2 PROPOSITIE. Laat $\mathbf{A}$, $\mathbf{B}$ en $\mathbf{C}$ structuren zijn.

- (i) 1_A is een endomorfisme van $\mathbf{A}$.
- (ii) Als $f: \mathbf{A} \rightarrow \mathbf{B}$ en $g: \mathbf{B} \rightarrow \mathbf{C}$, dan is $g \circ f$ een homomorfisme van $\mathbf{A}$ naar $\mathbf{C}$.

Bewijs. (i) Triviaal.

(ii) Vanzelfsprekend is $g \circ f$ een afbeelding van A in C .

Als $a \in \text{Dom } Q^A$, dan $f(Q^A(a)) = Q^B(f \circ a)$ omdat f een homomorfisme is; en $g(Q^B(f \circ a)) = Q^C(g \circ f \circ a)$ omdat g een homomorfisme is. $\square$

3 DEFINITIE. Zij $f: \mathbf{A} \rightarrow \mathbf{B}$ een homomorfisme. Dan is $f[\mathbf{A}]$, het *beeld van $\mathbf{A}$ onder f* , de zwakke substructuur van $\mathbf{B}$ met domein $f[A]$ en operaties $Q^{f[\mathbf{A}]}$ gedefinieerd door

$$Q^{f[\mathbf{A}]}(b) \simeq f(Q^A(a)) \triangleleft b = f \circ a.$$

De definitie van $f[\mathbf{A}]$ is correct omdat f een homomorfisme is: voor alle a zo dat $b = f \circ a$ en $f(Q^A(a)) \downarrow$ (dat is, $a \in \text{Dom } Q^A$), $f(Q^A(a)) = Q^B(b)$. Merk op dat f ook een homomorfisme is van $\mathbf{A}$ naar $f[\mathbf{A}]$.

Een structuur $\mathbf{B}$ heet een *homomorf beeld* van een structuur $\mathbf{A}$ als er een homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ bestaat zo dat $f[\mathbf{A}] = \mathbf{B}$.

Voorbeeld iv. Zij k een positief geheel getal, $\mathbf{N} = \langle \mathbb{N}, +, - \rangle$ de structuur der gehele getallen met optelling en aftrekking (§A, Voorbeeld (i)), en $\mathbf{Z}_k = \langle Z_k, +', -' \rangle$, met $Z_k = \{0, \dots, k-1\}$, en $x +' y$ gedefinieerd als $x + y$ wanneer $x + y < k$, en anders $x + y - k$, en $x -' y = z$ dan en slechts dan als $x = y +' z$. Definieer f op $\mathbf{N}$ door

$$f(n) \text{ is de unieke } x \in Z_k \text{ waarvoor } y \in \mathbb{N} \text{ bestaat zo dat } n = yk + x.$$

(Dus $f(n)$ is de rest bij deling van n door k . In de programmeertalen C en Java wordt $f(n)$ genoteerd als $n \% k$.) Dan $\mathbf{Z}_k = f[\mathbf{N}]$; $\mathbf{Z}_k$ is dus een homomorf beeld van $\mathbf{N}$.

§D Kategorieën

Een *kategorie* is een structuur bestaande uit een klasse met een binaire operatie $\circ$ (*samenstelling*) en een deelklasse E (de klasse der *eenheidselementen*), die voldoet aan de volgende axioma's:

1. Voor alle elementen x, y en z , $(x \circ y) \circ z \simeq x \circ (y \circ z)$. (*Associatieve wet*)
2. Voor alle x, y en z , als $x \circ y$ en $y \circ z$ bestaan, dan bestaat $(x \circ y) \circ z$.
3. Voor alle x en alle $e \in E$, $x \circ e \simeq x$ en $e \circ x \simeq x$.
4. Voor elke x bestaan $d, e \in E$ zo dat $x \circ d$ en $e \circ x$ bestaan.

Een kategorie heet *klein* als haar domein een verzameling is. Een kategorie die niet klein is, is *groot*. (Of, in de algemene terminologie: bovenmaats.)

Formeel hebben we hier van doen met structuren $\langle A, \mathcal{I} \rangle$ waarin $\mathcal{I}$ aan een vast binair operatiesymbool $\circ$ een binaire operatie $\mathcal{I}(\circ)$ over A toekent, en aan een vast unair operatiesymbool E een unaire operatie $\mathcal{I}(E)$ over A die voldoet aan de *relatiewet*

$$\mathcal{I}(E)(x) \simeq x \quad (\text{Rel}).$$

In de praktijk zullen we voor een symbool en zijn interpretatie vaak hetzelfde teken gebruiken.

Op grond van de associatieve wet kunnen we haakjes in complexe samenstellingen achterwege laten. Evenals het vermenigvuldigingssymbool $\cdot$ wordt het samenstellingssymbool $\circ$ vaak onderdrukt.

Als $x = y \circ z$, dan heten y en z *factoren* van x ; we zeggen ook dat x *factoriseert door* y en z .

1 PROPOSITIE. Voor ieder element x van een kategorie is er precies één eenheidselement d zo dat $x \circ d$ bestaat, en precies één eenheidselement e zo dat $e \circ x$ bestaat.

BEWIJS. Zij d een eenheidselement zo dat $x \circ d$ bestaat. Zulke d moeten er zijn, volgens axioma 4. Laat nu d' een willekeurig eenheidselement zijn waarvoor $x \circ d'$ gedefinieerd is. Dan impliceren de axioma's 3 en 1 dat

$$x \circ d' = (x \circ d) \circ d' = x \circ (d \circ d'),$$

dus $d \circ d'$ bestaat volgens de strichtheidswet. Omdat d en d' eenheidselementen zijn, hebben we

$$d = d \circ d' = d'.$$

Analoog kan men de uniciteit bewijzen van het eenheidselement e waarvoor $e \circ x$ gedefinieerd is. $\square$

Als d en e eenheidselementen zijn zo dat $(d \circ x \circ e) \downarrow$, dan noteren we ook wel $x: d \leftarrow e$ of $x: e \rightarrow d$.

Voorbeelden

i. De klasse *Rel* van alle drietallen $\langle Y, R, X \rangle$ bestaande uit verzamelingen Y en X en een relatie $R \subseteq Y \times X$ is het universum van een grote kategorie **Rel** waarin samenstelling is gedefinieerd door

$$\langle W, S, Z \rangle \circ \langle Y, R, X \rangle \simeq \langle W, S \circ R, X \rangle \triangleleft Z = Y,$$

en de eenheidselementen de drietallen $\langle X, \Delta_X, X \rangle$ zijn.

ii. De paren $\langle Y, f \rangle$ van een verzameling Y en een functie f waarvan het beeld bevat is in Y vormen de grote kategorie **Vrz**, met samenstelling gedefinieerd door

$$\langle Z, g \rangle \circ \langle Y, f \rangle \simeq \langle Z, g \circ f \rangle \triangleleft \text{Dom } g = Y;$$

en eenheidselementen $\langle X, 1_X \rangle$.

iii. Propositie 2 van §C impliceert het bestaan van een kategorie **Str** (*structuren*) van homomorfismen. Om precies te zijn, de elementen van **Str** zijn de drietallen $\langle \mathbf{B}, f, \mathbf{A} \rangle$ waarin $\mathbf{B}$ en $\mathbf{A}$ 'kleine' structuren zijn, met *verzamelingen* als domein en type, en $f: \mathbf{B} \leftarrow \mathbf{A}$ een homomorfisme is. Drietallen zijn samenstelbaar als ze aanpalende elementen gemeen hebben, dat wil zeggen,

$$(1) \quad \langle \mathbf{D}, g, \mathbf{C} \rangle \circ \langle \mathbf{B}, f, \mathbf{A} \rangle \text{ bestaat} \Leftrightarrow \mathbf{C} = \mathbf{B},$$

en de samengestelde is dan $\langle \mathbf{D}, g \circ f, \mathbf{A} \rangle$. Eenheidselementen zijn drietallen van de vorm $\langle \mathbf{A}, 1_{\mathbf{A}}, \mathbf{A} \rangle$.

— In de praktijk houden we de buitenleden van drietallen als in Voorbeelden (i) en (iii) gewoonlijk impliciet. Ze zijn wel van wezensbelang, zoals blijkt uit (1).

iv. 0 is de lege kategorie. Het domein is de lege verzameling, er zijn dus ook geen eenheidselementen, en de samenstelling is de lege operatie.

v. 1 is de kategorie met één element; dat moet dan een eenheidselement zijn.

vi. 2 is de kategorie met twee eenheidselementen d, e , en één niet-eenheidselement f zo dat $dfe \downarrow$.

vii. 3 is de kategorie met drie eenheidselementen c, d, e , en drie niet-eenheidselementen f, g, h zo dat $cf dge = h$. Enzovoort, langs alle natuurlijke getallen.

viii. $\Downarrow$ is de categorie met twee eenheidselementen d, e , en twee niet-eenheidselementen f, g zo dat $dfe \downarrow$ en $dge \downarrow$.

ix. $\searrow \swarrow$ is de categorie met drie eenheidselementen c, d, e , en twee niet-eenheidselementen f, g zo dat $cf d \downarrow$ en $cge \downarrow$.

x. $\swarrow \searrow$ is de categorie met drie eenheidselementen c, d, e , en twee niet-eenheidselementen f, g zo dat $cfe \downarrow$ en $dge \downarrow$.

xi. Een categorie $\mathbf{C}$ is *discreet* als $E^{\mathbf{C}} = C$.

2 Dualiteit. De *tegengestelde* of *duale* van een categorie $\mathbf{C} = \langle C, \circ, E \rangle$ is de structuur $\mathbf{C}^{\partial} = \langle C, \bullet, E \rangle$ waarin $\bullet$ de binaire operatie is gedefinieerd door

$$c \bullet d \simeq d \circ c.$$

De duale van een categorie is weer een categorie. Daaruit volgt het *dualiteitsprincipe* voor categorieën: als we in een bewering S die geldt voor alle categorieën de samenstellingen omdraaien, dan is het resultaat nog steeds geldig.

Kategorieën zijn niet de enige soort van dualiseerbare structuren. Als P en Q begrippen zijn, gedefinieerd in een of ander soort van dualiseerbare structuren, dan is Q de *duale van P* als voor elke structuur $\mathbf{A}$ van de beoogde soort de denotatie van Q in $\mathbf{A}$ precies de denotatie is van P in $\mathbf{A}^{\partial}$. In de categorieëentheorie heet het aan P duale begrip vaak *co- P* . Een voorbeeld daarvan is het begrippenpaar domein-codomein dat hieronder wordt ingevoerd. Een begrip dat zijn eigen duale is, heet *zelfduaal*. Bijvoorbeeld: in categorieën is E (het begrip ‘eenheidselement’) zelfduaal.

3 Domein en Bestemming. Categorieën kunnen ook worden opgezet als structuren

$$\langle C, \circ, d, b \rangle,$$

waarin de klasse der eenheidselementen vervangen is door twee unaire operaties: d (*domeineenheid*) en b (*bestemmingseenheid*). In de plaats van de axioma's 2-4 komen

2'. $x \circ y$ bestaat dan en slechts dan als $d(x) = b(y)$.

3'. $y \circ d(y) = y = b(y) \circ y$.

4'. Als $x \circ y$ bestaat, dan $d(x \circ y) = d(y)$ en $b(x \circ y) = b(x)$.

3.1 LEMMA. In een structuur die voldoet aan de axioma's 2'-4' geldt:

(i) de operaties d en b zijn totaal;

en voor alle x , (ii) $d(d(x)) = b(d(x)) = d(x)$, en

(iii) $b(b(x)) = d(b(x)) = b(x)$.

BEWIJS. (i) Neem een willekeurig element y . Volgens axioma 3' bestaat $y \circ d(y)$, en dat kan alleen als $y \in \text{Dom } d$. Insgelijks voor b .

(ii) Volgens axioma 3' bestaat $x \circ d(x)$, dus $d(x) = b(d(x))$ volgens axioma 2'. Evenzo bestaat $b(d(x)) \circ d(x)$, dus $d(x) \circ d(x)$ bestaat. Nu volgt uit axioma 2' dat $d(d(x)) = b(d(x))$.

(iii) Analoog aan (ii). ☒

3.2 STELLING. De twee definities van categorieën zijn equivalent. Om precies te zijn,

1° in een categorie volgens de eerste definitie, met eenheidselementen, kunnen operaties d en b worden gedefinieerd die voldoen aan de axioma's 2'-4';

2° in een categorie volgens de tweede definitie, met domein- en bestemmingsoperaties, kunnen eenheidselementen worden gedefinieerd die voldoen aan de axioma's 2-4.

Bewijs. 1° Stel dat de axioma's 1-4 gelden in een structuur **C**. Volgens Propositie 1 bestaat er voor elke $c \in C$ een uniek eenheidselement d zo dat $c \circ d$ bestaat. Definieer $d(c)$ als dat eenheidselement. Definieer analoog $b(c)$ als het eenheidselement b zo dat $b \circ c$ bestaat. Dan volgt axioma 3' onmiddellijk uit axioma 3.

Als $x \circ y$ bestaat, dan bestaat $(x \circ d(x)) \circ (b(y) \circ y)$ ook. Dus volgens axioma 1 bestaat $(x \circ (d(x) \circ b(y))) \circ y$, wat impliceert dat $d(x) \circ b(y)$ bestaat. Omdat $d(x)$ en $b(y)$ eenheidselementen zijn, $d(x) = d(x) \circ b(y) = b(y)$. Daarmee is één richting van 2' geverifieerd. Veronderstel voor de andere richting dat $d(x) = b(y) = e$. Dan bestaan $x \circ e$ en $e \circ y$, dus volgens axioma 2 bestaat $(x \circ e) \circ y$, en omdat e een eenheidselement is, $(x \circ e) \circ y = x \circ y$.

Axioma 4' volgt uit de gelijkheden

$$(x \circ y) \circ d(y) = x \circ y \quad \text{en} \quad b(x) \circ (x \circ y) = x \circ y,$$

omdat per definitie $d(x \circ y)$ het *unieke* eenheidselement d is zo dat

$$(x \circ y) \circ d = x \circ y,$$

en $b(x \circ y)$ het unieke eenheidselement e zo dat $e \circ (x \circ y) = x \circ y$.

2° Omgekeerd, stel dat de axioma's 1, 2', 3' en 4' gelden in een structuur **D**. Als $x \circ y$ en $y \circ z$ bestaan, dan geldt volgens 4' en 2' dat $d(x \circ y) = d(y) = b(z)$, dus volgens 2' bestaat $(x \circ y) \circ z$. Daarmee is axioma 2 bewezen.

Definieer E als het beeld van d . Stel dat $e \in E$, zeg $e = d(x)$. Als $y \circ e$ bestaat, dan $d(y) = b(e) = b(d(x)) = d(x) = e$ volgens axioma 2' en Lemma 3.1. Dus $y \circ e = y$ volgens axioma 3'. Analoog bewijst men $e \circ z = z$ uit het bestaan van $e \circ z$. Daarmee is axioma 3 bewezen.

Axioma 4, tenslotte, geldt omdat volgens Lemma 3.1 voor elke x , zowel $d(x)$ als $b(x)$ tot $\text{Im}(d)$ behoort. $\square$

De duale van een categorie $\mathbf{C} = \langle C, \circ, d, b \rangle$ is $\mathbf{C}^\partial = \langle C, \bullet, b, d \rangle$, waar $\bullet$ is gedefinieerd als in item 2. Merk op dat d en b verwisseld zijn. Bij het dualiseren van een bewering over domein-en-bestemming-kategorieën moeten we dus ook overal d substitueren voor b en vice versa.

4 Gerichtte grafen. Een (gerichte) *graaf* is een structuur $\mathbf{X} = \langle X, d, b \rangle$ waarin d en b unaire operaties zijn die voldoen aan

$$\begin{aligned} d(x) \downarrow & \text{ dan en slechts dan als } b(x) \downarrow; \\ dd(x) \uparrow & \text{ en } bb(x) \uparrow. \end{aligned}$$

De elementen van $\text{Dom}(d)$ zijn de *kanten*; de andere elementen zijn de *knopen* van de graaf. De *paden*, rijtjes van aansluitende knopen en kanten, vormen een categorie. (Zie Oefening 4.)

5 Objecten. Kategorieën als in de Voorbeelden (i) en (iii), bestaande uit drietallen die samenstelbaar zijn als hun aansluitende elementen overeenkomen, of als in Voorbeeld (ii), waar zulke drietallen eenvoudig kunnen worden geconstrueerd, komen veel voor. De buitenste elementen worden *objecten* genoemd. Dikwijls heten zulke categorieën naar hun objecten. (Dat kan verwarrend zijn: we hadden bijvoorbeeld **Rel** net zo goed naar verzamelingen kunnen noemen als **Vrz**.) Objecten corresponderen één op één met eenheidselementen. We kunnen dus in *elke* categorie van objecten spreken. We noteren de klasse der objecten van een categorie **C** als Ob C . Het eenheidselement behorend bij het object x schrijven we als 1_x . (Die notatie is al ingevoerd voor het bijzondere geval van de identieke afbeelding van een verzameling op zichzelf, in 1§H1.)

De eigenlijke elementen van een categorie noemt men ook wel — en in het bijzonder als er sprake is van objecten — *pijlen* of *morfismen*. Een pijl gaat van

een object, zijn *domein*, naar een object, zijn *codomein*. Bijvoorbeeld, een pijl $\langle Y, f \rangle \in \mathbf{Vrz}$ heeft codomein Y , en domein $\text{Dom} f$; als $\text{Dom} f = X$, dan schrijven we

$$f: Y \leftarrow X$$

of $f: X \rightarrow Y$. We schrijven $X = \text{dom}(Y, f)$, en $Y = \text{cod}(Y, f)$.

