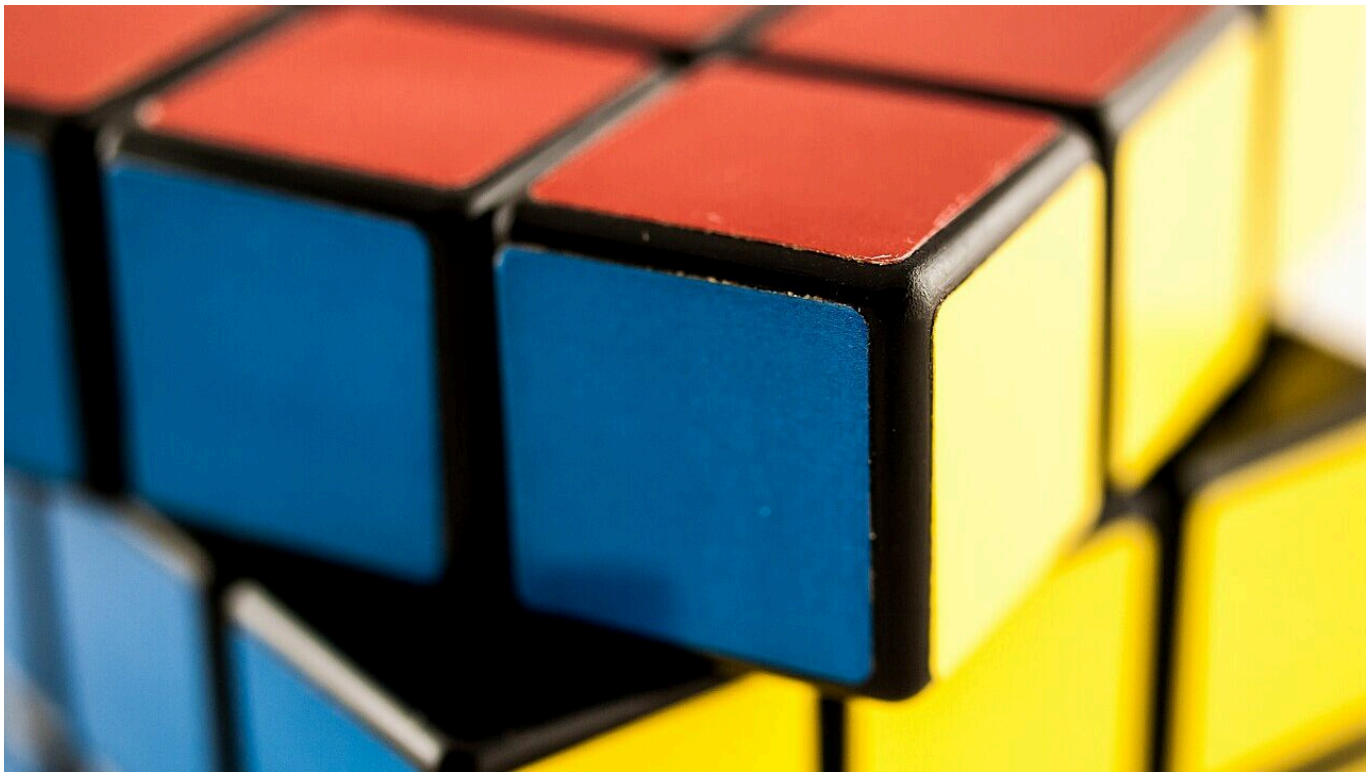
Representatietheorie (3): Groepentheorie