Laat x en y objecten zijn van een categorie $\mathbf{C}$; dan noteren we de klasse van alle pijlen van x naar y in $\mathbf{C}$, de *homklasse* van x naar y , als $[y \leftarrow x]^{\mathbf{C}}$ of $\mathbf{C}[y \leftarrow x]$.⁴ Als het niet nodig is om $\mathbf{C}$ te noemen, schrijven we in plaats van $f \in \mathbf{C}[y \leftarrow x]$ meestal $f: y \leftarrow x$ of $f: x \rightarrow y$. In de tweede alinea van deze § onderscheiden we tussen grote en kleine categorieën; dit is het moment om een tussenmaat, of misschien eerder een vorm van bescheidenheid bij grote categorieën, te vermelden. Een categorie $\mathbf{C}$ heet *locaal klein* als voor elk paar van objecten x en y , $\mathbf{C}[y \leftarrow x]$ een verzameling is. Voorbeelden van lokaal kleine categorieën zijn **Rel** en **Vrz**. Merk op dat

$$[x \leftarrow z]^{\mathbf{C}^{\partial}} = [z \leftarrow x]^{\mathbf{C}}.$$

We kunnen homklassen overigens ook definiëren voor eenheidselementen in plaats van objecten, en zelfs voor willekeurige pijlen:

$$[y \leftarrow x]^{\mathbf{C}} = \mathbf{C}[y \leftarrow x] = \{z \in \mathbf{C} \mid (y \circ z \circ x) \downarrow\}.$$

Formeel is een categorie-met-objecten een tweesoortige structuur $\mathbf{C}$ met (disjuncte) soorten $\text{Ob} \mathbf{C}$ en $\text{Pijl} \mathbf{C}$. Er zijn operaties

$$\circ: \text{Pijl} \times \text{Pijl} \rightarrow \text{Pijl},$$

$$\text{dom}: \text{Pijl} \rightarrow \text{Ob},$$

$$\text{cod}: \text{Pijl} \rightarrow \text{Ob}, \text{ en}$$

$$1_{_}: \text{Ob} \rightarrow \text{Pijl},$$

die voldoen aan Axioma 1 en

$$2''. f \circ g \text{ bestaat dan en slechts dan als } \text{dom}(f) = \text{cod}(g);$$

$$3''. f \circ 1_{\text{dom}(f)} = f = 1_{\text{cod}(f)} \circ f;$$

$$4''. \text{ als } f \circ g \text{ bestaat, dan } \text{dom}(f \circ g) = \text{dom}(g) \text{ en } \text{cod}(f \circ g) = \text{cod}(f);$$

$$5. \text{dom}(1_X) = X = \text{cod}(1_X).$$

5.1 LEMMA. Laat x en y objecten zijn in een tweesoortige categorie. Dan

$$x = y \Leftrightarrow 1_x = 1_y.$$

BEWIJS. ($\Rightarrow$) Triviaal.

($\Leftarrow$) Als $1_x = 1_y$, dan $x = \text{dom}(1_x) = \text{dom}(1_y) = y$, volgens Axioma 5. $\square$

Uit het lemma volgt dat als we voor pijlen f definiëren

$$\mathbf{d}(f) = 1_{\text{dom}(f)} \text{ en } \mathbf{b}(f) = 1_{\text{cod}(f)}$$

en de objecten verder vergeten, voldaan is aan de axioma's in sectie 4. Andersom kunnen we van een eensoortige categorie een tweesoortige maken door bij ieder eenheidselement e een object e' te hypostaseren, en te definiëren

$$\text{dom}(x) = \mathbf{d}(x)', \text{ cod}(x) = \mathbf{b}(x)',$$

$$1_{e'} = e.$$

⁴ De notatie $[X \rightarrow Y]$ is tamelijk standaard.

6 Functoren

Een homomorfisme tussen categorieën wordt gewoonlijk een *functor* genoemd. Nu hebben wij drie definities van categorieën gegeven; er zijn dus ook drie definities van *functor*. We zullen echter zien dat die op hetzelfde neerkomen. (Verderop zullen we algemene principes bespreken waaruit dat volgt. Voor het moment gaat het behalve om de inhoud vooral om de illustratie van het begrip ‘homomorfisme’.)

6.1 PROPOSITIE. Laat $\mathbf{A} = \langle A, \circ^{\mathbf{A}}, \mathbf{E}^{\mathbf{A}} \rangle$ en $\mathbf{B} = \langle B, \circ^{\mathbf{B}}, \mathbf{E}^{\mathbf{B}} \rangle$ categorieën zijn, en F een functor van $\mathbf{A}$ naar $\mathbf{B}$. Definieer operaties $d^{\mathbf{A}}$ en $b^{\mathbf{A}}$ op A door

$$\begin{aligned} x = d^{\mathbf{A}}(f) &\Leftrightarrow x \in \mathbf{E}^{\mathbf{A}} \text{ en } f \circ^{\mathbf{A}} x = f, \\ x = b^{\mathbf{A}}(f) &\Leftrightarrow x \in \mathbf{E}^{\mathbf{A}} \text{ en } x \circ^{\mathbf{A}} f = f, \end{aligned}$$

en analoog operaties $d^{\mathbf{B}}$ en $b^{\mathbf{B}}$ op B . Dan is F een homomorfisme van $\langle A, \circ^{\mathbf{A}}, d^{\mathbf{A}}, b^{\mathbf{A}} \rangle$ naar $\langle B, \circ^{\mathbf{B}}, d^{\mathbf{B}}, b^{\mathbf{B}} \rangle$.

BEWIJS. Uit Propositie 1 volgt dat de pijlen $d^{\mathbf{A}}(f)$ en $b^{\mathbf{A}}(f)$ voor elke $f \in A$ uniek bepaald zijn; en een analoge bewering voor $d^{\mathbf{B}}$ en $b^{\mathbf{B}}$.

Zij $x = d^{\mathbf{A}}(f)$. Dan $x \in \mathbf{E}^{\mathbf{A}}$, dus $Fx \in \mathbf{E}^{\mathbf{B}}$. Bovendien

$$Ff = F(f \circ^{\mathbf{A}} x) = Ff \circ^{\mathbf{B}} Fx,$$

dus $F(d^{\mathbf{A}}(f)) = Fx = d^{\mathbf{B}}(Ff)$. Analoog (dual) voor b . □

6.2 PROPOSITIE. Laat $\mathbf{A} = \langle A, \circ^{\mathbf{A}}, d^{\mathbf{A}}, b^{\mathbf{A}} \rangle$ en $\mathbf{B} = \langle B, \circ^{\mathbf{B}}, d^{\mathbf{B}}, b^{\mathbf{B}} \rangle$ categorieën zijn, en F een functor van $\mathbf{A}$ naar $\mathbf{B}$. Laat $\text{Ob}\mathbf{A}$ en $\text{Ob}\mathbf{B}$ klassen zijn disjunct met, respectievelijk, A en B ; laat $\phi^{\mathbf{A}}: \text{Im}d^{\mathbf{A}} \rightarrow \text{Ob}\mathbf{A}$ en $\phi^{\mathbf{B}}: \text{Im}d^{\mathbf{B}} \rightarrow \text{Ob}\mathbf{B}$ bijecties zijn. Definieer voor $f \in A$

$$\text{dom}^{\mathbf{A}}(f) = \phi^{\mathbf{A}}(d^{\mathbf{A}}(f)), \quad \text{cod}^{\mathbf{A}}(f) = \phi^{\mathbf{A}}(b^{\mathbf{A}}(f)),$$

en voor $x \in \text{Ob}\mathbf{A}$, $1_x^{\mathbf{A}} = (\phi^{\mathbf{A}})^{-1}(x)$; en definieer analoge operaties voor $\mathbf{B}$. Breid F uit tot een operatie F' op $A \cup \text{Ob}\mathbf{A}$ door de stipulatie

$$F'(x) = \phi^{\mathbf{B}}(F(1_x^{\mathbf{A}})).$$

Dan is F' een homomorfisme van de tweesoortige structuur

$$\langle \text{Ob}\mathbf{A}, A; \circ^{\mathbf{A}}, \text{dom}^{\mathbf{A}}, \text{cod}^{\mathbf{A}}, 1^{\mathbf{A}} \rangle$$

naar de tweesoortige structuur $\langle \text{Ob}\mathbf{B}, B; \circ^{\mathbf{B}}, \text{dom}^{\mathbf{B}}, \text{cod}^{\mathbf{B}}, 1^{\mathbf{B}} \rangle$.

BEWIJS. Per definitie beeldt F' objecten af naar objecten en pijlen naar pijlen. Het behoud van samenstellingen is triviaal: als $(f \circ^{\mathbf{A}} g) \downarrow$, dan

$$F'(f \circ^{\mathbf{A}} g) = F(f \circ^{\mathbf{A}} g) = Ff \circ^{\mathbf{B}} Fg = F'f \circ^{\mathbf{B}} F'g.$$

Zij $f \in A$; dan

$$\begin{aligned} F'(\text{dom}^{\mathbf{A}}(f)) &= F'(\phi^{\mathbf{A}}(d^{\mathbf{A}}(f))) = \phi^{\mathbf{B}}(F(1_{\phi^{\mathbf{A}}(d^{\mathbf{A}}(f)))}) && \text{per definitie,} \\ &= \phi^{\mathbf{B}}(F(d^{\mathbf{A}}(f))) && \text{omdat } 1^{\mathbf{A}} \text{ de inverse is van } \phi^{\mathbf{A}}, \\ &= \phi^{\mathbf{B}}(d^{\mathbf{B}}(F(f))) && \text{omdat } F \text{ een functor is,} \\ &= \text{dom}^{\mathbf{B}}(F'(f)) && \text{per definitie en omdat } F'(f) = F(f). \end{aligned}$$

Analoog $F'(\text{cod}^{\mathbf{A}}(f)) = \text{cod}^{\mathbf{B}}(F'(f))$. Tenslotte, voor $x \in \text{Ob}\mathbf{A}$

$$1_{F'x}^{\mathbf{B}} = (\phi^{\mathbf{B}})^{-1}(F'x) = (\phi^{\mathbf{B}})^{-1}(\phi^{\mathbf{B}}(F(1_x^{\mathbf{A}}))) = F(1_x^{\mathbf{A}}),$$

dus $F'(1_x^{\mathbf{A}}) = 1_{F'x}^{\mathbf{B}}$. □

6.3 PROPOSITIE. Laat

$\mathbf{A} = \langle \text{Ob } \mathbf{A}, \text{Pijl } \mathbf{A}; \circ^{\mathbf{A}}, \text{dom}^{\mathbf{A}}, \text{cod}^{\mathbf{A}}, 1^{\mathbf{A}} \rangle$ en $\mathbf{B} = \langle \text{Ob } \mathbf{B}, \text{Pijl } \mathbf{B}; \circ^{\mathbf{B}}, \text{dom}^{\mathbf{B}}, \text{cod}^{\mathbf{B}}, 1^{\mathbf{B}} \rangle$ categorieën zijn, en F een functor van $\mathbf{A}$ naar $\mathbf{B}$. Dan is $F \upharpoonright \text{Pijl } \mathbf{A}$ een homomorfisme van $\langle \text{Pijl } \mathbf{A}, \circ^{\mathbf{A}}, \text{Im } 1^{\mathbf{A}} \rangle$ naar $\langle \text{Pijl } \mathbf{B}, \circ^{\mathbf{B}}, \text{Im } 1^{\mathbf{B}} \rangle$.

BEWIJS. Het behoud van samenstellingen is triviaal; en eenheidselementen worden bewaard doordat $F(1_X^{\mathbf{A}}) = 1_{FX}^{\mathbf{B}}$. $\square$

Voorbeeld xii. Definieer, voor drietallen $\langle X, R, Y \rangle \in \mathbf{Rel}$:

$$\mathbf{P}(X, R, Y) = \langle \mathcal{P}X, R^{\mathcal{P}} \rangle,$$

waar de functie $R^{\mathcal{P}}$ gedefinieerd is op $\mathcal{P}Y$ door

$$R^{\mathcal{P}}(U) = R[U].$$

De operatie $\mathbf{P}$ is een functor van $\mathbf{Rel}$ naar $\mathbf{Vrz}$.

Een functor $F: \mathbf{C} \rightarrow \mathbf{D}$ is *getrouw* als voor alle $x, y \in \text{Ob } \mathbf{C}$ de restrictie van F tot $\mathbf{C}[y \leftarrow x]$ injectief is. Een getrouwe functor is dus een lokale injectie. We hebben ook een lokaal surjectiebegrip: de functor F is *vol* als voor alle $x, y \in \text{Ob } \mathbf{C}$ de restrictie van F tot $\mathbf{C}[y \leftarrow x]$ een surjectie is op $\mathbf{D}[Fy \leftarrow Fx]$.

Een substructuur van een categorie die een categorie is, heet een *subcategorie*. De onderstaande propositie volgt uit algemene principes, maar is op zichzelf niet moeilijk te bewijzen:

6.4 PROPOSITIE. Alle substructuren van categorieën van type $\{\circ, d, b\}$ of $\{\text{Ob}, \text{Pijl}; \circ, \text{dom}, \text{cod}, 1\}$ zijn categorieën.

Laat $\mathbf{A}$ en $\mathbf{B}$ categorieën zijn, $\mathbf{A} \leq \mathbf{B}$. Dan is de kanonieke inbedding $1_B^{\mathbf{A}}$ een getrouwe functor van $\mathbf{A}$ naar $\mathbf{B}$. Als $1_B^{\mathbf{A}}$ ook vol is, heet $\mathbf{A}$ een *volle* subcategorie van $\mathbf{B}$.

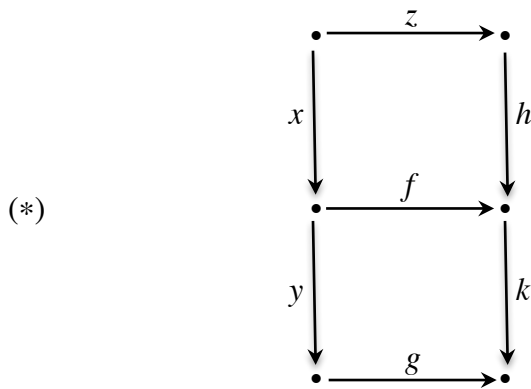
Voorbeeld xiii. De categorie $\mathbf{Vrz}$ (of, om precies te zijn, de variant van $\mathbf{Vrz}$ die pijlen $\langle Y, f, \text{Dom } f \rangle$ heeft in plaats van $\langle Y, f \rangle$) is een subcategorie van $\mathbf{Rel}$, maar geen volle.

Als $\mathbf{A}$ een subcategorie is van $\mathbf{B}$, dan is $\mathbf{A}^{\partial}$ een subcategorie van $\mathbf{B}^{\partial}$; is $\mathbf{A}$ vol, dan is $\mathbf{A}^{\partial}$ het ook.

Een *concrete categorie* is een paar $\langle \mathbf{C}, U \rangle$ van een categorie $\mathbf{C}$ en een getrouwe functor $U: \mathbf{C} \rightarrow \mathbf{Vrz}$. In typische gevallen is de functor U impliciet gegeven in de definitie van $\mathbf{C}$. Bijvoorbeeld, $\mathbf{Str}$ is een concrete categorie omdat homomorfismen van een structuur $\mathbf{A}$ naar een structuur $\mathbf{B}$ gedefinieerd zijn als afbeeldingen van de verzameling A naar de verzameling B die aan zekere extra eisen voldoen.

7 Diagrammen

Een *diagram* is een grafische weergave van een aantal pijlen (in een gegeven categorie) met hun domein en codomein. Bijvoorbeeld, het diagram



laat zien dat $\text{dom } x = \text{dom } z$, $\text{cod } x = \text{dom } y$, enzovoort.

Een diagram *commuteert* als de samengestelden met hetzelfde domein en hetzelfde codomein identiek zijn. In diagram (*) houdt dat in dat $f \circ x = h \circ z$ en $g \circ y = k \circ f$ — uit het commuteren van de beide *vierkanten* volgt het commuteren van de hele *rechthoek*.

§E Algebra's

Een structuur is een (ongesorteerde, éénsoortige, enkelsoortige) *algebra* als haar domein niet leeg is en al haar basisoperaties totaal zijn. Een niet-lege substructuur van een algebra is een algebra; we spreken dan van een *subalgebra*.

Voorbeeld i. Een *groepoïde* is een verzameling S met een totale binaire operatie $\cdot$ (product). Een groepoïde is een *halfgroep* als haar product associatief is.

Bijvoorbeeld, de verzameling $S = X^+$ der niet-lege rijtjes van elementen van een verzameling X , met concatenatie als productoperatie, is een halfgroep, de halfgroep der niet-lege *woorden over het alfabet* X . We noteren die woorden gewoonlijk *als woorden*, dat wil zeggen, zonder komma's, spaties of haakjes. Een woord w van lengte 4 is dus $w_0w_1w_2w_3$. Bovendien onderdrukken we het concatenatiesymbool, vw schrijvend in plaats van $v * w$. Dat kan allemaal zolang we voor willekeurige woorden andere letters gebruiken dan voor letters en één-letterwoorden; zoals u, v, w versus x, y, z .

Met samenstelling vormen de relaties (voorzover ze verzamelingen zijn) en de functies grote halfgroepen.

Een halfgroep $\langle S, \cdot \rangle$ is *commutatief* of *abels* als de productoperatie commutatief is:

$$\text{voor alle } x, y \in S, x \cdot y = y \cdot x.$$

Voor abelse halfgroepen gebruikt men soms *additieve* notatie. Men schrijft dan $+$ in plaats van $\cdot$. De algebra $\langle \mathbb{Z}_+, + \rangle$ is een concreet voorbeeld van een abelse halfgroep.

Het productsymbool $\cdot$ wordt, net als het samenstellingssymbool $\circ$, vaak weggelaten. Verder gebruikt men exponentnotatie voor herhaalde vermenigvuldiging. De inductieve definitie daarvan luidt: $x^1 = x$;

$$x^{n+1} = x^n \cdot x, \text{ voor } n \geq 1.$$

1 LEMMA. Zij $S = \langle S, \cdot \rangle$ een halfgroep, en $x \in S$. Voor $m, n \geq 1$ geldt:

$$x^m \cdot x^n = x^{m+n}.$$

BEWIJS. Inductie naar n . Als $n = 1$, dan $x^m \cdot x^n = x^m \cdot x = x^{m+1} = x^{m+n}$. Als $n = k + 1$, $k \geq 1$, dan

$$\begin{aligned} x^m \cdot x^n &= x^m \cdot x^k \cdot x = x^{m+k} \cdot x && \text{volgens inductiehypothese} \\ &= x^{m+n}. && \square \end{aligned}$$

Merk op dat het lemma impliceert dat $x^m \cdot x^n = x^n \cdot x^m$.