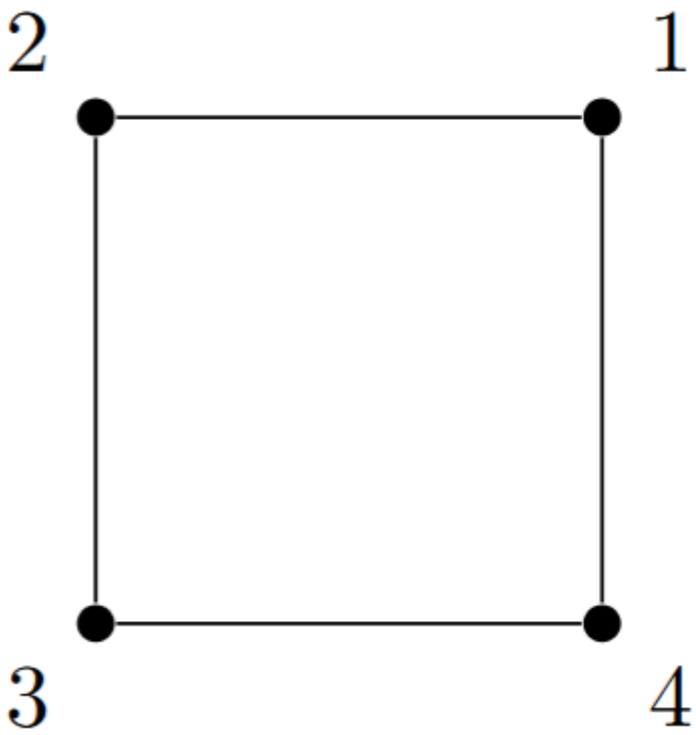
Symmetrie vormt een sleutelbegrip in de moderne natuurkunde. Zo ligt door de symmetrie van de ruimte vast welke elementaire deeltjes zouden kunnen bestaan, komt elektromagnetisme voort uit een interne rotatiesymmetrie en worden de kleuren van quarks bepaald door de symmetrie van hun interactie. Vanuit wiskundig oogpunt wordt symmetrie beschreven door zogeheten groepen en representaties, maar hoe leidt dit tot natuurkunde? Op weg naar het antwoord op die vraag besprak ik in deze serie al verzamelingenleer en lineaire algebra. In dit artikel komt het laatste ingrediënt aan bod: groepentheorie.



Een Rubik's-kubus. De operaties die je op een dergelijke kubus kunt doen zijn een voorbeeld van wat wiskundigen een "groep" noemen.

Een vierkant

Groepentheorie zou kunnen worden omschreven als de theorie van symmetrieën. Dat komt doordat de wiskundige axioma's van groepen gemodelleerd zijn naar de eigenschappen die we van symmetrieën kennen. Om dit te begrijpen, kunnen we het beste een voorbeeld in gedachten nemen. Hiervoor beschouwen we een vierkant:



Afbeelding 1. Een vierkant. Een vierkant met de hoekpunten genummerd van 1 tot en met 4.

Een *symmetrie* van het vierkant is een handeling waarmee we, na het uitvoeren van de handeling, weer een soortgelijk vierkant terugkrijgen. Een voorbeeld is een rotatie van 90 graden: als we het vierkant 90 graden draaien, is het plaatje niet veranderd. We kunnen nog twee rotaties doen die dat voor elkaar krijgen, namelijk een van 180 graden of een van 270 graden. Een flauwe handeling, maar ook een symmetrie, is niets doen. Dit noemen we de identiteitshandeling. Als we willen dat het vierkant niet verandert, kunnen nog meer doen dan roteren, namelijk spiegelen. Het spiegelen kan over vier assen: een horizontale as, een verticale as en twee diagonale assen. Zo hebben we in totaal 8 verschillende handelingen die het vierkant onveranderd laten.

Twee zulke symmetriehandelingen kunnen worden gecombineerd, en de combinatie van twee handelingen is opnieuw een symmetrie: als je iets doet waardoor het vierkant niet verandert, en je doet nóg iets waardoor het vierkant niet verandert, dan blijft ook na die twee handelingen het vierkant natuurlijk onveranderd. Het blijkt dat het combineren van twee rotaties opnieuw een rotatie geeft (of de identiteitshandeling), terwijl de combinatie van een rotatie en een spiegeling precies één van de andere spiegelingen is. De combinatie van twee spiegelingen, ten slotte, geeft een rotatie (of de identiteitshandeling). Het is een leuke opdracht om deze eigenschappen voor jezelf na te gaan. Verder blijkt dat deze handelingen ook álle symmetrieën van het vierkant zijn, wat rigoureus kan worden aangetoond door te kijken waar de hoekpunten 1 t/m 4 eindigen na de handelingen.

Ten slotte kun je zien dat er voor elke handeling precies één andere handeling is waarvoor geldt dat, als we de twee combineren, we de identiteitshandeling krijgen. Eerst roteren over 90 graden en daarna over 270 graden geeft bijvoorbeeld een rotatie over 360 graden, wat hetzelfde is als niets doen[1].

De verzameling van alle symmetriehandelingen van het vierkant samen noemen wiskundigen een groep, en het voorbeeld geeft al goed weer wat de axioma's van een groep zijn. Ik zal hier preciezer op in gaan.