Als we additieve notatie gebruiken, schrijven we veelvouden in plaats van exponenten: nx in plaats van x^n .

ii. Een *monoïde* is een halfgroep $\langle M, \cdot \rangle$ met een *eenheidselement*, i.e. een element e zo dat voor alle $x \in M$: $xe = ex = x$. Een halfgroep van woorden met concatenatie wordt een monoïde wanneer we het lege woord ε toevoegen. Notatie:

$$X^* = X^+ \cup \{\varepsilon\}.$$

2 STELLING. Zij $\mathbf{A} = \langle A, \cdot, e \rangle$ een monoïde en f een afbeelding van een verzameling X naar het domein A . Dan bestaat er precies één homomorfisme f^* van de monoïde $\mathbf{X}^* = \langle X^*, *, \varepsilon \rangle$ naar $\mathbf{A}$ dat f uitbreidt.

BEWIJS. Zo'n homomorfisme zou moeten voldoen aan de clausules

$$\begin{aligned} (*) \quad & f^*(\varepsilon) = e, \\ & f^*(wx) = f^*(w) \cdot f(x) \quad \text{voor } w \in X^* \text{ en } x \in X. \end{aligned}$$

Merk op dat $(*)$ een afbeelding van X^* naar A definieert; de uniciteit van f^* is daardoor gegarandeerd. Rest slechts te bewijzen dat f^* een f uitbreidend homomorfisme is.

1° Zij $x \in X$. Dan $f^*(x) = f^*(\varepsilon x) = f^*(\varepsilon) \cdot f(x) = e \cdot f(x) = f(x)$. Dus $f^* \supseteq f$.

2° Per definitie $f^*(\varepsilon) = e$. We bewijzen dat $f^*(vw) = f^*(v) \cdot f^*(w)$ met inductie naar de lengte van w .

— $f^*(v\varepsilon) = f^*(v) = f^*(v) \cdot e = f^*(v) \cdot f^*(\varepsilon)$.

— Stel dat $w = ux$ en $f^*(vu) = f^*(v) \cdot f^*(u)$. Dan

$$\begin{aligned} f^*(vw) &= f^*(vux) = f^*(vu) \cdot f(x) && \text{volgens } (*) \\ &= f^*(v) \cdot f^*(u) \cdot f(x) && \text{volgens inductiehypothese} \\ &= f^*(v) \cdot f^*(w) && \text{volgens } (*). \end{aligned}$$

Dus f^* is inderdaad een homomorfisme. $\square$

Vanwege deze opmerkelijke eigenschap heet $\mathbf{X}^*$, in terminologie waar we nog op terug zullen komen, de *vrije monoïde voortgebracht door X*.

Met samenstelling als operatie vormen de binaire relaties over een verzameling X een monoïde. Hetzelfde geldt voor de afbeeldingen van X naar zichzelf. Een monoïde heet *commutatief* (abels) als haar halfgroepproduct commutatief is; een concreet voorbeeld is $\langle \mathbb{N}, +, 0 \rangle$.

Voor monoïden kunnen we de exponentnotatie uitbreiden met

$$x^0 = e.$$

Het is niet moeilijk het bewijs van Lemma 1 aan te passen, en dan hebben we

3 LEMMA. Zij $\mathbf{M} = \langle M, \cdot, e \rangle$ een monoïde, en $x \in M$. Voor alle $m, n \in \mathbb{N}$ geldt:

$$x^m \cdot x^n = x^{m+n}.$$

iii. Een productoperatie over een verzameling X is *idempotent* als $xx = x$, voor alle $x \in X$. Een *halftralie* is een commutatieve halfgroep waarin het product idempotent is. De operatie van een halftralie wordt vaak aangeduid met $\vee$ of $\wedge$ in plaats van het vermenigvuldigingsteken $\cdot$.

iv. Een *inverse* van een element x in een monoïde is een element x^{-1} zodanig dat $x \cdot x^{-1} = x^{-1} \cdot x = e$. Zo'n inverse is uniek: als y en z inversen zijn van x , dan

$$y = y \cdot e = y \cdot x \cdot z = e \cdot z = z.$$

Uit de definitie van inverse volgt dus

$$x^{-1} \downarrow \Rightarrow (x^{-1})^{-1} = x.$$

Een *groep* is een monoïde $\langle G, \cdot, e \rangle$ waarin ieder element een inverse heeft. De *permutaties* van een verzameling X , d.i. de bijecties van X op X , vormen met functiesamenstelling als productoperatie een groep, de *symmetriegroep* S_X .

4 STELLING. Laat $\mathbf{G} = \langle G, \cdot, {}^{-1}, d \rangle$ en $\mathbf{H} = \langle H, \cdot, {}^{-1}, e \rangle$ groepen zijn.⁵ Ieder homomorfisme van $\langle G, \cdot \rangle$ naar $\langle H, \cdot \rangle$ is ook een homomorfisme van $\mathbf{G}$ naar $\mathbf{H}$.

BEWIJS. Zij $f: \langle G, \cdot \rangle \rightarrow \langle H, \cdot \rangle$ een homomorfisme. Het eenheidselement is het enige idempotente element van $\mathbf{H}$; want als $xx = x$, dan

$$x = x \cdot x \cdot x^{-1} = x \cdot x^{-1} = e.$$

Dus $f(d) = e$. Bovendien zijn inversen uniek bepaald; dus omdat

$$f(u) \cdot f(u^{-1}) = f(d) = e,$$

$$f(u^{-1}) = f(u)^{-1}.$$

☐

In het bijzonder fixeert de definitie van de symmetriegroep S_X haar eenheidselement en haar inversie-operatie.

In een groep definiëren we negatieve exponenten door

$$x^{-n} = (x^{-1})^n.$$

5 LEMMA. Zij $\mathbf{G} = \langle G, \cdot, {}^{-1}, e \rangle$ een groep, $x \in G$, en $n \in \mathbb{N}$. Dan

$$x^{-n} = (x^n)^{-1}.$$

BEWIJS. Met inductie naar n tonen we aan dat $x^{-n} \cdot x^n = e$. Daaruit volgt onze bewering: $x^{-n} = x^{-n} \cdot e = x^{-n} \cdot x^n \cdot (x^n)^{-1} = e \cdot (x^n)^{-1} = (x^n)^{-1}$.

Als $n = 0$, dan $x^{-n} = e = e^{-1}$. Als $n = k + 1$, dan

$$\begin{aligned} x^{-n} \cdot x^n &= (x^{-1})^n \cdot x^n \\ &= (x^{-1})^k \cdot x^{-1} \cdot x \cdot x^k && \text{volgens Lemma 3} \\ &= (x^{-1})^k \cdot e \cdot x^k = x^{-k} \cdot x^k = e \end{aligned}$$

volgens inductiehypothese.

☐

Nu kunnen we Lemma 1 verder uitbouwen.

6 LEMMA. Zij $\mathbf{G} = \langle G, \cdot, {}^{-1}, e \rangle$ een groep, en $x \in G$. Voor $z, z' \in \mathbb{Z}$ geldt:

$$x^z \cdot x^{z'} = x^{z+z'}.$$

BEWIJS. Als z en z' beide niet-negatief zijn, of beide negatief, volgt de bewering direct uit Lemma 3. Als $z = m$ en $z' = -n$ ($m, n \in \mathbb{N}$), en $m \geq n$, dan

⁵ De operaties $\cdot$ en ${}^{-1}$ van $\mathbf{G}$ worden hier — natuurlijk — evenmin verondersteld dezelfde te zijn als die van $\mathbf{H}$ als de eenheidselementen; maar het zou te veel moeite kosten om verschillende notaties in te voeren.

$$\begin{aligned}
 x^z \cdot x^{z'} &= x^{m-n} \cdot x^n \cdot x^{-n} && \text{volgens Lemma 3} \\
 &= x^{m-n} \cdot e && \text{volgens Lemma 5} \\
 &= x^{z+z'}.
 \end{aligned}$$

Als $m < n$, dan redeneren we analoog via $x^z \cdot x^{z'} = x^m \cdot x^{-m} \cdot x^{m-n}$. De resterende gevallen ruimen we op door substitutie: $x^{-m} \cdot x^n = (x^{-1})^m \cdot (x^{-1})^{-n}$. $\square$

De operaties van een abelse groep worden vaak additief geschreven: naast $+$ hebben we dan 0 en $-$ in plaats van e (of 1) en $^{-1}$. Een bekende abelse groep is de groep $\mathbf{Z} = \langle \mathbb{Z}, +, -, 0 \rangle$ der gehele getallen. (Het minteken is hier éénplaatsig.)

7 STELLING. Zij $\mathbf{G} = \langle G, \cdot, ^{-1}, e \rangle$ een groep, en $x \in G$. Er bestaat precies één homomorfisme $f: \mathbf{Z} \rightarrow \mathbf{G}$ zo dat $f(1) = x$.

BEWIJS. Voor iedere $z \in \mathbb{Z}$ is de exponent x^z eenduidig gedefinieerd. We beweren nu dat de afbeelding

$$f: z \mapsto x^z$$

een homomorfisme is. Inderdaad geldt volgens Lemma 6 dat

$$f(z + z') = f(z) \cdot f(z'),$$

en volgens Stelling 4 is dat genoeg.

Als $h: \mathbf{Z} \rightarrow \mathbf{G}$ en $h(1) = x$, dan $h(-1) = x^{-1}$; men bewijst nu eenvoudig, inductief, dat $h(z) = h(x^z)$, en dus $h = f$. $\square$

In de terminologie van de opmerking onder Stelling 2 heet $\mathbf{Z}$ de *vrije groep op één voortbrenger*. In Stelling 7 is 1 de voortbrenger; we hadden ook -1 kunnen nemen.

Voorbeelden

v. Een *ring* is een algebra $\mathbf{R} = \langle R, +, 0, -, \cdot \rangle$ waarvan het reduct $\langle R, +, 0, - \rangle$ een abelse groep is en het reduct $\langle R, \cdot \rangle$ een halfgroep, en waarin de volgende *distributieve wetten* gelden:

$$\text{voor alle } x, y, z \in R, x \cdot (y + z) = xy + xz \text{ en } (x + y) \cdot z = xz + yz.$$

Een *eenheidselement* van $\mathbf{R}$ is een eenheidselement van $\langle R, \cdot \rangle$, en $\mathbf{R}$ heet *commutatief* als $\cdot$ commutatief is. Een bekende commutatieve ring met eenheidselement is de ring $\mathbf{Z} = \langle \mathbb{Z}, +, 0, -, \cdot \rangle$ der gehele getallen.

vi. Een ring $\mathbf{R}$ met eenheidselement 1 is een *delingsring* als $\langle R \setminus \{0\}, \cdot, 1 \rangle$ een groep is. Het is gebruikelijk om de inversie-operatie van de *multiplicatieve groep* $\langle R \setminus \{0\}, \cdot, 1 \rangle$ van $\mathbf{R}$ *niet* tot de basisoperaties van $\mathbf{R}$ te rekenen. Doen we dat wel, dan zijn delingsringen geen algebra's. Een *lichaam* is een commutatieve delingsring. De structuur $\langle \mathbb{Q}, +, 0, -, \cdot, 1 \rangle$ der rationale getallen is een lichaam.

vii. Een *tralie* is een algebra $\langle L, \vee, \wedge \rangle$ waarin $\langle L, \vee \rangle$ en $\langle L, \wedge \rangle$ halftralies zijn, en de beide operaties — de eerste heet *voeg* en de tweede *moet* — zijn verbonden door de *absorptiewetten*:

$$x \wedge (x \vee y) = x; \quad x \vee (x \wedge y) = x.$$

Een tralie $\mathbf{L} = \langle L, \vee, \wedge \rangle$ is *boven begrensd* als het een eenheidselement voor de moet bevat, en *beneden begrensd* als het een eenheidselement heeft voor de voeg. De gebruikelijke notatie voor het eerste eenheidselement is 1 : $x \wedge 1 = x$ voor alle $x \in L$; en voor het tweede 0 : $x \vee 0 = x$ voor alle $x \in L$. We noemen een tralie $\mathbf{L}$ *begrensd* als het zowel boven als beneden begrensd is.

viii. Een tralie $\langle L, \vee, \wedge \rangle$ is *distributief* als voor alle $x, y, z \in L$,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad (1),$$

of equivalent, voor alle $x, y, z \in L$,

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad (2).$$

De deelverzamelingen van een gegeven verzameling K vormen een distributief tralie, met vereniging en doorsnede als operaties.

ix. Zij $\langle L, \vee, \wedge \rangle$ een begrensd distributief tralie. Een *complement* van $x \in L$ is een element y van L zo dat $x \vee y = 1$ en $x \wedge y = 0$. De definitie impliceert dat als x het complement is van y , y het complement is van x .

8 PROPOSITIE. Een element van een begrensd distributief tralie heeft hoogstens één complement.

BEWIJS. Laat y en z complementen zijn van x in een begrensd distributief tralie $L = \langle L, \vee, \wedge, 0, 1 \rangle$. Dan

$$y = y \wedge 1 = y \wedge (x \vee z) = (y \wedge x) \vee (y \wedge z) = 0 \vee (y \wedge z) = y \wedge z,$$

en analoog $z = z \wedge y$. ☒

Voorbeeld x. Een *Boole-algebra* is een begrensd distributief tralie waarin ieder element x een (uniek) complement $\neg x$ bezit.

Zij X een willekeurige verzameling. Dan is $\mathbf{PX} := \langle \mathcal{P}X, \cup, \cap, \emptyset, X, \neg \rangle$ een Boole-algebra, als we $\bar{A}$ definiëren als $X \setminus A$. De waarheidswaarden 0 (*onwaar*) en 1 (*waar*), met de operaties $\vee, \wedge$ en $\neg$ gedefinieerd door de tabellen

$\vee$	1	0
1	1	1
0	1	0

$\wedge$	1	0
1	1	0
0	0	0

$\neg$	$\neg x$
1	0
0	1

vormen de standaard-Boole-algebra **2**.

§F Relatieve stelsels

Een benoemde structuur $\mathbf{A}$ is een *relationeel stelsel* als voor elke $Q \in \text{Nom } \mathbf{A}$ van niet-lege plaatsigheid een element k^* van K_Q bestaat zo dat voor alle $a \in A^{K_Q}$, $Q(a) \simeq a_{k^*}$. In wezen is een relationeel stelsel een drietal $\mathbf{A} = \langle A, R, C \rangle$ van een verzameling A , een familie (of, en dat is niet hetzelfde, een collectie) R van relaties over A , en een familie of verzameling C van elementen van A , de *constanten* van $\mathbf{A}$.

Enige klassen van relationele stelsels

I. Een *gesorteerde verzameling* is een paar $\langle A, \mathcal{P} \rangle$ van een verzameling A en een partitie $\mathcal{P}$ van A ; of een benoemde structuur $\mathbf{A}$ waarvan de nomenclatuur bestaat uit eenplaatsige operaties zo dat

- (i) voor alle $P \in \text{Nom } \mathbf{A}$, $P^{\mathbf{A}}(a) \simeq a$,
- (ii) voor alle onderscheiden $P, Q \in \text{Nom } \mathbf{A}$, $\text{Dom } P^{\mathbf{A}}$ en $\text{Dom } Q^{\mathbf{A}}$ disjunct zijn, en
- (iii) $\bigcup \{\text{Dom } P^{\mathbf{A}} \mid P \in \text{Nom } \mathbf{A}\} = A$.

II. Een *quasiorde* is een verzameling X met een binaire relatie over X die X -reflexief is en transitief — een *quasiordening op X* .

Een binaire relatie R is *antisymmetrisch* als

$$xRy \ \& \ yRx \Rightarrow x = y.$$

Een *orde* is een quasioorde $\langle X, R \rangle$ met antisymmetrische R ; de relatie heet in dit geval een *ordening*.

Quasiordeningen worden vaak aangeduid met het symbool $\leq$. De inverse van een gegeven relatie $\leq$ noteert men als $\geq$; $\geq$ is ook een quasiordening. In de context van een relatie die wordt aangeduid met $\leq$ betekent ' $x < y$ ' dat $x \leq y$ en $x \neq y$. De inverse van $<$ is $>$. Merk op dat in een orde, $x > y$ dan en slechts dan als $x \geq y$ en $x \neq y$.

Omdat de inverse van een (quasi)ordening weer een (quasi)ordening is, blijft elke universeel geldige bewering over (quasi)ordeningen $\leq$ geldig als daarin elke ' $\leq$ ' wordt omgedraaid. Dit dualiteitsprincipe voor quasioordes kan worden opgevat als een speciaal geval van het dualiteitsprincipe voor categorieën, zie Oefening 5. De duale van een quasioorde $\mathbf{Q} = \langle Q, \leq \rangle$ is $\mathbf{Q}^\partial := \langle Q, \geq \rangle$.

Zij $\mathbf{Q} = \langle Q, \leq \rangle$ een quasioorde en $X \subseteq Q$. Een element x van X is een *kleinste* element van X als voor alle $y \in X$, $x \leq y$; x is een *minimaal* element als voor alle $y \in X$, als $y \leq x$, dan $x \leq y$. Als $\mathbf{Q}$ een ordening is, heeft X hoogstens één kleinste element. Duaal hebben we *grootste* en *maximale* elementen.

Intervallen. Een *interval* in a quasioorde is de verzameling van alle elementen *tussen* twee gegeven elementen, of, bij uitbreiding, *voorbij* een gegeven element. Er zijn meerder mogelijkheden. Laat $\mathbf{Q} = \langle Q, \leq \rangle$ een quasioorde zijn, en $x, y \in Q$. Dan

$\text{Iv}_{\mathbf{Q}}[x, y] = \{q \in Q \mid x \leq q \leq y\}$, het gesloten interval tussen x en y ;

$\text{Iv}_{\mathbf{Q}}(x, y) = \{q \in Q \mid x < q < y\}$, het open interval tussen x en y ;

$\text{Iv}_{\mathbf{Q}}(x, y] = \{q \in Q \mid x < q \leq y\}$,

$\text{Iv}_{\mathbf{Q}}[x, y) = \{q \in Q \mid x \leq q < y\}$, halfopen intervallen tussen x en y ;

$\text{Iv}_{\mathbf{Q}}(\leftarrow y) = \text{Iv}_{\mathbf{Q}}(y) = \{q \in Q \mid q \leq y\}$, het gesloten onbegrensde interval onder y ;

$\text{Iv}_{\mathbf{Q}}(\leftarrow y) = \{q \in Q \mid q < y\}$, het open onbegrensde interval onder y ;

$\text{Iv}_{\mathbf{Q}}[x \rightarrow) = \text{Iv}_{\mathbf{Q}}(x) = \{q \in Q \mid x \leq q\}$, het gesloten onbegrensde interval boven x ;

$\text{Iv}_{\mathbf{Q}}(x \rightarrow) = \{q \in Q \mid x < q\}$, het open onbegrensde interval boven x .