Groepen

Zoals ik in het eerste artikel in deze serie heb uitgelegd, bestaat een groot deel van de wiskunde uit de studie van verzamelingen die voldoen aan een aantal eisen. In het vorige artikel liet ik zien wat de eisen waren waar een *vectorruimte* aan moet voldoen. In dit artikel bestuderen we een andere structuur: die van groepen.

Een *groep* is een verzameling G met een *operatie* $\cdot$ die elementen $a,b\in G$ combineert tot een nieuw element $a\cdot b \in G$. Verder moet de verzameling met operatie voldoen aan een drietal eisen:

- De operatie moet *associatief* zijn, wat wil zeggen dat voor elke drie elementen $a,b,c\in G$, de uitkomst van $(a\cdot b)\cdot c$ gelijk is aan die van $a\cdot (b\cdot c)$.
- Er is een *identiteitselement* $e\in G$, vaak ook de *eenheid* genoemd, waarvoor geldt

dat $e\cdot a=a\cdot e=a$ voor alle $a\in G$. Het identiteitselement is uniek, oftewel, er is precies één identiteitselement.
- Elk element heeft een *inverse*, wat wil zeggen dat er voor elke $a\in G$ een $b\in G$ bestaat zodat $a\cdot b=b\cdot a=e$. Dit element b is uniek, en wordt aangeduid met a^{-1}.

We zagen hierboven al een voorbeeld van een groep: de verzameling van symmetrieën van een vierkant, waarbij de operatie $\cdot$ simpelweg “de handelingen na elkaar doen” is. De afspraak hierbij is dat we $a \cdot b$ interpreteren als “éérst b doen, en dán a. Deze groep wordt ook wel D_4 genoemd. Op dezelfde manier vormen de symmetrieën van andere veelhoeken ook groepen. Laat ik daarnaast nog een aantal voorbeelden beschrijven.

Om te beginnen: de gehele getallen, die ik in het eerste artikel in deze serie heb beschreven en aanduid met $\mathbb{Z}$. Om deze verzameling van getallen tot een groep te maken, hebben we een operatie nodig. Die wordt gegeven door het optellen van getallen[2]. Dit is een goed bepaalde operatie op de verzameling van gehele getallen, omdat de som van elke twee gehele getallen opnieuw een geheel getal is. De verzameling van gehele getallen met optelling vormt inderdaad een groep, wat we kunnen verifiëren door de verschillende eisen na te gaan. Ten eerste is optelling associatief, want voor alle $a,b,c\in\mathbb{Z}$ geldt dat $(a+b)+c=a+(b+c)$. Het identiteitselement is het getal 0. En ten slotte is de inverse van $a\in\mathbb{Z}$ gegeven door[3] $a^{-1}=-a$, want $a+ (-a)=0=(-a)+a$.

Een ander bekend voorbeeld van een groep is de cyclische groep van orde 12, aangeduid met $\mathbb{Z}_{12}$. Dit klinkt misschien buitenaards, maar waarschijnlijk gebruik je deze groep dagelijks. Hij zit namelijk verscholen achter het idee van klokkijken. De cyclische groep van orde 12 bestaat als verzameling uit de getallen $\mathbb{Z}_{12}= \{0,1,2,...,11 \}$. De operatie is optelling, waarbij de som van twee getallen ofwel hun som in $\mathbb{Z}$ is (als de uitkomst niet groter is dan elf), ofwel hun som in $\mathbb{Z}$ minus twaalf (als de oorspronkelijke uitkomst wel groter is dan elf). Dat wil zeggen: $3+5=8$, maar $9+6=3$. Deze optelling kennen we van de 12-uursklok, waar de tijd altijd tussen de 0 en 12 ligt: als het nu 9 uur is, dan is het 6 uur later niet 15 uur, maar 3 uur. Vanuit de definitie van de optelling is het duidelijk dat de som van twee getallen opnieuw tussen de 0 en 12 ligt. Je kan voor jezelf nagaan dat deze optelling ook associatief is. Het

identiteitselement is 0. De inverse van $a\in\mathbb{Z}_{12}$ is $12-a$. Inderdaad laat een berekening zien dat $a+(12-a)=0=(12-a)+a$. Uiteraard kunnen we het getal 12 ook vervangen door andere (natuurlijke) getallen, om zo cyclische groepen van andere ordes te krijgen.

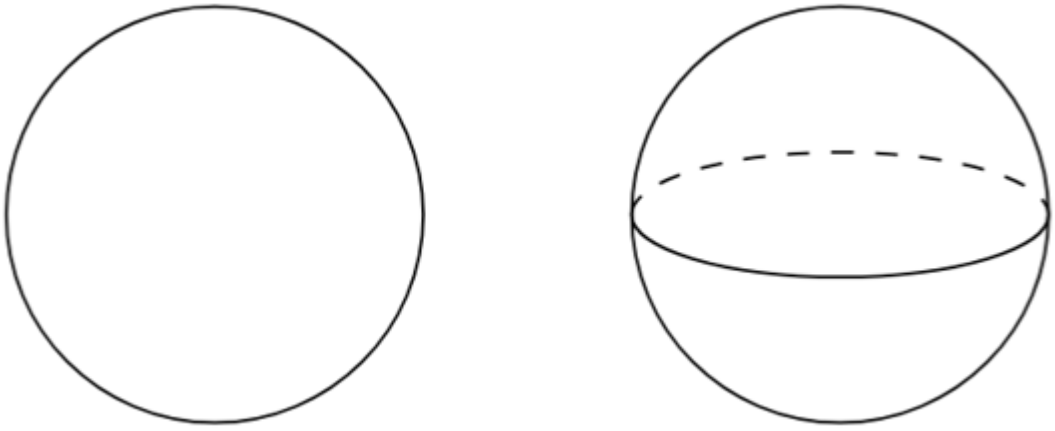
Afbeelding 2: Een klok. Voor het klokkijken gebruik je de cyclische groep van orde 12. Bron: public domain vectors.

Alle drie de voorbeelden die ik nu heb beschreven zijn voorbeelden van *discrete groepen*, wat betekent dat de bijbehorende verzamelingen uit losse elementen bestaan[4]. Er zijn ook *continue groepen*; laat ik daar ook een paar voorbeelden van beschrijven. Allereerst vormen de reële getallen $\mathbb{R}$ een groep onder optelling, op dezelfde manier als we hierboven zagen voor de gehele getallen. Die groep wordt genoteerd als $(\mathbb{R},+)$.

De reële getallen vormen ook *bijna* een groep onder vermenigvuldiging. Ik zeg bijna, omdat

er een klein probleem is. De eenheid van vermenigvuldiging is het getal 1, en voor de meeste reële getallen $a\in\mathbb{R}$ geldt dat er een ander getal is waarmee het vermenigvuldigt tot 1 – een inverse dus, zoals in de tweede eis voor groepen – namelijk: $1/a$. Dit gaat alleen mis als $a=0$. Dus pas als we 0 weglaten uit de verzameling krijgen we een groep onder vermenigvuldiging. Deze groep wordt aangeduid met $\mathbb{R}^*$.

Het laatste voorbeeld van groepen dat ik nog wil behandelen is dat van groepen van rotaties. We hebben gezien dat we het vierkant maar op vier daadwerkelijk verschillende manieren konden roteren zodat we het vierkant terugkregen, namelijk over 0, 90, 180 of 270 graden. Een cirkel daarentegen kan over een willekeurige hoek worden gedraaid zonder te veranderen. De groep van rotatiesymmetrieën van de cirkel is dus een continue groep, en deze groep wordt $SO(2)$ genoemd. Een cirkel kun je zien als een “bal in twee dimensies”. Als we een “normale” bal beschouwen, oftewel een bal in drie dimensies, kan die over willekeurige hoeken in verschillende richtingen worden gedraaid. De groep van symmetrieën die op die manier wordt verkregen heet $SO(3)$. Je kan je misschien voorstellen dat we dit kunnen doorzetten naar “ballen” in nog meer dimensies. De groep van rotaties van een bal in d dimensies heet $SO(d)$.



Afbeelding 3. Een cirkel en een bal. De symmetriegroep van een cirkel (links) is SO(2). De symmetriegroep van een bal (rechts) is SO(3).

Homomorfismen

Voor verzamelingen besprak ik in het eerste artikel van deze serie *functies* van één verzameling naar een andere. Voor vectorruimtes vertelde ik dat we naar functies tussen

vectorruimten kijken die de lineaire structuur behoudt. Op diezelfde manier bekijken wiskundigen functies tussen groepen die de groepsstructuur behoudt. Zulke functies heten *homomorfismen*.