We laten het subscript, en zelfs het etiket "Iv", soms weg als de context dat toelaat. Merk op dat ieder begrensd interval de doorsnede is van twee onbegrensde. Bijvoorbeeld, $(x, y] = (x \rightarrow) \cap (y]$.

Cofinale verzamelingen. Zij $\mathbf{Q} = \langle Q, \leq \rangle$ een quasioorde, en $X \subseteq Q$. Dan is X *cofinaal* in $\mathbf{Q}$ als voor elke $q \in Q$, $\text{Iv}_{\mathbf{Q}}[q \rightarrow) \cap X \neq \emptyset$. Bijvoorbeeld, volgens de Stelling van Euclides zijn de priemgetallen cofinaal in $\langle \mathbb{N}, \leq \rangle$.

Voor elke verzameling X is $\langle \mathcal{P}X, \subseteq \rangle$ een orde.

Elementen x en y van een quasioorde $\langle X, \leq \rangle$ zijn *vergelijkbaar* als $x \leq y$ of $y \leq x$.

III. Een binaire relatie R is *irreflexief* als er geen x bestaat zo dat xRx . Een *sterke orde* is een verzameling X met een relatie over X die irreflexief is en transitief (een *sterke ordening*).

Voor elke verzameling X is $\langle \mathcal{P}X, \subset \rangle$ een sterke orde.

Sterke ordeningen worden vaak aangeduid met het symbool $<$.

1 PROPOSITIE. Zij R een binaire relatie over een verzameling X . Dan is

- (i) als R een quasiordening is van X , $R \setminus R^{-1}$ een sterke ordening;
- (ii) als R een sterke ordening is, $R \cup \Delta_X$ een ordening op X .

De ordening $R \cup \Delta_X$ heet de *zwakke* ordening geassocieerd met R . Intervallen in een sterke orde zijn gedefinieerd via de geassocieerde zwakke orde.

IV. Een *keten* (een *totale* of *lineaire* orde) is een orde waarin elk tweetal elementen vergelijkbaar is. Een *keten in een quasioorde* $\langle X, \leq \rangle$ is een deelverzameling C van X zo dat $\langle C, \leq|_C \rangle$ een keten is. We gebruiken dezelfde terminologie voor sterke ordes: een sterke orde $\langle X, < \rangle$ is een keten als de corresponderende zwakke orde $\langle X, \leq \rangle$ er een is, enzovoort.

V. Zij R een binaire relatie over een klasse A . Dan heet R *gefundeerd* als iedere niet-lege subklasse X van A een element x bevat zo dat

$$X \cap x/R = \emptyset.$$

Als R een sterke ordening is, noemen we zo'n element x een *R -minimaal* element van X .

Zij bijvoorbeeld A een willekeurige klasse. Dan is de relatie $\in|_A$ gefundeerd. Want stel dat X een niet-lege deelverzameling is van A . Volgens het Regulariteitsaxioma heeft X een element x waarmee het disjunct is. Dat wil zeggen:

$$X \cap x/\in = \emptyset;$$

waaruit $X \cap x/(\in|_A) = \emptyset$ onmiddellijk volgt.

Voor relationele stelsels $\mathbf{A}$ en $\mathbf{B}$ geldt

$$\mathbf{A} \leq \mathbf{B} \Leftrightarrow \mathbf{A} \subseteq \mathbf{B}.$$

Voorbeelden

i. $\langle \mathbb{Z}, < \rangle$ en $\langle \mathbb{Z}_+, | \rangle$ (waar $x|y$ betekent dat x een deler is van y , dat wil zeggen, dat er een z bestaat zo dat $x \cdot z = y$) zijn zwakke, maar geen gesloten, substructuren van $\langle \mathbb{Z}, \leq \rangle$.

ii. Zij $\mathbf{A} = \langle A, R \rangle$ een quasioorde, en α de equivalentierelatie $R \cap R^{-1}$. Definieer: $B = A/\alpha$, $S = (\exists \circ R \circ \in)|_B$, en $\mathbf{B} = \langle B, S \rangle$. Dan is $a \mapsto a/\alpha$ een homomorfisme van $\mathbf{A}$ op $\mathbf{B}$; merk op dat $\mathbf{B}$ een orde is.

iii. Een *transitiesysteem* is een tweesoortig relationeel stelsel $\mathbf{A} = \langle X, S; R \rangle$ waarin $R \subseteq S \times X \times S$. De soort X is de *invoerverzameling* of het *actie-alfabet*, de elementen van S heten *toestanden* of *processen*, en R is de *staprelatie*. Men kan zich $\mathbf{A}$ voorstellen als een apparaat dat wanneer het in toestand $s \in S$ de invoer $x \in X$ krijgt, overgaat in een toestand t waarvoor geldt dat $Rsxt$; of als een collectie van processen s die door een actie x overgaan in een proces t zo dat $Rsxt$. Definieer een functie $f: X \rightarrow \mathcal{P}(S \times S)$ door

$$f(x) = \{ \langle s, t \rangle | Rsxt \}.$$

Laat ρ het unieke homomorfisme van $\mathbf{X}^*$ naar de monoïde $\langle \mathcal{P}(S \times S), \circ, \Delta_S \rangle$ zijn dat f uitbreidt (§E, Stelling 2). Het homomorfisme ρ is de *overgangsfunctie* van $\mathbf{A}$: als $w = w_0 \dots w_{n-1} \in X^*$, en $\langle s, t \rangle \in \rho_w$, dan is er een overgang van s naar t door de successieve invoer van $w_0, \dots, w_{n-1} \in X$, of via acties $w_0, \dots, w_{n-1}$.

De drietallen $\langle s, w, t \rangle$ waarvoor geldt dat $\langle s, t \rangle \in \rho_w$ vormen een categorie met de toestanden als objecten, eenheidselementen $\langle s, \varepsilon, s \rangle$, en samenstelling

$$\langle r, v, s \rangle \circ \langle s, w, t \rangle = \langle r, vw, t \rangle.$$

Het transitiesysteem $\mathbf{A}$ is een *deterministische automaat* als er voor elke toestand s en elke invoer x precies één toestand t bestaat zo dat $Rsxt$.

§G Kategorieën: Bijzondere pijlen

Secties en retracties

Monoïden zijn categorieën met een enkel object. Om precies te zijn:

1 PROPOSITIE. (a) Zij $\mathbf{M} = \langle M, \cdot, e \rangle$ een monoïde. Dan is $\langle M, \cdot, \{e\} \rangle$ een categorie.

(b) Zij $\mathbf{K} = \langle K, \circ, E \rangle$ een niet-lege categorie. Dan geldt

1° de operatie $\circ$ is totaal dan en slechts dan als $|E| = 1$;

2° als $E = \{u\}$, dan is $\langle K, \circ, u \rangle$ een monoïde.

Andersom is een categorie een gegeneraliseerde monoïde. In dat algemenere kader zullen we nu het begrip *inverse* beschouwen.

Notatie. In plaats van ' $f \in E$ ' schrijven we vaak ' $f = 1$ '. De lezer moet er daarom op bedacht zijn dat in een categorische context verschillende voorkomens van 1 niet per se naar hetzelfde ding verwijzen.

2 DEFINITIE. Zij $\mathbf{C}$ een categorie. Een pijl $s \in C$ is een *sectie* als er een pijl $r \in C$ bestaat zo dat $rs = 1$.

Voorbeelden

i. Een pijl $\langle Y, f \rangle$ van $\mathbf{Vr}_z$ is een sectie dan en slechts dan als f injectief is en ofwel Y leeg of f niet-leeg.

ii. Zij $\langle Y, f \rangle$ een pijl in $\mathbf{Vr}_z$. Dan is de afbeelding $x \mapsto \langle f(x), x \rangle$ van $\text{Dom } f$ in f een sectie.

iii. Als in een monoïde $\mathbf{M}$ ieder element een sectie is, dan is $\mathbf{M}$ een groep. Want stel $rs = e$ en $qr = e$. Dan $q = qrs = s$, dus s heeft een inverse.

3 PROPOSITIE. Als f en g secties zijn, en gf bestaat, dan is gf een sectie.

BEWIJS. Als $qf, rg = 1$, dan $b(r) = d(g) = b(f) = d(q)$, and $qr \circ gf = 1$. ☒

4 PROPOSITIE. Als gf een sectie is, dan f ook.

BEWIJS. Als $r \circ gf = 1$, dan ook $rg \circ f = 1$. ☒

5 DEFINITIE. Zij $\mathbf{C}$ een categorie. Een pijl $r \in C$ is een *retractie* als er een pijl $s \in C$ bestaat zo dat $rs = 1$.

Voorbeeld iv. Een element $\langle Y, f \rangle$ van $\mathbf{Vr}_z$ is een retractie dan en slechts dan als f surjectief is. (Dit is in feite een herformulering van het Keuze-Axioma.)

6 PROPOSITIE. *Sectie* en *retractie* zijn duale begrippen.

7 DEFINITIE. Zij $\mathbf{C}$ een categorie. Een element van C is een *isomorfisme* als het zowel een sectie is als een retractie.

8 GEVOLG. *Isomorfisme* is een zelfduaal begrip.

9 PROPOSITIE. Samengestelden van isomorfismen zijn isomorfismen.

Als $f \circ g = 1$, dan heet f een *linksinverse* van g , en g een *rechtsinverse* van f . Secties zijn gedefinieerd als pijlen met een linksinverse, en retracties, dual, als pijlen met een rechtsinverse.

10 PROPOSITIE. Zij $\mathbf{C}$ een categorie. Een pijl $f \in C$ is een isomorfisme dan en slechts dan als f een unieke rechtsinverse h heeft en een unieke linksinverse k , en $h = k$.

Bewijs. ($\Rightarrow$) Omdat f een retractie is, heeft f een rechtsinverse h , en omdat f een sectie is, heeft f een linksinverse k . Als $fh' = 1$, dan $h' = kfh' = k = kfh = h$, dus h is uniek en $k = h$; bijgevolg is k ook uniek.

($\Leftarrow$) Triviaal. ☒

We noteren de (unieke, tweezijdige) inverse van een isomorfisme f als f^{-1} . We gebruiken de afkorting *Sec* ter aanduiding van de klasse der secties, *Ret* voor de klasse der retracties, en *Iso* voor de klasse der isomorfismen. Merk op dat eenheidselementen isomorfismen zijn: dus

$$E \subseteq Iso = Sec \cap Ret.$$

Voorbeelden

v. (a) Blijkens Propositie 1.4 in §H van Hoofdstuk 1 zijn de isomorfismen in **Vrz** bijecties. Omgekeerd is eenvoudig in te zien dat bijecties isomorfismen zijn.

(b) Ook in **Rel** zijn de isomorfismen de bijecties. Stel maar dat $R: X \leftarrow Y$ en $S: Y \leftarrow X$ elkaars inversen zijn, i.e. $R \circ S = \Delta_X$ en $S \circ R = \Delta_Y$. Voor elke $x \in X$ is er dan een $y \in Y$ zo dat $xRySx$; in het bijzonder

$$(1) \quad \forall x \in X \exists y \in Y ySx.$$

Evenzo geldt natuurlijk

$$(2) \quad \forall x \in X \exists y \in Y xRy.$$

Stel nu dat ySx en zSx . Wegens (2) bestaat er een $w \in Y$ zo dat xRw . Omdat $S \circ R = \Delta_Y$, moet gelden dat $y = w = z$. Dus S is een functie; wegens (1) is S een afbeelding van X naar Y . Evenzo is R een afbeelding van Y naar X . Dus $\langle X, R \rangle$ en $\langle Y, S \rangle$ zijn inversen in **Vrz**, en, volgens (a), bijecties. Het omgekeerde, dat bijecties isomorfismen zijn in **Rel**, is evident.

vi. In de optiek van Propositie 1 is een groep een niet-lege categorie met totale samenstelling waarvan alle pijlen isomorfismen zijn.

11 GEVOLG. Zij f een isomorfisme. Dan is f^{-1} ook een isomorfisme, en

$$(f^{-1})^{-1} = f.$$

Bovendien $d(f) = b(f^{-1})$, en a fortiori $d(f^{-1}) = b(f)$.

Isomorfie

Isomorfie is een relatie tussen pijlen, en a fortiori tussen objecten.

12 DEFINITIE. Zij C een categorie. Pijlen $f, g \in C$ zijn *isomorf*, notatie $f \cong g$, als er isomorfismen h en k bestaan zo dat $hf = gk$.

In het bijzonder zijn eenheidspijlen u en v isomorf als (en alleen als) ufv bestaat voor een of ander isomorfisme f ; en objecten heten isomorf als hun identiteitspijlen dat zijn, dus $X \cong Y$ dan en slechts dan als er een isomorfisme van X naar Y bestaat.

13 PROPOSITIE. Een pijl f is een isomorfisme dan en slechts dan als f isomorf is met een eenheidselement.

Bewijs. ($\Rightarrow$) Als f een isomorfisme is, dan $f^{-1} \circ f = 1 = 1 \circ 1$.

($\Leftarrow$) Als er $h, k \in Iso$ bestaan zo dat $hf = 1 \circ k$, dan $f = h^{-1} \circ k \in Iso$. □

14 PROPOSITIE. Isomorfie is een equivalentierelatie.

Bewijs. Isomorfie is reflexief, want $1 \circ f = f \circ 1$. Symmetrisch, want als h and k isomorfismen zijn, en $hf = gk$, dan $f \circ k^{-1} = h^{-1} \circ g$. En transitief, want als h_i and k_i isomorfismen zijn, $i = 1, 2$, en $h_1f = gk_1$, $h_2g = mk_2$, dan

$$h_2h_1f = h_2gk_1 = mk_2k_1. \quad \square$$

Voorbeeld vii. $\mathbf{Rel}^0 \cong \mathbf{Rel}$. Definieer $F: \mathbf{Rel} \rightarrow \mathbf{Rel}$ door

$$F(X, R, Y) = \langle Y, R^{-1}, X \rangle.$$

Dan $F \upharpoonright E = 1_E$, en

$$\begin{aligned} F(\langle X, R, Y \rangle \bullet \langle U, S, V \rangle) &\simeq F(\langle U, S, V \rangle \circ \langle X, R, Y \rangle) \\ &\simeq F(U, S \circ R, Y) \triangleleft X = V \\ &\simeq \langle Y, (S \circ R)^{-1}, U \rangle \triangleleft X = V \\ &\simeq \langle Y, R^{-1} \circ S^{-1}, U \rangle \triangleleft X = V \\ &\simeq \langle Y, R^{-1}, X \rangle \circ \langle V, S^{-1}, U \rangle \\ &\simeq F(X, R, Y) \circ F(U, S, V), \end{aligned}$$

dus F is een functor; en $F \circ F = 1$. — Algemeen heet een pijl die haar eigen inverse is een *involutie*. Een typisch voorbeeld is de complementeringsoperatie in een Boole-algebra.

Monomorfismen en Epimorfismen

In Oefening 2 van Hoofdstuk 1, §H, worden twee *wiseigenschappen* van pijlen geformuleerd, één behorend bij surjecties en één behorend bij injecties, die (zoals we zullen zien) algemener zijn dan de inverteerbaarheidseigenschappen van retracts en secties.

15 DEFINITIE. Zij $\mathbf{C}$ een categorie. Een pijl $m \in C$ is *linkswisbaar*, of een *monomorfisme*, als voor alle $h, k \in C$,

$$mh = mk \Rightarrow h = k.$$

We duiden de klasse der monomorfismen aan met *Mon*.

Voorbeeld viii. In $\mathbf{Vrz}$ bestaat *Mon* uit de injectieve functies — om precies te zijn, uit de paren $\langle Y, f \rangle \in \mathbf{Vrz}$ waarin f injectief is. In het bijzonder is ieder paar $\langle Y, \emptyset \rangle$ een monomorfisme; dus niet alle monomorfismen zijn secties.

We formuleren de karakterisering van de monomorfismen in $\mathbf{Str}$ als een stelling.

16 STELLING. Een homomorfisme is een monomorfisme in $\mathbf{Str}$ dan en slechts dan als het injectief is.

BEWIJS. Zij $f: \mathbf{A} \rightarrow \mathbf{B}$ een homomorfisme.

Als $f: A \rightarrow B$ een monomorfisme is in $\mathbf{Vrz}$, dan is $f: \mathbf{A} \rightarrow \mathbf{B}$ een monomorfisme in $\mathbf{Str}$. (Zie het bovenstaande Voorbeeld.)

Omgekeerd, stel dat f niet injectief is, zeg $f(a_0) = f(a_1)$ waar $a_0 \neq a_1$. Zij

$$g = \{\langle a_0, x \rangle\} \text{ en } h = \{\langle a_1, x \rangle\}.$$

Dan zijn g en h homomorfismen van $\{x\}$ naar $\mathbf{A}$, en $f \circ g = f \circ h$; maar $g \neq h$. $\square$

17 PROPOSITIE. (i) Als $m, n \in \mathbf{Mon}$, dan $m \circ n \in \mathbf{Mon}$.

(ii) Als $f \circ g \in \mathbf{Mon}$, dan $g \in \mathbf{Mon}$.

(iii) $\mathbf{Sec} \subseteq \mathbf{Mon}$.

BEWIJS. (i) Laat m en n monomorfismen zijn; stel $mnh = mnk$. Omdat m een monomorfisme is, geldt $nh = nk$; en vervolgens omdat $n \in \mathbf{Mon}$, $h = k$. Dus $mn \in \mathbf{Mon}$.