Om precies te maken wat dit betekent, hebben we twee groepen nodig; laat ik die G en H noemen. Ik noteer de uitkomst van de operatie op twee elementen $g_1, g_2\in G$ als $g_1 g_2$ (de $\cdot$ laten we voor het gemak dus weg), en ik gebruik dezelfde notatie voor elementen van H. Een homomorfisme $f:G\rightarrow H$ is een functie van G naar H zodat voor alle $g_1, g_2 \in G$ geldt dat $f(g_1 g_2)=f(g_1) f(g_2)$. In woorden: het maakt niet uit of je éérst vermenigvuldigt en dan de functie toepast, of dat je eerst de functie toepast op de losse elementen en dan pas vermenigvuldigt.

Een wiskundige die deze definitie voor het eerst ziet, zou zich afvragen of dit genoeg is. Om de structuur van de groep te behouden zou je namelijk willen dat ook de eenheid van G naar de eenheid van H wordt gestuurd, en dat de inverse van $g\in G$ naar de inverse van $f(g)$ wordt gestuurd. Het zou natuurlijker aanvoelen om dit ook te eisen van een homomorfisme, maar het blijkt dat deze natuurlijke eigenschappen automatisch al volgen uit de ene eis hierboven. Ik zal laten zien waarom dit zo is voor de eenheid.

Laat ik de eenheid van G noteren met e_G, en de eenheid van H met e_H. Dan geldt dat

$$f(e_G)=f(e_G e_G)$$

omdat e_G de eenheid in G is, en als we nu gebruiken dat f een homomorfisme is geldt ook dat

$$f(e_G)= f(e_G) f(e_G).$$

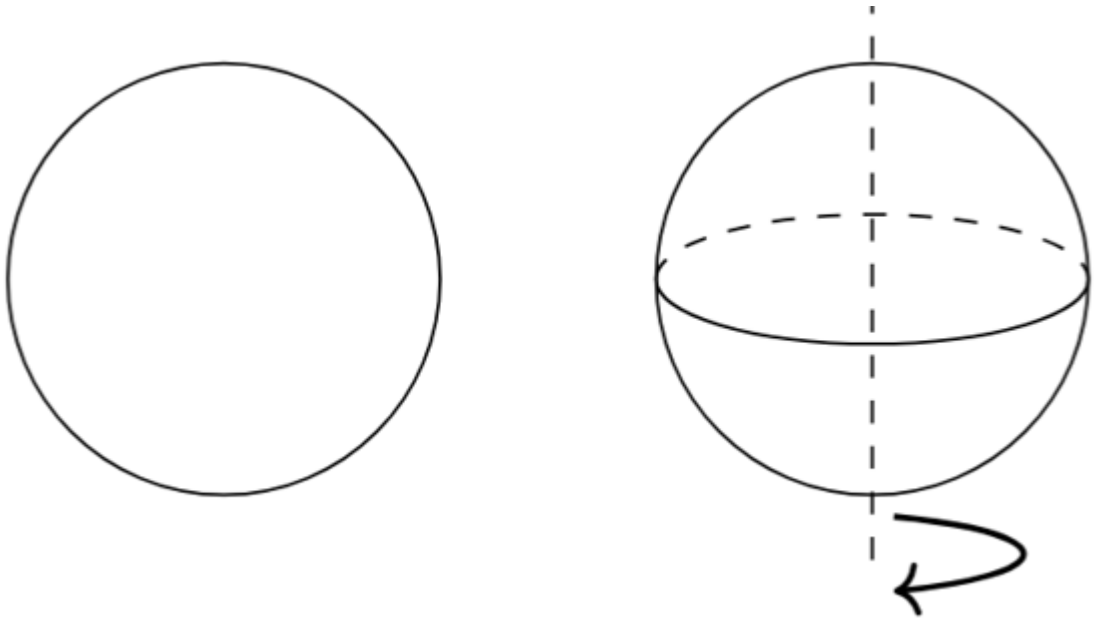
Als je nu beide kanten van de gelijkheid van rechts vermenigvuldigt met $f(e_G)^{-1}$, en gebruikt dat $f(e_G)f(e_G)^{-1}=e_H$ en vervolgens dat $f(e_G)e_H=f(e_G)$, vind je dat $e_H=f(e_G)$. Dus inderdaad wordt de eenheid van G naar de eenheid van H gestuurd. Eenzelfde soort bewijs kan worden gegeven om te laten zien dat voor elke $g\in G$ geldt dat $f(g^{-1})=f(g)^{-1}$. Ik laat het aan de enthousiaste lezer over om dit als opgave zelf te proberen.

Een voorbeeld van een homomorfisme is de functie van de cyclische groep van orde vier naar de symmetrieën van het vierkant: $f:\mathbb{Z}_4 \rightarrow D_4$, die gedefinieerd wordt door

$$f(0)=r_0, f(1)=r_{90}, f(2)=r_{180}, f(3)=r_{270}.$$

Hier staat bijvoorbeeld r_{90} voor een rotatie met 90 graden, en de andere r_n zijn op dezelfde manier gedefinieerd. Het is inderdaad niet lastig om in te zien dat $f(n+m)=f(n)f(m)$, voor $n,m\in\{0,1,2,3\}$, doordat bijvoorbeeld $r_{270}r_{180}=r_{90}$.

Een ander voorbeeld van een homomorfisme is $\varphi:SO(2)\rightarrow SO(3)$, gedefinieerd door $SO(2)$ af te beelden rotaties rondom een vast gekozen as door de bol die $SO(3)$ definieert. Dit homomorfisme is afgebeeld in de onderstaande afbeelding. Het voorbeeld kan worden gegeneraliseerd naar homomorfismen $\varphi:SO(p)\rightarrow SO(p+q)$, voor $p,q\in \mathbb{N}$.



Afbeelding 4. Van SO(2) naar SO(3). Er bestaat een homomorfisme van SO(2) naar SO(3) door af te beelden op rotaties rondom de verticale as.

Isomorfismen

Speciale soorten functies zijn, zoals we al in de twee eerdere artikelen zagen, injecties, surjecties en bijecties. Deze zijn ook voor groepen belangrijk. De twee voorbeelden van

homomorfismen van hierboven zijn bijvoorbeeld beide injectief (verschillende elementen worden nooit op hetzelfde element afgebeeld), maar niet surjectief (niet elk element kun je “bereiken” met de functie). Een voorbeeld van een surjectief homomorfisme is het homomorfisme van de groep van symmetrieën van het vierkant, D_4, naar de cyclische groep $\mathbb{Z}_2$, die de rotaties naar het getal 0 stuurt, en die de spiegelingen naar het getal 1.

Een bijectief homomorfisme, dus een homomorfisme dat zowel injectief als surjectief is, wordt een *isomorfisme* genoemd. Als twee groepen isomorf zijn, dan zijn ze eigenlijk gewoon dezelfde groep. Dan wordt namelijk elk element van de ene groep naar precies één element van de andere groep gestuurd, elk element in die andere groep wordt zo ook bereikt, en de groepsoperatie van beide groepen is hetzelfde.

Ondergroepen

Voor verzamelingen heb ik uitgelegd wat deelverzamelingen zijn, en voor vectorruimtes heb ik verteld wat deelruimtes zijn. Hetzelfde concept bestaat voor groepen; hier noemen wiskundigen een groep die deel uitmaakt van een andere groep een *ondergroep*. Om precies te zijn: een ondergroep H van een groep G is een deelverzameling van die groep, die de identiteit bevat, dus $e_G\in H$; die inverses bevat, wat wil zeggen dat voor elke $h\in H$, ook $h^{-1}\in H$; en waarvoor het product van elke twee elementen in H ook weer in H bevat is. Meestal is de ondergroep H dus een kleinere groep die zich “in G bevindt”, maar ook de hele groep G is volgens deze definitie dus een ondergroep van zichzelf.

Een voorbeeld van een ondergroep zijn de vier rotaties in de symmetriegroep D_4 van het vierkant; alle elementen behalve de spiegelingen, dus. Inderdaad is, zoals ik hierboven al noemde, een combinatie van twee rotaties opnieuw een rotatie, en is de identiteit ook een rotatie, over 0 graden. De vier spiegelingen vormen daarentegen geen ondergroep: ten eerste is de identiteit geen spiegeling, en ten tweede is de combinatie van twee spiegelingen zelf geen spiegeling, maar een rotatie.

In $SO(3)$ vormt het beeld van $SO(2)$ onder het eerder beschreven homomorfisme φ een ondergroep. Iets soortgelijks blijkt algemener te gelden: het beeld $\psi(G_1)$ van een groepshomomorfisme $\psi:G_1\rightarrow G_2$ is een ondergroep van G_2.