(ii) Stel fg is een monomorfisme, en $gh = gk$. Dan $fgh = fgk$, dus omdat $fg \in \mathbf{Mon}$, $h = k$. Daarmee is aangetoond dat $g \in \mathbf{Mon}$.

(iii) Stel $m \in \text{Sec}$. Dan bestaat r zo dat $rm = 1$. Stel nu dat $mh = mk$. Dan $rmh = rmk$, dus $h = k$, waarmee is aangetoond dat $m \in \text{Mon}$. $\square$

18 PROPOSITIE. $\text{Iso} = \text{Mon} \cap \text{Ret}$.

BEWIJS. Stel $f \in \text{Mon} \cap \text{Ret}$; zeg $fs = 1$. Dan $fsf = f = f \circ 1$, dus omdat $f \in \text{Mon}$, $sf = 1$. $\square$

19 DEFINITIE. Zij $\mathbf{C}$ een kategorie. Een pijl $e \in C$ is *rechtswisbaar*, of een *epimorfisme*, als voor alle $h, k \in C$,

$$he = ke \Rightarrow h = k.$$

We duiden de klasse der epimorfismen aan met Epi .

Voorbeeld ix. Een element $\langle Y, f \rangle$ van $\mathbf{Vrz}$ is een epimorfisme dan en slechts dan als f surjectief is. Slechts dan als: stel dat f niet surjectief is; zeg

$$z \in Y \setminus \text{Im} f.$$

Laat $A = \{a, b\}$ een verzameling zijn met twee elementen, en definieer

$$h, k: A \leftarrow Y$$

door: $h(y) = a$ voor alle $y \in Y$, en $k(y) = a$ als $y \neq z$, $k(z) = b$. Dan $hf = kf$, maar $h \neq k$, dus f is geen epimorfisme. Dan als: zie 1§H, Oefening 2(i). In $\mathbf{Vrz}$ zijn dus alle epimorfismen retracties (cf. Voorbeeld (iv)).

20 PROPOSITIE. *Monomorfisme* en *epimorfisme* zijn duale begrippen.

GEVOLG. (a) Als $d, e \in \text{Epi}$, dan $de \in \text{Epi}$.

(b) Als $fg \in \text{Epi}$, dan $f \in \text{Epi}$.

(c) $\text{Ret} \subseteq \text{Epi}$.

(d) $\text{Iso} = \text{Epi} \cap \text{Sec}$.

Op de koop toe hebben we een voorbeeld van een kategorie met epimorfismen die geen retracties zijn: neem $\mathbf{Vrz}^\partial$, en hergebruik het voorbeeld van monomorfismen die geen secties zijn.

§H Bijzondere homomorfismen; congruentierelaties en quotienten

Het begrip *homomorfisme* heeft een aantal nuttige verfijningen. Ze komen voort uit de omstandigheid dat een homomorfisme tussen *algebra's* automatisch bepaalde plezierige eigenschappen heeft; in het algemene geval mogen we die niet verwachten, maar dat doet aan hun belang niet af.

Zij $f: \mathbf{A} \rightarrow \mathbf{B}$ een homomorfisme, waar $\mathbf{A}$ een algebra is en $\text{Nom} \mathbf{B} = \text{Nom} \mathbf{A}$. Als $f(x) = Q^{\mathbf{B}}(f \circ a)$, dan moet er een familie a' bestaan zo dat

$$f(Q^{\mathbf{A}}(a')) = f(x);$$

we kunnen zelfs $a' = a$ nemen. Of op een subtiel verschillende toer, als

$$Q^{\mathbf{B}}(f \circ a) \downarrow,$$

dan bestaat $Q^{\mathbf{A}}(a)$ ook. Voor algebra's is dat allemaal triviaal; voor structuren in het algemeen zijn de zojuist beschreven eigenschappen, *volheid* en *geslotenheid*, onafhankelijk van de definiërende eigenschappen van homomorfismen.

Reflectiviteit

Laat $\mathbf{A}$ en $\mathbf{B}$ structuren zijn. Een functie $f: A \rightarrow B$ is een *zwakke reflectie* van $\mathbf{B}$ in $\mathbf{A}$ als voor ieder operatiesymbool Q en alle $a \in A^{K_Q}$,

$$Q^{\mathbf{B}}(f \circ a) \in \text{Im} f \Rightarrow \exists a' \in \text{Dom} Q^{\mathbf{A}}. f \circ a' = f \circ a.$$

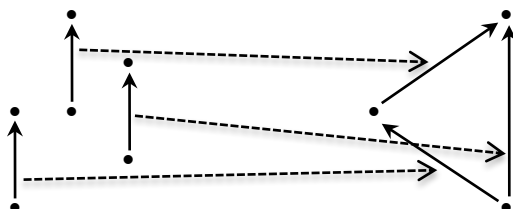
1 PROPOSITIE. Laat $\mathbf{A}$, $\mathbf{B}$ en $\mathbf{C}$ structuren zijn, en $A \xrightarrow{f} B \xrightarrow{g} C$ functies. Als f een zwakke reflectie is van $\mathbf{B}$ in $\mathbf{A}$ en g een zwakke reflectie van $\mathbf{C}$ in $\mathbf{B}$, en f is surjectief, dan is $g \circ f$ een zwakke reflectie van $\mathbf{C}$ in $\mathbf{A}$.

BEWIJS. Stel $Q^{\mathbf{C}}(g \circ f \circ a) \in \text{Im} gf$; zeg $Q^{\mathbf{C}}(g \circ f \circ a) = gf(x)$. Omdat g een zwakke reflectie is van $\mathbf{C}$ in $\mathbf{B}$, en $\text{Im} gf \subseteq \text{Im} g$, bestaat er een familie $b \in \text{Dom} Q^{\mathbf{B}}$ zo dat $g \circ f \circ a = g \circ b$. Omdat f surjectief is, $\text{Im} b \cup \{Q^{\mathbf{B}}(b)\} \subseteq \text{Im} f$. Omdat f een zwakke reflectie is van $\mathbf{B}$ in $\mathbf{A}$ volgt daaruit het bestaan van een familie $d \in \text{Dom} Q^{\mathbf{A}}$ zo dat $f \circ d = b$. Dan $g \circ f \circ a = g \circ b = g \circ f \circ d$. $\square$

Een homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ is *vol* als de onderliggende functie $f: A \rightarrow B$ een zwakke reflectie is van $\mathbf{B}$ in $\mathbf{A}$.

Voorbeelden

- i. Het homomorfisme f van §C, Voorbeeld (iv), is vol. Algemeener is voor ieder homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ het afgeleide homomorfisme $f: \mathbf{A} \rightarrow f[\mathbf{A}]$ vol.
- ii Als $\mathbf{A} \subseteq \mathbf{B}$, dan is de kanonieke inbedding $1_{\mathbf{B}}^{\mathbf{A}}$ een vol homomorfisme van $\mathbf{A}$ naar $\mathbf{B}$.
- iii (botsende terminologie). Een functor is een homomorfisme tussen categorieën, maar een volle functor is niet noodzakelijk een vol homomorfisme, en evenmin is een functor die vol is qua homomorfisme per se een volle functor.



De bovenstaande figuur schetst een volle functor die geen vol homomorfisme is; de injectieve functoren van $\mathbf{2}$ naar $\Downarrow$ zijn voorbeelden van volle homomorfismen die geen volle functoren zijn.

De volheidsimplicaties tussen homomorfismen en hun samengestelden — die ook homomorfismen zijn, wegens §C, Propositie 2(ii) — zijn als volgt.

2 STELLING. Laat $f: \mathbf{A} \rightarrow \mathbf{B}$ en $g: \mathbf{B} \rightarrow \mathbf{C}$ homomorfismen zijn.

- (i) Als f en g vol zijn, en (a) f is surjectief of (b) g injectief, dan is $g \circ f$ vol.
- (ii) Als $g \circ f$ vol is, en g is injectief, dan is f vol.
- (iii) Als $g \circ f$ vol is, en f is surjectief, dan is g vol.
- (iv) Als $g \circ f$ vol is en surjectief, dan is g vol en surjectief.

Bewijs. (i) Laat f en g vol zijn.

(ia) Als f surjectief is, dan volgt de conclusie direct uit Propositie 1 hierboven.

(ib) Stel dat g injectief is. Zij $gf(x) = Q^{\mathbf{C}}(g \circ f \circ a)$. Omdat g vol is, is er dan een familie $b \in \text{Dom} Q^{\mathbf{B}}$ zo dat

$$g \circ b = g \circ f \circ a.$$

Omdat g injectief is, volgt meteen dat $b = f \circ a$. Bovendien

$$g(Q^{\mathbf{B}}(f \circ a)) = Q^{\mathbf{C}}(g \circ f \circ a) = gf(x)$$

omdat g een homomorfisme is, dus omdat g injectief is, $Q^{\mathbf{B}}(f \circ a) = f(x)$. Omdat f vol is, volgt daaruit het bestaan van $a' \in \text{Dom } Q^{\mathbf{A}}$ zo dat $f \circ a' = f \circ a$. Dan

$$g \circ f \circ a' = g \circ f \circ a,$$

dus $g \circ f$ is vol.

(ii) Zij $g \circ f$ vol en g injectief. Stel dat $Q^{\mathbf{B}}(f \circ a) \in \text{Im } f$. Dan $Q^{\mathbf{C}}(g \circ f \circ a) \in \text{Im } gf$, en omdat $g \circ f$ vol is, bestaat er een familie $a' \in \text{Dom } Q^{\mathbf{A}}$ zo dat

$$g \circ f \circ a' = g \circ f \circ a.$$

Omdat g injectief is, volgt daaruit dat $f \circ a' = f \circ a$; en daarmee is bewezen dat f vol is.

(iii) Zij $g \circ f$ vol en f surjectief. Stel dat $Q^{\mathbf{C}}(g \circ b) \in \text{Im } g$. Omdat f surjectief is, is er een familie $a \in A^{K_Q}$ zo dat $b = f \circ a$. Dan $Q^{\mathbf{C}}(g \circ f \circ a) \in \text{Im } gf$, want uit de surjectiviteit van f volgt dat $\text{Im } g = \text{Im } gf$. Omdat $g \circ f$ vol is, bestaat er een familie $a' \in \text{Dom } Q^{\mathbf{A}}$ zo dat $g \circ f \circ a' = g \circ f \circ a = g \circ b$. Omdat f een homomorfisme is, $f \circ a' \in \text{Dom } Q^{\mathbf{B}}$; en daarmee is bewezen dat g vol is.

(iv) Zij $g \circ f$ vol en surjectief. Dat g surjectief is, volgt dan onmiddellijk. Stel nu dat $Q^{\mathbf{C}}(g \circ b) \in \text{Im } g$. Omdat $g \circ f$ surjectief is, is er een familie $a \in A^{K_Q}$ zo dat

$$g \circ b = g \circ f \circ a.$$

Omdat $g \circ f$ surjectief is, hebben we dan

$$Q^{\mathbf{C}}(g \circ f \circ a) \in \text{Im } gf.$$

Omdat $g \circ f$ vol is, impliceert dit het bestaan van een familie $a' \in \text{Dom } Q^{\mathbf{A}}$ zo dat

$$g \circ f \circ a' = g \circ f \circ a = g \circ b.$$

Omdat f een homomorfisme is, $f \circ a' \in \text{Dom } Q^{\mathbf{B}}$; en daarmee is bewezen dat g vol is. $\square$

3 GEVOLG. Zij $f: \mathbf{A} \rightarrow \mathbf{B}$ een homomorfisme. Dan

$$f[\mathbf{A}] \subseteq \mathbf{B} \Leftrightarrow f \text{ vol is.}$$

BEWIJS. ($\Rightarrow$) Stel $f[\mathbf{A}] \subseteq \mathbf{B}$. Dan is $1_B^{f[\mathbf{A}]}$ een vol injectief homomorfisme van $f[\mathbf{A}]$ naar $\mathbf{B}$, en $f: \mathbf{A} \rightarrow \mathbf{B}$ is de samengestelde van $1_B^{f[\mathbf{A}]}$ met het volle homomorfisme $f: \mathbf{A} \rightarrow f[\mathbf{A}]$; dus f is een vol homomorfisme van $\mathbf{A}$ naar $\mathbf{B}$, volgens Stelling 2(i).

($\Leftarrow$) Stel dat $f: \mathbf{A} \rightarrow \mathbf{B}$ vol is. Omdat $f = 1_B^{f[\mathbf{A}]} \circ f$, en $f: \mathbf{A} \rightarrow f[\mathbf{A}]$ surjectief is, is $1_B^{f[\mathbf{A}]}$ volgens Stelling 2(iii) vol, i.e. $f[\mathbf{A}] \subseteq \mathbf{B}$. $\square$

Laat $\mathbf{A}$ en $\mathbf{B}$ structuren zijn. Een functie $f: A \rightarrow B$ *halfreflecteert* $\mathbf{B}$ in $\mathbf{A}$ als voor ieder operatiesymbool Q ,

$$Q^{\mathbf{B}}(f \circ a) \in \text{Im } f \Rightarrow a \in \text{Dom } Q^{\mathbf{A}}.$$

4 PROPOSITIE. Als f de structuur $\mathbf{B}$ halfreflecteert in $\mathbf{A}$, en g halfreflecteert $\mathbf{C}$ in $\mathbf{B}$, en $f: A \rightarrow B$ is surjectief, dan halfreflecteert $g \circ f$ de structuur $\mathbf{C}$ in $\mathbf{A}$.

BEWIJS. Stel dat $Q^{\mathbf{C}}(g \circ f \circ a) \in \text{Im } gf$. Omdat g de structuur $\mathbf{C}$ halfreflecteert in $\mathbf{B}$, en $\text{Im } gf \subseteq \text{Im } g$, $f \circ a \in \text{Dom } Q^{\mathbf{B}}$. Dan moet, omdat f surjectief is,

$$Q^{\mathbf{B}}(f \circ a) \in \text{Im } f.$$

Uit het gegeven dat f de structuur $\mathbf{B}$ halfreflecteert in $\mathbf{A}$ volgt nu dat $a \in \text{Dom } Q^{\mathbf{A}}$. $\square$

Een homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ is *halfreflectief* als de onderliggende functie de structuur $\mathbf{B}$ halfreflecteert in $\mathbf{A}$.

Halfreflectieve homomorfismen zijn vol. Stelling 2 kan worden vereenvoudigd:

5 STELLING. Laat $f: \mathbf{A} \rightarrow \mathbf{B}$ en $g: \mathbf{B} \rightarrow \mathbf{C}$ homomorfismen zijn.

- (i) Als f en g halfreflectief zijn, en (a) f is surjectief of (b) g injectief, dan is $g \circ f$ halfreflectief.
- (ii) Als $g \circ f$ halfreflectief is, dan is f halfreflectief.
- (iii) Als $g \circ f$ halfreflectief is, en f is surjectief, dan is g halfreflectief.

Bewijs. (i) Laat f en g halfreflectief zijn.

- (ia) Als f surjectief is, dan volgt de conclusie direct uit Propositie 4 hierboven.
- (ib) Stel dat g injectief is. Zij $gf(x) = Q^{\mathbf{C}}(g \circ f \circ a)$. Omdat g halfreflectief is,

$$f \circ a \in \text{Dom } Q^{\mathbf{B}}.$$

Bovendien $g(Q^{\mathbf{B}}(f \circ a)) = Q^{\mathbf{C}}(g \circ f \circ a) = gf(x)$ omdat g een homomorfisme is, dus omdat g injectief is, $Q^{\mathbf{B}}(f \circ a) = f(x)$. Omdat f halfreflectief is, volgt daaruit dat $a \in \text{Dom } Q^{\mathbf{A}}$. Dus $g \circ f$ is halfreflectief.

- (ii) Zij $g \circ f$ halfreflectief. Stel dat $Q^{\mathbf{B}}(f \circ a) \in \text{Im } f$. Dan $Q^{\mathbf{C}}(g \circ f \circ a) \in \text{Im } gf$, en omdat $g \circ f$ halfreflectief is, $a \in \text{Dom } Q^{\mathbf{A}}$.

- (iii) Zij $g \circ f$ halfreflectief en f surjectief. Stel dat $Q^{\mathbf{C}}(g \circ b) \in \text{Im } g$. Omdat f surjectief is, is er een familie $a \in A^{K_Q}$ zo dat $b = f \circ a$. Dan $Q^{\mathbf{C}}(g \circ f \circ a) \in \text{Im } gf$, want uit de surjectiviteit van f volgt dat $\text{Im } g = \text{Im } gf$. Omdat $g \circ f$ halfreflectief is, $a \in \text{Dom } Q^{\mathbf{A}}$. Omdat f een homomorfisme is, $f \circ a \in \text{Dom } Q^{\mathbf{B}}$; en daarmee is bewezen dat g halfreflectief is. $\square$

Een functie $f: \mathbf{A} \rightarrow \mathbf{B}$ *reflecteert* de structuur $\mathbf{B}$ in de structuur $\mathbf{A}$ als voor ieder operatiesymbool Q ,

$$f(x) = Q^{\mathbf{B}}(f \circ a) \Rightarrow x = Q^{\mathbf{A}}(a).$$

6 PROPOSITIE. Als f de structuur $\mathbf{B}$ reflecteert in $\mathbf{A}$ en g reflecteert $\mathbf{C}$ in $\mathbf{B}$, dan reflecteert $g \circ f$ de structuur $\mathbf{C}$ in $\mathbf{A}$.

BEWIJS. Stel dat $gf(x) = Q^{\mathbf{C}}(g \circ f \circ a)$. Omdat g de structuur $\mathbf{C}$ reflecteert in $\mathbf{B}$, $f(x) = Q^{\mathbf{B}}(f \circ a)$. En omdat f de structuur $\mathbf{B}$ reflecteert in $\mathbf{A}$, $x = Q^{\mathbf{A}}(a)$. $\square$

Een homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ is *reflectief* als de onderliggende functie de structuur $\mathbf{B}$ reflecteert in $\mathbf{A}$.

Reflectieve homomorfismen zijn halfreflectief. Omgekeerd zijn volle *injectieve* homomorfismen reflectief. Vereenvoudiging van de bewijzen van 2(ib) en 5(ib) toont aan:

7 GEVOLG. Als $\mathbf{A} \xrightarrow{f} \mathbf{B} \xrightarrow{g} \mathbf{C}$ homomorfismen zijn, g reflectief, dan is

- (i) $g \circ f$ vol als f vol is;
- (ii) $g \circ f$ halfreflectief als f halfreflectief is.