Als opgave kun je proberen om dit te bewijzen.

Een belangrijk voorbeeld

We hebben een aantal voorbeelden gezien van groepen. Sommige van deze groepen waren groepen van symmetrieën van een object, zoals de symmetrieën van een vierkant. Andere waren bijvoorbeeld de cyclische groepen of de reële getallen met vermenigvuldiging. Wat al deze groepen gemeen hebben, is dat een groepselement gezien kan worden als een functie van een verzameling naar zichzelf. Inderdaad: de symmetrieën van een vierkant, oftewel de elementen van D_4, zijn functies van het vierkant naar zichzelf. Zo ook zijn elementen van $\mathbb{R}^*$ functies van $\mathbb{R}^*$ naar zichzelf: de functie vermenigvuldigt elk getal met het gekozen element.

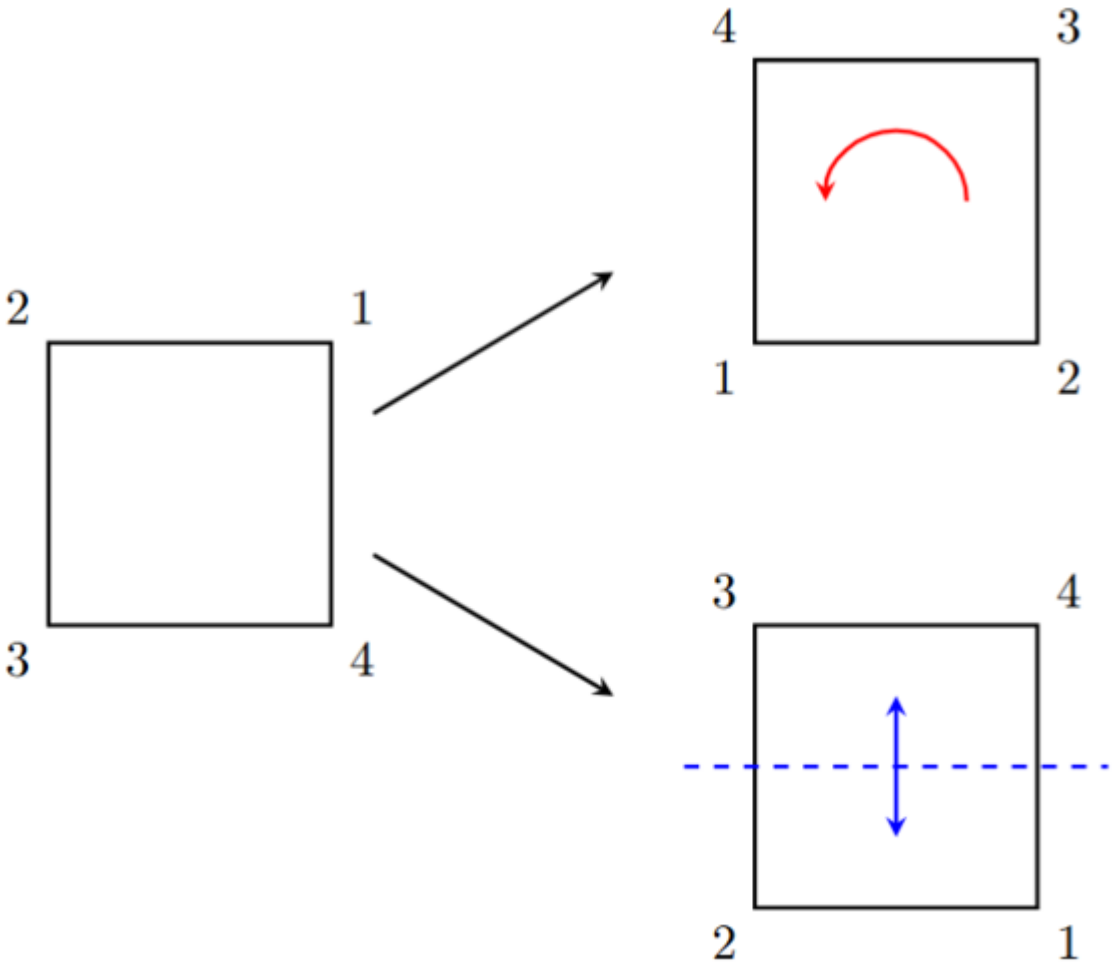
Dit geeft een manier om groepen te construeren: neem een verzameling en bekijk functies van die verzameling naar zichzelf. Niet alle functies kunnen echter elementen van die nieuwe groep zijn. Een groep moet bijvoorbeeld inverses bevatten, dus de functies in de groep moeten inverteerbaar zijn. Alle *inverteerbare* functies van een verzameling A naar zichzelf vormen wel een groep, die wordt genoteerd als $\mbox{Aut}(A)$ (hier staat $\mbox{Aut}$ voor '*automorfisme*': een inverteerbare functie van een wiskundig object naar zichzelf). Aangezien samenstelling van functies associatief is (probeer jezelf daarvan te overtuigen), de identiteitsfunctie inverteerbaar is, en de samenstelling van een inverteerbare functie met zijn inverse de identiteit geeft, vormt $\mbox{Aut}(A)$ inderdaad een groep.