8 STELLING. Laat $f: \mathbf{A} \rightarrow \mathbf{B}$ en $g: \mathbf{B} \rightarrow \mathbf{C}$ homomorfismen zijn.

- (i) Als f en g reflectief zijn, dan is $g \circ f$ reflectief.
- (ii) Als $g \circ f$ reflectief is, dan is f reflectief.
- (iii) Als $g \circ f$ reflectief is, en f is surjectief, dan is g reflectief.

Bewijs. (i) Volgt direct uit Propositie 6.

(ii) Zij $g \circ f$ reflectief. Stel $f(x) = Q^B(f \circ a)$. Dan

$$gf(x) = g(Q^B(f \circ a)) = Q^C(g \circ f \circ a)$$

omdat g een homomorfisme is; en omdat $g \circ f$ reflectief is, $x = Q^A(a)$.

(iii) Zij $g \circ f$ reflectief en f surjectief. Stel $g(y) = Q^C(g \circ b)$. Omdat f surjectief is, bestaan er $x \in A$ en $a \in A^{KQ}$ zo dat $y = f(x)$ en $b = f \circ a$. Dan $gf(x) = Q^C(g \circ f \circ a)$. Omdat $g \circ f$ reflectief is, $x = Q^A(a)$. Dan $y = f(x) = f(Q^A(a)) = Q^B(b)$ omdat f een homomorfisme is. $\square$

9 DEFINITIE. Een injectief homomorfisme $f: A \hookrightarrow B$ is een *inbedding* als het B reflecteert in A .

Opmerking. Grätzer [GrL] definieert inbeddingen van zwakke tralies als *injectieve gesloten homomorfismen*. Wat ‘gesloten’ in dit verband betekent, wordt hieronder uitgelegd.

Voorbeelden.

iv. De kanonieke injectie f van de structuur N van §A Voorbeeld (i) in haar uitbreiding $Z = \langle \mathbb{Z}, +, - \rangle$ is een inbedding. In het bijzonder geldt: als $x - y \in \text{Im} f$, voor natuurlijke getallen x en y , dan $x - y \in \mathbb{N}$.

Dit laat zich generaliseren: elke kanonieke injectie in een uitwendige uitbreiding is een inbedding.

v. Isomorfismen zijn reflectief. Want, als $f: A \rightarrow B$ een isomorfisme is, en

$$f(x) = Q^B(f \circ a),$$

dan $x = f^{-1}(f(x)) = f^{-1}(Q^B(f \circ a)) = Q^A(f^{-1} \circ f \circ a) = Q^A(a)$ omdat f^{-1} een homomorfisme is.

10 GEVOLG. De reflectieve homomorfismen vormen een categorie.

BEWIJS. Uit het laatste voorbeeld volgt dat voor elke structuur A de identieke functie 1_A een reflectief homomorfisme is; en volgens Stelling 8(i) is de klasse der reflectieve homomorfismen gesloten onder samenstellingen. $\square$

11 PROPOSITIE. Een bijectief homomorfisme is een isomorfisme dan en slechts dan als het vol is.

BEWIJS. Zij $h: A \rightarrow B$ een bijectief homomorfisme: de eis dat h^{-1} een homomorfisme is, komt evident op hetzelfde neer als de conditie

$$h(x) = Q^B(h \circ a) \Rightarrow x = Q^A(a)$$

van reflectiviteit. Voor injectieve homomorfismen is dat equivalent met volheid. $\square$

Voorbeeld vi (Burmeister). Laat $2\mathbb{N}$ de verzameling der even natuurlijke getallen zijn; beschouw de structuur $\langle \mathbb{N}, 2\mathbb{N} \rangle$. Definieer $h: \mathbb{N} \rightarrow \mathbb{N}$ door:

$$h(2n) = 2n + 2; \quad h(1) = 0; \quad h(2n + 3) = 2n + 1.$$

Dan is h een bijectief endomorfisme, maar niet vol, dus geen isomorfisme.

12 PROPOSITIE. Zij $\mathbf{A}$ een niet-lege structuur. Dan zijn equivalent:

- (i) $\mathbf{A}$ is een algebra;
- (ii) ieder homomorfisme van $\mathbf{A}$ naar een gelijknamige structuur is vol;
- (iii) ieder bijjectief homomorfisme van $\mathbf{A}$ op een gelijknamige structuur is een isomorfisme.

Bewijs. (i) $\Rightarrow$ (ii) Als $Q \in \text{Nom } \mathbf{A}$, dan $\text{Dom } Q^{\mathbf{A}} = A^{K_Q}$.

(ii) $\Rightarrow$ (iii) Gebruik Propositie 11.

(iii) $\Rightarrow$ (i) Stel dat $\mathbf{A}$ geen algebra is. Neem $c \in A$, en definieer voor iedere $Q \in \text{Nom } \mathbf{A}$, voor alle $a \in A^{K_Q}$,

$$Q^{\mathbf{A}*}(a) = Q^{\mathbf{A}}(a) \triangleleft a \in \text{Dom } Q^{\mathbf{A}} \triangleright c.$$

Dan is $1_A: \mathbf{A} \rightarrow \mathbf{A}^*$ een bijjectief homomorfisme, maar geen isomorfisme. $\square$

Recapitulatie. De drie trappen van reflectiviteit verhouden zich als volgt: gegeven een homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ impliceert $f(x) = Q^{\mathbf{B}}(f \circ a)$ dat

x', a' bestaan zo dat $f(x) = f(x'), f \circ a = f \circ a'$, en $x' = Q^{\mathbf{A}}(a')$: als f vol is;

x' bestaat zo dat $f(x) = f(x')$ en $x' = Q^{\mathbf{A}}(a)$: als f halfreflectief is;

$x = Q^{\mathbf{A}}(a)$: als f reflectief is.

Automorfismen

Een *automorfisme* van een structuur $\mathbf{A}$ is een endomorfisme van $\mathbf{A}$ dat een isomorfisme is in **Str**.

We noteren de collectie van alle automorfismen van $\mathbf{A}$ als $\text{Aut } \mathbf{A}$.

13 PROPOSITIE. Zij $\mathbf{A}$ een structuur. Dan is

- (i) $\text{End } \mathbf{A} := \langle \text{End } \mathbf{A}, \circ, 1_A \rangle$ een monoïde, en
- (ii) $\text{Aut } \mathbf{A} := \langle \text{Aut } \mathbf{A}, \circ, {}^{-1}, 1_A \rangle$ een groep.

14 STELLING (Cayley/Birkhoff). (i) Elke monoïde is isomorf met de endomorfismenmonoïde van een algebra.

(ii) Elke groep is isomorf met de automorfismengroep van een algebra.

Bewijs. (i) Zij $\mathbf{M} = \langle M, \cdot, e \rangle$ een monoïde. Definieer voor elke $m \in M$ een operatie

$$R_m: x \mapsto x \cdot m \quad (\text{rechtse actie van } m)$$

op M . Zij $\mathbf{M}^* := \langle M, \{R_m \mid m \in M\} \rangle$. We zullen bewijzen dat $\text{End } \mathbf{M}^* \cong \mathbf{M}$.

Elke $m \in M$ heeft ook een linkse actie:

$$l_m: x \mapsto m \cdot x.$$

Zo'n linkse actie is een endomorfisme van $\mathbf{M}^*$:

$$l_m(R_n(x)) = m \cdot (x \cdot n) = (m \cdot x) \cdot n = R_n(l_m(x)).$$

Sterker nog, ieder endomorfisme van $\mathbf{M}^*$ is een linkse actie. Zij namelijk $g \in \text{End } \mathbf{M}^*$. Zeg dat $g(e) = m$. Neem $x \in M$ willekeurig; dan

$$g(x) = g(e \cdot x) = g(R_x(e)) = R_x(g(e)) = m \cdot x = l_m(x),$$

dus $g = l_m$.

De toekenning $l: m \mapsto l_m$ is dus een surjectie van M op $\text{End } \mathbf{M}^*$. Ze is ook injectief, omdat $l_m(e) = m$. En l is een homomorfisme: voor $m, n, x \in M$,

$$l_{mn}(x) = (m \cdot n) \cdot x = m \cdot (n \cdot x) = l_m(l_n(x)),$$

dus $l_{mn} = l_m \circ l_n$; en $l_e = 1_M$. Volgens Propositie 12 is daarmee bewezen dat l een isomorfisme is.

(ii) Zij $\mathbf{G} = \langle G, \cdot, ^{-1}, e \rangle$ een groep. Definieer voor elke $x \in G$ operaties R_x en l_x als in (i). Zij $\mathbf{G}^* := \langle G, \{R_x | x \in G\} \rangle$. We gaan bewijzen dat $\mathbf{Aut} \mathbf{G}^* \cong \mathbf{G}$.

Net als in (i) zijn de linkse acties endomorfismen van $\mathbf{G}^*$. In dit geval zijn ze echter ook bijtief: als $l_x(y) = l_x(z)$, dan $y = l_{x^{-1}}(l_x(y)) = l_{x^{-1}}(l_x(z)) = z$; en

$$y = l_x(x^{-1}y).$$

Dus volgens Propositie 12 zijn de linkse acties automorfismen. Evenals in (i) is ieder endomorfisme van $\mathbf{G}^*$ een linkse actie. (In het voorbijgaan zien we dat alle endomorfismen van $\mathbf{G}^*$ automorfismen zijn.)

In het licht van §E, Stelling 4, toont de afsluitende redenering van (i) nu aan dat de toekenning $l: x \mapsto l_x$ een isomorfisme is van $\mathbf{G}$ op $\mathbf{Aut} \mathbf{G}^*$. $\square$

We merken nog op dat alle operaties van de algebra's $\mathbf{M}^*$ en $\mathbf{G}^*$ in het bovenstaande bewijs unair zijn. Een structuur met uitsluitend unaire operaties heet een *unaire structuur*. We hebben dus:

15 GEVOLG. (i) Elke monoïde is isomorf met de endomorfismenmonoïde van een unaire algebra.

(ii) Elke groep is isomorf met de automorfismengroep van een unaire algebra.

Gesloten functies

Laat $\mathbf{A}$ en $\mathbf{B}$ structuren zijn. Een functie $f: A \rightarrow B$ is *zwak gesloten* van $\mathbf{A}$ naar $\mathbf{B}$ als voor ieder operatiesymbool Q en alle $a \in A^{K_Q}$,

$$f \circ a \in \text{Dom } Q^{\mathbf{B}} \Rightarrow \exists a' \in \text{Dom } Q^{\mathbf{A}}. f \circ a' = f \circ a.$$

16 PROPOSITIE. Als f een zwak gesloten functie is van $\mathbf{A}$ naar $\mathbf{B}$, dan is f een zwakke reflectie van $\mathbf{B}$ in $\mathbf{A}$.

In feite is de definitie van zwakke geslotenheid een vereenvoudiging van de definitie van zwakke reflectie, en daardoor kunnen we de stellingen van de subparagraaf over zwak reflectieve functies, volle homomorfismen etcetera, omzetten in stellingen over diverse soorten zwak gesloten functies, door de bewijzen te vereenvoudigen.

17 (cf. 1) PROPOSITIE. Als f een surjectieve zwak gesloten functie is van $\mathbf{A}$ naar $\mathbf{B}$, en g een zwak gesloten functie van $\mathbf{B}$ naar $\mathbf{C}$, dan is $g \circ f$ een zwak gesloten functie van $\mathbf{A}$ naar $\mathbf{C}$.

Bewijs. Stel dat $g \circ f \circ a \in \text{Dom } Q^{\mathbf{C}}$. Omdat g zwak gesloten is van $\mathbf{B}$ naar $\mathbf{C}$, bestaat er een familie $b \in \text{Dom } Q^{\mathbf{B}}$ zo dat $g \circ f \circ a = g \circ b$. Omdat f surjectief is, bestaat er een familie $d \in A^{K_Q}$ zo dat $f \circ d = b$. Dan $f \circ d \in \text{Dom } Q^{\mathbf{B}}$, dus omdat f zwak gesloten is van $\mathbf{A}$ naar $\mathbf{B}$ bestaat er een familie $a' \in \text{Dom } Q^{\mathbf{A}}$ zo dat

$$f \circ d = f \circ a'.$$

Er geldt dan: $g \circ f \circ a' = g \circ f \circ d = g \circ b = g \circ f \circ a$. $\square$

Een homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ is zwak gesloten als de onderliggende functie zwak gesloten is van $\mathbf{A}$ naar $\mathbf{B}$. Zwak gesloten homomorfismen zijn vol.

Voorbeelden

vii. Het homomorfisme $f: \mathbf{N} \rightarrow \mathbf{Z}_k$ van Voorbeeld (i) is zwak gesloten. Algemeener is voor ieder homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ het geïnduceerde homomorfisme $f: \mathbf{A} \rightarrow f[\mathbf{A}]$ zwak gesloten.

viii. De functie f in Voorbeeld (iv) is niet zwak gesloten, want $0 - 1$ behoort niet tot $\mathbb{N}$, maar 0 en 1 doen dat wèl.

Laat $\mathbf{A}$ en $\mathbf{B}$ structuren zijn. Een functie $f: A \rightarrow B$ is *gesloten* van $\mathbf{A}$ naar $\mathbf{B}$ als voor ieder operatiesymbool Q en alle $a \in A^{K_Q}$,

$$f \circ a \in \text{Dom } Q^{\mathbf{B}} \Rightarrow a \in \text{Dom } Q^{\mathbf{A}}.$$

Merk op dat *injectieve* zwak gesloten functies gesloten zijn.

Een homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ is gesloten als de onderliggende functie gesloten is van $\mathbf{A}$ naar $\mathbf{B}$. Gesloten homomorfismen zijn reflectief. Grätzer [GrU] noemde gesloten homomorfismen *strong homomorphisms*.

Voorbeelden

ix. Het homomorfisme $f: \mathbf{N} \rightarrow \mathbf{Z}_k$ van de voorbeelden (i) en (vii) is niet gesloten: $0 - 1$ bestaat niet in $\mathbf{N}$.

x. De afbeelding $\langle Y, f \rangle \mapsto \langle Y, f, \text{Dom}(f) \rangle$ is een gesloten inbedding van de categorie **Vrz** in de categorie **Rel**.

xi (cf. v) Isomorfismen zijn gesloten.

18 PROPOSITIE. Als $\mathbf{A}$ een algebra is en $\text{Nom } \mathbf{B} \subseteq \text{Nom } \mathbf{A}$, dan is ieder homomorfisme van $\mathbf{A}$ naar $\mathbf{B}$ gesloten.

19 (cf. 2, 5, 7) **STELLING.** Laat $f: \mathbf{A} \rightarrow \mathbf{B}$ en $g: \mathbf{B} \rightarrow \mathbf{C}$ homomorfismen zijn.

(i) Als f en g zwak gesloten zijn, en f is surjectief of g injectief, dan is $g \circ f$ zwak gesloten.

(ii) Als f zwak gesloten is en g gesloten, dan is $g \circ f$ zwak gesloten.

(iii) Als $g \circ f$ zwak gesloten is, en g is injectief, dan is f zwak gesloten.

(iv) Als $g \circ f$ zwak gesloten is, en f is surjectief, dan is g zwak gesloten.

(v) Als $g \circ f$ zwak gesloten is en surjectief, dan is g zwak gesloten en surjectief.

Bewijs. (i) Laat f en g zwak gesloten zijn. Als f surjectief is, dan volgt de conclusie direct uit Propositie 17. Als g injectief is, dan volgt de conclusie uit onderdeel (ii) en het feit dat injectieve zwak gesloten functies gesloten zijn.

(ii) Zij f zwak gesloten en g gesloten. Stel $g \circ f \circ a \in \text{Dom } Q^{\mathbf{C}}$. Omdat g gesloten is, $f \circ a \in \text{Dom } Q^{\mathbf{B}}$. Omdat f zwak gesloten is, is er dan een familie $a' \in \text{Dom } Q^{\mathbf{A}}$ zo dat $f \circ a = f \circ a'$, en a fortiori $g \circ f \circ a = g \circ f \circ a'$.

(iii) Zij $g \circ f$ zwak gesloten en g injectief. Stel dat $f \circ a \in \text{Dom } Q^{\mathbf{B}}$. Dan

$$g \circ f \circ a \in \text{Dom } Q^{\mathbf{C}}$$

omdat g een homomorfisme is; en omdat $g \circ f$ zwak gesloten is, bestaat er een familie $a' \in \text{Dom } Q^{\mathbf{A}}$ zo dat

$$g \circ f \circ a' = g \circ f \circ a.$$

Omdat g injectief is, volgt daaruit dat $f \circ a' = f \circ a$; en daarmee is bewezen dat f zwak gesloten is.

(iv) Zij $g \circ f$ zwak gesloten en f surjectief. Stel dat $g \circ b \in \text{Dom } Q^{\mathbf{C}}$. Omdat f surjectief is, is er een familie $a \in A^{K_Q}$ zo dat $b = f \circ a$. Dan $g \circ f \circ a \in \text{Dom } Q^{\mathbf{C}}$. Omdat $g \circ f$ zwak gesloten is, bestaat er een familie $a' \in \text{Dom } Q^{\mathbf{A}}$ zo dat

$$g \circ f \circ a' = g \circ f \circ a = g \circ b.$$

Omdat f een homomorfisme is, $f \circ a' \in \text{Dom } Q^{\mathbf{B}}$; en daarmee is bewezen dat g zwak gesloten is.

(v) Zij $g \circ f$ zwak gesloten en surjectief. Dat g surjectief is, volgt dan onmiddellijk. Stel nu dat $g \circ b \in \text{Dom } Q^{\mathbf{C}}$. Omdat $g \circ f$ surjectief is, is er een familie $a \in A^{K_Q}$

zo dat $g \circ b = g \circ f \circ a$. Omdat $g \circ f$ zwak gesloten is, bestaat er een familie $a' \in \text{Dom } Q^A$ zo dat $g \circ f \circ a' = g \circ f \circ a = g \circ b$. Omdat f een homomorfisme is, $f \circ a' \in \text{Dom } Q^B$; en daarmee is bewezen dat g zwak gesloten is. $\square$

20 (cf. **3**) GEVOLG. Zij $f: A \rightarrow B$ een homomorfisme. Dan

$$f[A] \leq B \Leftrightarrow f \text{ zwak gesloten is.}$$

BEWIJS. ($\Rightarrow$) Stel $f[A] \leq B$. Dan is $1_B^{f[A]}$ een gesloten homomorfisme van $f[A]$ naar B , en $f: A \rightarrow B$ is de samengestelde van $1_B^{f[A]}$ met het zwak gesloten homomorfisme $f: A \rightarrow f[A]$; dus f is een zwak gesloten homomorfisme van A naar B , volgens Stelling 19(ii).

($\Leftarrow$) Stel dat $f: A \rightarrow B$ zwak gesloten is. Omdat $f = 1_B^{f[A]} \circ f$, en $f: A \rightarrow f[A]$ surjectief is, is $1_B^{f[A]}$ volgens Stelling 19(iv) zwak gesloten, en dus gesloten; i.e. $f[A] \leq B$. $\square$

21 (cf. **6**) PROPOSITIE. Als f een gesloten functie is van A naar B , en g van B naar C , dan is $g \circ f$ een gesloten functie van A naar C .

BEWIJS. Stel dat $g \circ f \circ a \in \text{Dom } Q^C$. Omdat g gesloten is, $f \circ a \in \text{Dom } Q^B$. En omdat f gesloten is, $a \in \text{Dom } Q^A$. $\square$

22 (cf. **10**) GEVOLG. De gesloten homomorfismen vormen een categorie.

BEWIJS. Uit Voorbeeld (xi) volgt dat voor elke structuur A de identieke functie 1_A een gesloten homomorfisme is; en uit Propositie 21 volgt dat de klasse der gesloten homomorfismen gesloten is onder samenstellingen. $\square$

23 (cf. **8**) PROPOSITIE. Laat $f: A \rightarrow B$ en $g: B \rightarrow C$ homomorfismen zijn; stel dat $g \circ f$ gesloten is. Dan is

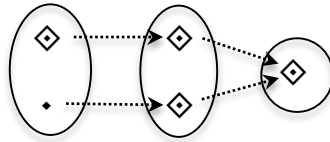
(a) f gesloten;

(b) g gesloten als f surjectief is.

Bewijs. (a) Stel $f \circ a \in \text{Dom } Q^B$. Omdat g een homomorfisme is, moet dan ook $g \circ f \circ a \in \text{Dom } Q^C$. Omdat $g \circ f$ gesloten is, volgt daaruit dat $a \in \text{Dom } Q^A$.

(b) Stel $g \circ b \in \text{Dom } Q^C$. Omdat f surjectief is, bestaat er een familie $a \in A^{K_Q}$ zo dat $b = f \circ a$. Dan $g \circ f \circ a \in \text{Dom } Q^C$, dus omdat $g \circ f$ gesloten is, $a \in \text{Dom } Q^A$. Uit het gegeven dat f een homomorfisme is volgt dan dat $b \in \text{Dom } Q^B$. $\square$

Voorbeeld xii. Deel (a) van de propositie geldt niet als we *gesloten* vervangen door *vol*. Hieronder is een tegenvoorbeeld geschetst, voor structuren met één unair predikaat $\diamond$.



24 PROPOSITIE. Een bijjectief homomorfisme is een isomorfisme dan en slechts dan als het gesloten is.

BEWIJS. ($\Rightarrow$) Voorbeeld (xi).

($\Leftarrow$) Uit Propositie 16 volgt dat gesloten homomorfismen vol zijn. Pas nu Propositie 11 toe. $\square$

Congruëntierelaties en quotiënten

Laat I een verzameling zijn, R een binaire relatie, en a en b I -geïndexeerde families. Dan korten we “voor alle $i \in I, a_i R b_i$ ” af tot $a R^I b$. Een binaire relatie R is *compatibel* met een I -plaatsige operatie f als

voor alle a, b zo dat $a R^I b$: als $f(a), f(b) \in \text{Vld}(R)$, dan $\langle f(a), f(b) \rangle \in R$.

Van een verzameling F van operaties zeggen we dat R compatibel is met F als R compatibel is met ieder element van F . Als $\mathbf{A}$ een structuur is, dan zeggen we dat R compatibel is met $\mathbf{A}$ als R compatibel is met de basisoperaties van $\mathbf{A}$.

25 DEFINITIE. Zij $\mathbf{A}$ een structuur. Een *congruentierelatie* (of kortweg: *congruentie*) van $\mathbf{A}$ is een equivalentierelatie op A die compatibel is met $\mathbf{A}$.

26 PROPOSITIE. Zij $\mathbf{A}$ een structuur en $\alpha \in \text{Eqv} A$. Dan is α een congruentie van $\mathbf{A}$ dan en slechts dan als

voor alle $Q \in \text{Nom} \mathbf{A}$: voor alle $a, b \in \text{Dom } Q^{\mathbf{A}}$: $a \alpha^Q b \Rightarrow \langle Q^{\mathbf{A}}(a), Q^{\mathbf{A}}(b) \rangle \in \alpha$.

BEWIJS. Omdat $\text{Vld}(\alpha) = A$, is de voorwaarde dat $Q^{\mathbf{A}}(a)$ en $Q^{\mathbf{A}}(b)$ tot $\text{Vld}(\alpha)$ behoren vervuld zodra ze bestaan. $\square$

Voorbeelden

xiii. Zij $\mathbf{N} = \langle \mathbb{N}, +, \cdot, -, S, 0 \rangle$ de structuur der natuurlijke getallen met optelling, vermenigvuldiging, partiële aftrekking (gedefinieerd door

$$x - y = z \Leftrightarrow x = z + y,$$

als in Voorbeeld A.i), opvolgeroperatie ($Sx = x + 1$) en nul; en n een natuurlijk getal. Gehelen x en y zijn *congruent modulo* n als $x - y$ of $y - x$ een veelvoud is van n . Men noteert

$$x \equiv y \text{ modulo } n,$$

of $x \equiv y (n)$ (cf. Voorbeeld 1.G.ii). Congruentie modulo n is een congruentierelatie van $\mathbf{N}$.

xiv. In iedere structuur $\mathbf{A}$ zijn Δ_A en ∇_A congruentierelaties.

We noteren de verzameling der congruentierelaties van een structuur $\mathbf{A}$ als $\text{Con} \mathbf{A}$. Geïnspireerd door Voorbeeld (xiii) schrijven we vaak, voor elementen a en b die met elkaar in de congruentierelatie θ staan,

$$a \equiv b \text{ modulo } \theta,$$

of $a \equiv b (\theta)$.

27 GEVOLG. Als $\mathbf{B} \subseteq \mathbf{A}$ en $\alpha \in \text{Con} \mathbf{A}$, dan $\alpha|_B \in \text{Con} \mathbf{B}$.

28 PROPOSITIE. Als f een homomorfisme is van $\mathbf{A}$, dan $\ker f \in \text{Con} \mathbf{A}$.

NOTATIE. Als α een equivalentierelatie is op de verzameling A , dan is q_α de *quotientafbeelding* $a \mapsto a/\alpha$, van A op A/α .⁶

29 DEFINITIE. Zij $\mathbf{A} = \langle A, \mathcal{I} \rangle$ een structuur, en $\theta \in \text{Con} \mathbf{A}$. Het *quotient* van $\mathbf{A}$ over θ is de structuur $\mathbf{A}/\theta = \langle A/\theta, \mathcal{J} \rangle$ waarin voor elk symbool Q ,

$$\mathcal{J}(Q) = \{ \langle \mathcal{I}(Q)(a)/\theta, q_\theta \circ a \rangle \mid a \in \text{Dom } \mathcal{I}(Q) \}.$$

⁶ Eerder genoemd in 1§H, onder 1.3.

De bovenstaande definitie bepaalt inderdaad een structuur *als* de erin gedefinieerde relaties $\mathcal{I}(Q)$ inderdaad operaties zijn. Concreet: als $a = \langle a_k | k \in K_Q \rangle$ en $b = \langle b_k | k \in K_Q \rangle$ dezelfde familie $X = \langle X_k | k \in K_Q \rangle$ van equivalentieklassen representeren, i.e. als telkens $a_k, b_k \in X_k$, en zowel a als b behoort tot $\text{Dom } \mathcal{I}(Q)$, dan moeten we ervan op aan kunnen dat $\mathcal{I}(Q)(a)/\theta = \mathcal{I}(Q)(b)/\theta$. Dit is nu juist wat de compatibiliteitseis uitdrukt.

Merk op dat $\text{Nom}(\mathbf{A}/\theta) = \text{Nom } \mathbf{A}$.

30 LEMMA. Zij $\mathbf{A}$ een structuur, en $\theta \in \text{Con } \mathbf{A}$. Dan is de quotientafbeelding q_θ een vol homomorfisme van $\mathbf{A}$ op $\mathbf{A}/\theta$.

BEWIJS. Als $a \in \text{Dom } Q^{\mathbf{A}}$, dan $q_\theta(Q^{\mathbf{A}}(a)) = Q^{\mathbf{A}}(a)/\theta = Q^{\mathbf{A}/\theta}(q_\theta \circ a)$ per definitie. Ook per definitie bestaat $Q^{\mathbf{A}/\theta}(q_\theta \circ a)$ alleen dan als er families $b \in \text{Dom } Q^{\mathbf{A}}$ bestaan zo dat $q_\theta \circ a = q_\theta \circ b$. $\square$

31 HOMOMORFIESTELLING. Zij $f: \mathbf{A} \rightarrow \mathbf{B}$ een homomorfisme, en $\theta \subseteq \ker f$ een congruentie van $\mathbf{A}$.

(a) Er bestaat precies één homomorfisme $g: \mathbf{A}/\theta \rightarrow \mathbf{B}$ zo dat $g \circ q_\theta = f$. Dit homomorfisme g is injectief dan en slechts dan als $\ker f = \theta$; en surjectief dan en slechts dan als f surjectief is.

(b) Bovendien is g vol dan en slechts dan als f vol is; en

(c) zijn g en q_θ beide gesloten dan en slechts dan als f gesloten is.

BEWIJS. (a) Merk op dat $\ker q_\theta = \theta$; pas het driehoeksluitingslemma (1§H, Gevolg 1.3) toe. We weten dan dat er een unieke kandidaat

$$g: a/\theta \mapsto f(a)$$

is, die bovendien de injectiviteits- en surjectiviteitsbeloften inlost. We moeten alleen nog inzien dat g een homomorfisme is. Zij $X \in \text{Dom } Q^{\mathbf{A}/\theta}$. Volgens Definitie 29 kunnen we dan $a \in \text{Dom } Q^{\mathbf{A}}$ kiezen zo dat $X = q_\theta \circ a$. Dan

$$\begin{aligned} g(Q^{\mathbf{A}/\theta}(X)) &= g(Q^{\mathbf{A}/\theta}(q_\theta \circ a)) = g(q_\theta(Q^{\mathbf{A}}(a))) && \text{volgens Definitie 29} \\ &= f(Q^{\mathbf{A}}(a)) && \text{omdat } g \circ q_\theta = f \\ &= Q^{\mathbf{B}}(f \circ a) && \text{omdat } f \text{ een homomorfisme is} \\ &= Q^{\mathbf{B}}(g \circ q_\theta \circ a) = Q^{\mathbf{B}}(g \circ X). \end{aligned}$$

(b) Als g vol is, dan is, omdat q_θ ook vol is en bovendien surjectief, $f (= g \circ q_\theta)$ vol wegens Stelling 2(i). Andersom: omdat q_θ surjectief is, is g vol als f vol is, volgens Stelling 2(iii).

(c) Als g en q_θ gesloten zijn, dan is f gesloten volgens Propositie 22. Andersom, als f gesloten is, dan zijn g en q_θ het ook, volgens Propositie 23 en omdat q_θ surjectief is. $\square$

GEVOLG I. Ieder homomorfisme is een samenstelling van een injectief homomorfisme en een vol surjectief homomorfisme. Ieder vol homomorfisme is een samenstelling van een inbedding en een vol surjectief homomorfisme.

BEWIJS. Zij $f: \mathbf{A} \rightarrow \mathbf{B}$ een homomorfisme, en $\theta = \ker f$. Volgens onderdeel (a) van de Homomorfiestelling is er een homomorfisme g zo dat $f = g \circ q_\theta$, en is g injectief. De quotientafbeelding $q_\theta: \mathbf{A} \rightarrow \mathbf{A}/\theta$ is evident surjectief, en volgens Lemma 30 is q_θ een vol homomorfisme van $\mathbf{A}$ op $\mathbf{A}/\theta$.

Als f vol is, dan is g ook vol, volgens onderdeel (b) van de Homomorfiestelling; volgens Definitie 9 en de opmerking boven Gevolg 7 is g dan een inbedding. $\square$

GEVOLG II. Als $f: \mathbf{A} \rightarrow \mathbf{B}$ een vol surjectief homomorfisme is, dan

$$\mathbf{A}/\ker f \cong \mathbf{B}.$$

In het bijzonder $\mathbf{A}/\ker f \cong f[\mathbf{A}]$.

BEWIJS. Zij $f = g \circ q_{\ker f}$. Volgens de Homomorfiestelling is g een vol bijtief homomorfisme; volgens Propositie 11 is g dan een isomorfisme.

In Voorbeeld (i) is opgemerkt dat het afgeleide homomorfisme $f: \mathbf{A} \rightarrow f[\mathbf{A}]$ vol is. $\square$

Omdat $\ker q_\theta = \theta$, voor elke congruentie θ , impliceert gevolg II dat de isomorfieklassen van homomorfe beelden van een structuur $\mathbf{A}$ gerepresenteerd worden door de quotienten van $\mathbf{A}$.

Clausule (c) van de Homomorfiestelling verdient een nadere beschouwing. Laat R een binaire relatie zijn, en f een I -plaatsige operatie. We zullen zeggen dat R gesloten is onder f als

$$\text{voor alle } a, b \text{ zo dat } aR^I b: \text{ als } f(a) \in \text{Vld}(R), \text{ dan } \langle f(a), f(b) \rangle \in R.$$

Merk op dat een relatie die gesloten is onder f ook compatibel is met f . Van een verzameling F van operaties zeggen we dat R gesloten is onder F als R gesloten is onder ieder element van F . Als $\mathbf{A}$ een structuur is, dan zeggen we dat R gesloten is in $\mathbf{A}$ als R gesloten is onder de basisoperaties van $\mathbf{A}$.

32 DEFINITIE. Zij $\mathbf{A}$ een structuur. Een *gesloten congruentierelatie* (of kortweg: *gesloten congruentie*) van $\mathbf{A}$ is een equivalentierelatie op A die gesloten is in $\mathbf{A}$.

33 PROPOSITIE. Zij $\mathbf{A}$ een structuur en $\alpha \in \text{Eqv } A$. Dan is α een gesloten congruentie van $\mathbf{A}$ dan en slechts dan als

$$\forall Q \in \text{Nom } \mathbf{A}: \forall a \in \text{Dom } Q^{\mathbf{A}}: \forall b \in A^{K_Q}: a\alpha^{K_Q} b \Rightarrow \langle Q^{\mathbf{A}}(a), Q^{\mathbf{A}}(b) \rangle \in \alpha.$$

BEWIJS. Omdat $\text{Vld}(\alpha) = A$ is de voorwaarde dat $Q^{\mathbf{A}}(a)$ tot $\text{Vld}(\alpha)$ behoort vervuld als $Q^{\mathbf{A}}(a)$ bestaat. $\square$

Voorbeelden

xv. Als $n \geq 1$, dan is congruentie modulo n geen gesloten congruentie van de structuur $\mathbf{N}$ van Voorbeeld (xiii). Immers, n is congruent met 0 , en 0 met n ; maar $n - 0$ is niet congruent met $0 - n$, omdat $0 - n$ niet bestaat.

xvi. Congruentie modulo 0 is wél een gesloten congruentie, en algemener: in iedere structuur $\mathbf{A}$ is $\Delta_{\mathbf{A}}$ een gesloten congruentie.

xvii. Daarentegen is $\bar{V}_{\mathbf{A}}$ dan en alleen dan een gesloten congruentie van een structuur $\mathbf{A}$ als alle basisoperaties van $\mathbf{A}$ totaal zijn.

We noteren de verzameling der gesloten congruentierelaties van een structuur $\mathbf{A}$ als $\text{C}\bar{\text{on}} \mathbf{A}$. Kennelijk geldt algemeen:

$$\text{C}\bar{\text{on}} \mathbf{A} \subseteq \text{Con } \mathbf{A} \subseteq \text{Eqv } A.$$

In bepaalde gevallen gelden ook omgekeerde inclusies:

34 STELLING. Als $\mathbf{A}$ een algebra is, dan $\text{C}\bar{\text{on}} \mathbf{A} = \text{Con } \mathbf{A}$.

BEWIJS. Zij $\mathbf{A}$ een algebra. Het volstaat te bewijzen dat $\text{Con } \mathbf{A} \subseteq \text{C}\bar{\text{on}} \mathbf{A}$.

Zij $Q \in \text{Nom } \mathbf{A}$. Zij $\theta \in \text{Con } \mathbf{A}$; stel dat voor $a \in \text{Dom } Q^{\mathbf{A}}$ en $b \in A^{K_Q}$ geldt dat $a\alpha^{K_Q} b$. Omdat $Q^{\mathbf{A}}$ totaal is, behoort ook b tot $\text{Dom } Q^{\mathbf{A}}$. Dus volgens Propositie 26, $\langle Q^{\mathbf{A}}(a), Q^{\mathbf{A}}(b) \rangle \in \theta$. $\square$

35 STELLING. Als $\mathbf{A}$ een relationeel stelsel is, dan $\text{Con}\mathbf{A} = \text{Eqv}\mathbf{A}$.

BEWIJS. Zij $\mathbf{A}$ een relationeel stelsel. Het volstaat te bewijzen dat

$$\text{Eqv}\mathbf{A} \subseteq \text{Con}\mathbf{A}.$$

Zij $R \in \text{Nom}\mathbf{A}$. Er is een index $k^* \in K_R$ zo dat voor alle $a \in A^{K_R}$:

$$R^{\mathbf{A}}(a) \simeq a_{k^*}.$$

Zij $\alpha \in \text{Eqv}\mathbf{A}$; stel dat voor $a, b \in \text{Dom} R^{\mathbf{A}}$ geldt dat $a\alpha^{K_R}b$. Dan geldt in het bijzonder dat $a_{k^*}\alpha b_{k^*}$, dus $R^{\mathbf{A}}(a) \equiv R^{\mathbf{A}}(b) (\alpha)$. $\square$

OPMERKING. Een equivalentie op het domein van een relationeel stelsel is niet per se een *gesloten* congruentie. Als $a \in \text{Dom} R^{\mathbf{A}}$ en $a\alpha^{K_R}b$, dan is het wel zo dat $a_{k^*}\alpha b_{k^*}$, maar daar volgt alleen uit dat $R^{\mathbf{A}}(a) \equiv R^{\mathbf{A}}(b) (\alpha)$ als $b \in \text{Dom} R^{\mathbf{A}}$.

Voorbeeld xviii. Zij $\mathbf{Q} = \langle Q, \prec \rangle$ een quasi-orde. Definieer een relatie θ op Q door

$$p\theta q :\Leftrightarrow p \prec q \ \& \ q \prec p.$$

Dan is θ een equivalentie, en dus een congruentie van $\mathbf{Q}$. Het quotient $\mathbf{Q}/\theta$ noemen we het *antisymmetrisch quotient* van $\mathbf{Q}$. In §F is opgemerkt (Voorbeeld ii) dat $\mathbf{Q}/\theta$ een orde is. Als f een homomorfisme is van $\mathbf{Q}$ naar een orde, dan $\theta \subseteq \ker f$; al zulke homomorfismen factoriseren dus door de quotientafbeelding q_θ .

36 LEMMA. Als η en θ congruenties zijn van een structuur $\mathbf{A}$, $\eta \subseteq \theta$, en θ is gesloten, dan is η ook gesloten.

BEWIJS. Zij Q een K -plaatsige basisoperatie van $\mathbf{A}$; stel $a\eta^K b$ en $a \in \text{Dom} Q$. Dan ook $a\theta^K b$, want $\eta \subseteq \theta$. Dus $\langle Q(a), Q(b) \rangle \in \theta$ wegens geslotenheid. Dus $b \in \text{Dom} Q$. Dus $\langle Q(a), Q(b) \rangle \in \eta$ omdat η een congruentie is. $\square$

37 PROPOSITIE. (a) Een vol homomorfisme met gesloten kern is gesloten.
(b) De kern van een gesloten homomorfisme is gesloten.

BEWIJS. Laat een vol homomorfisme $f: \mathbf{A} \rightarrow \mathbf{B}$ gegeven zijn; definieer $\theta := \ker f$.
(a) Stel dat θ gesloten is. Als $f \circ a \in \text{Dom} Q^{\mathbf{B}}$, dan is er, omdat f vol is, een familie $a' \in \text{Dom} Q^{\mathbf{A}}$ zo dat $f \circ a' = f \circ a$. Dus $a'\theta^{K_Q}a$, en omdat $a' \in \text{Dom} Q^{\mathbf{A}}$,

$$\langle Q^{\mathbf{A}}(a'), Q^{\mathbf{A}}(a) \rangle \in \theta.$$

In het bijzonder geldt dan dat $a \in \text{Dom} Q^{\mathbf{A}}$.

(b) Stel dat f gesloten is. Stel dat $a\theta^{K_Q}b$ en $a \in \text{Dom} Q^{\mathbf{A}}$. Er geldt dat $f(Q^{\mathbf{A}}(a)) = Q^{\mathbf{B}}(f \circ a)$ omdat f een homomorfisme is. Maar $a\theta^{K_Q}b$ betekent dat $f \circ a = f \circ b$, dus $f \circ b \in \text{Dom} Q^{\mathbf{B}}$; omdat f gesloten is, volgt daaruit dat $b \in \text{Dom} Q^{\mathbf{A}}$. Maar

$$f(Q^{\mathbf{A}}(b)) = Q^{\mathbf{B}}(f \circ b) = f(Q^{\mathbf{A}}(a)),$$

dus $\langle Q^{\mathbf{A}}(a), Q^{\mathbf{A}}(b) \rangle \in \theta$. $\square$

Voorbeeld xix. Laat $\mathbf{A}$ een structuur zijn; stel $\mathcal{N} \subset \text{Nom}\mathbf{A}$. Dan is $1_{\mathbf{A}}$ een niet-gesloten homomorfisme van $\mathbf{A} \upharpoonright \mathcal{N}$ op $\mathbf{A}$, maar $\ker 1_{\mathbf{A}} = \Delta_{\mathbf{A}}$, dus $\ker 1_{\mathbf{A}}$ is gesloten.

GEVOLG. Zij $\mathbf{A}$ een structuur, en $\theta \in \text{Con}\mathbf{A}$. Dan is de quotientafbeelding q_θ gesloten dan en slechts dan als θ gesloten is.

Oefeningen

§D

1. Verifieer dat de drietallen $\langle Y, f, X \rangle$ van verzamelingen Y en X en een operatie $f: Y \leftarrow\!\!\!\circ\!\!\! X$, met samenstelling

$$\langle Y, f, X \rangle \circ \langle U, g, V \rangle \simeq \langle Y, f \circ g, V \rangle \triangleleft X = U,$$

een categorie vormen. Hoe verhoudt die categorie zich tot **Rel** en **Vrz**?

2(a) Bewijs dat de surjecties, met verzamelingen als objecten en samenstelling gebaseerd op functiesamenstelling, een categorie vormen.

(b) Insgelijks voor de injecties.

3. Bewijs dat een pijl u in een categorie een eenheidselement is dan en slechts dan als $\forall f. u \circ f \simeq f$.

4. Zij $\mathbf{X} = \langle X, d, b \rangle$ een gerichte graaf. Definieer een structuur

$$\mathbf{C}(\mathbf{X}) := \langle C(\mathbf{X}), \circ, \mathbf{d}, \mathbf{b} \rangle$$

als volgt. Het domein $C(\mathbf{X})$ bestaat uit de *paden* van $\mathbf{X}$, i.e. de rijtjes $\langle x_0, \dots, x_{2k} \rangle$ zo dat

x_{2i} ($i \leq k$) een knoop is,

x_{2i+1} ($i < k$) een kant,

en voor alle $i < k$, $\mathbf{b}(x_{2i+1}) = x_{2i}$ en $\mathbf{d}(x_{2i+1}) = x_{2i+2}$.

Laten we rijtjes nu als woorden schrijven, i.e. zonder haakjes, komma's of spaties (cf. §E, Voorbeeld (i)). Voor elk pad $x_0 \dots x_{2k}$ definiëren we:

$$\mathbf{b}(x_0 \dots x_{2k}) = x_0 \text{ en } \mathbf{d}(x_0 \dots x_{2k}) = x_{2k};$$

voor paden $x_0 \dots x_{2k}$ en $y_0 \dots y_{2m}$ bestaat $x_0 \dots x_{2k} \circ y_0 \dots y_{2m}$ dan en slechts dan als $x_{2k} = y_0$, en dan is het $y_0 \dots y_{2m}$ ingeval $k = 0$, en anders $x_0 \dots x_{2k-1} y_0 \dots y_{2m}$.

Bewijs dat $\mathbf{C}(\mathbf{X})$ een categorie is.

§E

1. Zij $\langle X, \cdot \rangle$ een groeпоїde, en $\equiv$ een equivalentierelatie op X die voldoet aan de voorwaarde

$$\text{als } x \equiv y \text{ en } u \equiv z, \text{ dan } x \cdot u \equiv y \cdot z. \quad (*)$$

(Een dergelijke relatie heet een *congruentierelatie*, zie §H.) Definieer producten van rijtjes van elementen van X inductief, als volgt:

x is het product van het eenlingrijtje $\langle x \rangle$;

als $1 \leq n < m$, s een product is van $\langle x_1, \dots, x_n \rangle$, en t een product van $\langle x_{n+1}, \dots, x_m \rangle$, dan is $s \cdot t$ een product van $\langle x_1, \dots, x_m \rangle$.

Bewijs: als $x \cdot (y \cdot z) \equiv (x \cdot y) \cdot z$ voor alle $x, y, z \in X$, dan $s \equiv t$ wanneer s en t producten zijn van hetzelfde rijtje.

2. Zij $\mathbf{A} = \langle A, \cdot \rangle$ een halfgroep en f een afbeelding van een verzameling X naar het domein A . Bewijs dat er precies één homomorfisme f^+ bestaat van de halfgroep $\mathbf{X}^+ = \langle X^+, * \rangle$ naar $\mathbf{A}$ dat f uitbreidt.

3. Zij X een niet-lege verzameling; definieer M als $\mathcal{P}(X \times X)$, en $\mathbf{M}$ als $\langle M, \circ \rangle$, waarin $\circ$ de samenstellingsoperatie is. Laat zien dat $\mathbf{M}$ een monoïde is.

4. Een *links eenheidselement* in een halfgroep $\langle X, \cdot \rangle$ is een element e zo dat voor alle $x \in X$, $ex = x$. Een *linksinverse* van x in een halfgroep $\langle X, \cdot \rangle$ tot een element

e is een element y zo dat $yx = e$. Bewijs: een halfgroep met een links eenheidselement waartoe ieder element van de halfgroep een linksinverte heeft is een groep.

5. Laat zien dat in elke ring de gelijkheden

$$0 \cdot x = x \cdot 0 = 0$$

en

$$x \cdot (-y) = (-x) \cdot y = -(xy)$$

gelden.

6. Zij X een niet-lege verzameling. Bestaat er een ring $\mathbf{R}$ zo dat $\mathbf{X}^*$ een expansie is van de multiplicatieve halfgroep van $\mathbf{R}$?

7. Zij $\mathbf{A} = \langle A, +, 0, - \rangle$ een groep. Definieer $f + g$, voor afbeeldingen f en g van A in zichzelf, door

$$(f + g)(x) = f(x) + g(x).$$

(a) Bewijs dat $\langle A^A, + \rangle$ een groep is.

Neem voor de volgende onderdelen aan dat $\mathbf{A}$ abels is.

(b) Bewijs dat $\mathbf{End} \mathbf{A} := \langle \mathbf{End} \mathbf{A}, +, \circ \rangle$ een ring is met eenheidselement.

(c) Definieer de operatie $\bullet$ op A^A door

$$f \bullet g = g \circ f,$$

en zij $\mathbf{End}^\theta \mathbf{A} := \langle \mathbf{End} \mathbf{A}, +, \bullet \rangle$. Constateer dat $\mathbf{End}^\theta \mathbf{A}$ een ring is met eenheidselement.

8. Zij $\mathbf{R} = \langle R, +, 0, -, \cdot \rangle$ een algebra waarvan het reduct $\mathbf{R}_0 = \langle R, +, 0, - \rangle$ een groep is en het reduct $\mathbf{R}_1 = \langle R, \cdot \rangle$ een halfgroep, en die voldoet aan de distributieve wetten van Voorbeeld (v).

(a) Laat zien dat de operatie $+$ niet noodzakelijk commutatief is.

(b) Definieer de *linkse actie* van een element $x \in R$ als de afbeelding

$$l_x: y \mapsto x \cdot y$$

van R in zichzelf. Analoog is er een *rechtse actie*

$$r_x: y \mapsto y \cdot x.$$

Laat zien dat l_x en r_x endomorfismen zijn van $\mathbf{R}_0$.

(c) Bewijs dat $l: x \mapsto l_x$ een homomorfisme is van $\mathbf{R}$ naar (een expansie van) $\mathbf{End} \mathbf{R}$.

(d) Bewijs dat $r: x \mapsto r_x$ een homomorfisme is van $\mathbf{R}$ naar (een expansie van) $\mathbf{End}^\theta \mathbf{R}$.

(e) Bewijs dat $\mathbf{R}_0$ abels is als l of r injectief is.

(f) Bewijs dat l injectief is als er een $x \in R$ bestaat zo dat r_x injectief is, en dat r injectief is als er een $x \in R$ bestaat zo dat l_x injectief is.

(g) Concludeer dat $\mathbf{R}_0$ abels is als $\mathbf{R}_1$ een eenheidselement bezit.

9. Bewijs dat voor ieder element x van een begrensde tralie geldt dat $x \vee 1 = 1$ en $x \wedge 0 = 0$.

10. Bewijs dat in ieder tralie de distributieve wetten (1) en (2) van Voorbeeld (viii) equivalent zijn.

11. Een *Boolese ring* is een ring $\mathbf{R} = \langle R, +, 0, -, \cdot \rangle$ met idempotente vermenigvuldiging.

- (a) Laat zien dat in Boolese ringen de gelijkheid $x + x = 0$ geldt (zodat $x = -x$), en de vermenigvuldiging commutatief is.
- (b) Zij $\langle B, \vee, \wedge, 0, 1, \neg \rangle$ een Boole-algebra. Definieer:

$$b + c := (b \wedge \neg c) \vee (\neg b \wedge c); b \cdot c := b \wedge c; \text{ en } -b := b.$$

Verifieer dat $\langle B, +, 0, 1, -, \cdot \rangle$ een Boolese ring is met multiplicatief eenheidselement 1.

- (c) Zij $\langle R, +, 0, 1, -, \cdot \rangle$ een Boolese ring met multiplicatief eenheidselement 1. Definieer operaties $\vee, \wedge$ en $\neg$ zo dat $\langle R, \vee, \wedge, 0, 1, \neg \rangle$ een Boole-algebra is.

12. (Generalisatie van de distributieve wetten). Schrijf $(X \cup Y) \cap (Z \cup W)$ als een vereniging van doorsneden van X, Y, Z en W . Wat is de formule in het algemene geval, voor een doorsnede

$$\bigcap_{i \in I} \bigcup_{j \in J_i} X_{ij}?$$

(Het dualiteitsprincipe impliceert dat een soortgelijke wet geldt voor de distributie van vereniging over doorsnede.)

13. Zij $\mathbf{R} = \langle R, +, 0, -, \cdot \rangle$ een delingsring. (N.B.: we rekenen het multiplicatieve eenheidselement hier *niet* tot de basisoperaties.) Bewijs: als $f: \mathbf{R} \rightarrow \mathbf{S}$ een ringhomomorfisme is, en f is niet injectief, dan $\text{Im } f = \{0\}$.

§F

- Bewijs dat Δ_X de enige relatie is over X die zowel een equivalentierelatie is als een ordening van X .
- Definieer, voor structuren $\mathbf{Q} = \langle Q, R \rangle$ met één binaire relatie,

$$\begin{aligned} Z(\mathbf{Q}) &= \langle Q, R \cup \Delta_Q \rangle, \\ S(\mathbf{Q}) &= \langle Q, R \setminus R^{-1} \rangle. \end{aligned}$$

Bewijs dat een quasioorde $\mathbf{Q}$ een orde is dan en slechts dan als $ZS(\mathbf{Q}) = \mathbf{Q}$.

3. Een *echte deler* van een geheel getal x is een geheel getal $y \neq x$ dat een deler is van x . Beschouw de relatie $\{\langle m, n \rangle \in \mathbb{N} \times \mathbb{N} \mid m \text{ is een echte deler van } n\}$. Is ze gefundeerd?

4. Bewijs dat een relatie R *niet* gefundeerd is dan en slechts dan als er een rij $\langle x_n \mid n \in \mathbb{N} \rangle$ bestaat zo dat voor elke $n \in \mathbb{N}$, $x_{n+1} R x_n$.

5. Zij $\langle X, R \rangle$ een quasioorde. Definieer een binaire operatie $\circ$ over R door

$$\langle x, y \rangle \circ \langle u, v \rangle := \langle x, v \rangle \triangleleft y = u.$$

Bewijs dat $\langle R, \circ, \Delta_X \rangle$ een categorie is.

6. Zij $\mathbf{C} = \langle C, \circ, E \rangle$ een categorie. Bewijs dat

$$\langle E, \{\langle u, v \rangle \in E^2 \mid \mathbf{C}[u \leftarrow v] \neq \emptyset\} \rangle$$

een qoza is.

7. Laat, voor elke categorie $\mathbf{C}$, $\mathbf{C}^R$ het relationale stelsel zijn gedefinieerd in de vorige oefening; en voor elke quasioorde $\mathbf{Q}$, $\mathbf{Q}^K$ de categorie gedefinieerd in Oefening 5. Zij $\mathbf{X}$ een quasioorde.

(a) Toon aan dat $(\mathbf{X}^K)^R \cong \mathbf{X}$.

(b) Verifieer dat $(\mathbf{X}^\partial)^K \cong (\mathbf{X}^K)^\partial$, en dat voor elke categorie $\mathbf{C}$, $(\mathbf{C}^\partial)^R = (\mathbf{C}^R)^\partial$.

§G

- Bewijs Propositie 1.
- Verifieer Voorbeeld (i).
- Verifieer Voorbeeld (iv).

4. Verifieer Voorbeeld (vi).

5. De orde $\mathbf{2}$ heeft domein $\{0, 1\}$, met $0 \leq 1$. Bewijs dat $\mathbf{2}$ isomorf is met de orde $\mathbf{P}\{0\} := \langle \mathcal{P}\{0\}, \subseteq \rangle$.

6. Laat f en g isomorfe pijlen zijn met hetzelfde domein. Is het algemeen waar dat er een isomorfisme h bestaat zo dat $hf = g$?

7(a) Karakteriseer de secties en de retracties in **Rel**.

(b) Bewijs dat ieder monomorfisme in **Rel** een sectie is.

(c) Concludeer dat in **Rel** alle epimorfismen retracties zijn.

8. Laat $\mathbf{P}: \mathbf{Rel} \rightarrow \mathbf{Vr}$ de functor zijn die is gedefinieerd in Voorbeeld (xii) van §D.

Bewijs dat $\langle X, R, Y \rangle$ een monomorfisme is in **Rel** dan en slechts dan als $\mathbf{P}(X, R, Y)$ een monomorfisme is in **Vr**, en een epimorfisme dan en slechts dan als $\mathbf{P}(Y, R^{-1}, X)$ een monomorfisme is.

§H

Ga na dat een bijectief homomorfisme van een algebra naar een gelijknamige structuur noodzakelijkerwijs vol is, en dus een isomorfisme.