Vervolgens kunnen andere groepen worden gerealiseerd door zekere extra eisen te stellen aan de functies in de groep. Laat ik dit toelichten met het voorbeeld waarbij $A=\{1,2,3,4\}$. De inverteerbare functies $f\colon A\rightarrow A$ zijn precies alle functies die de getallen 1 t/m 4 husselen of, zoals wiskundigen dat noemen, *permuteren*. De volgorde van de getallen geef ik aan door ze tussen ronde haakjes te zetten, dus met (1234) bedoel ik de getallen 1 t/m 4 in de volgorde 1-2-3-4. Een permutatie is dan bijvoorbeeld de functie $f\colon A\rightarrow A$ gedefinieerd door $(1234)\mapsto (2143)$. Deze stuurt 1 naar 2, 2 naar 1, 3 naar 4 en 4 naar 3. De groep van alle permutaties van de getallen 1 t/m 4 noteren wiskundigen als S_4.

We kunnen nu bijvoorbeeld van de functies eisen dat de getallen altijd in dezelfde óf omgekeerde volgorde moeten blijven staan, maar niet in andere willekeurige volgordes,

zodat bijvoorbeeld \((1234) \mapsto (3412) \) en \((1234) \mapsto (4321) \) wel zijn toegestaan (dit zijn een verschuiving van het rijtje 1-2-3-4 naar het rijtje 3-4-1-2, en de omkering van hetzelfde rijtje naar 4-3-2-1), maar bijvoorbeeld \((1234) \mapsto (1342) \) niet. De functies die aan deze eisen voldoen vormen ook een groep – om precies te zijn vormen ze een groep die isomorf is met de groep van symmetrieën van het vierkant, \(D_4 \). Dit is in te zien door de hoeken van het vierkant te nummeren van 1 tot en met 4 zoals in afbeelding 1, en je te realiseren dat een rotatie precies een verschuiving van de nummering is, en een spiegeling de volgorde juist omdraait. Van \(D_4 \) is een ondergroep weer de groep van rotaties, zoals ik eerder al had laten zien. Zo krijgen we als het ware de keten van inclusies

\(S_4 \supset D_4 \supset \mathbb{Z}_4 \).



Afbeelding 5. Permutaties. De permutatie die (1234) naar (3412) stuurt, kan worden gezien als een rotatie met 180 graden van een vierkant, zoals aangegeven met de rode pijl. De permutatie die (1234) naar (4321) stuurt, kan worden gezien

als een spiegeling van een vierkant door de horizontale as, zoals aangegeven met de blauwe pijl.

Liegroepen

Hetzelfde principe als in de vorige paragraaf werkt ook voor vectorruimtes. Een vectorruimte is zelf een verzameling, en dus vormt de verzameling van inverteerbare functies van de vectorruimte naar zichzelf een groep. We kunnen van deze functies vervolgens eisen dat het lineaire afbeeldingen zijn, zoals die in het vorige artikel in deze serie zijn gedefinieerd. Ook deze vormen met elkaar een groep: een groep van matrices. In het vorige artikel had ik die groep voor de vectorruimte $V=\mathbb{R}^n$ al genoteerd als $GL(n)$. Ik beschreef ook ondergroepen van deze groep, zoals $O(n)$ en $SO(n)$; deze laatste is precies dezelfde $SO(n)$ waarmee ik eerder in dit artikel de groep van rotaties van een n-dimensionale bol aanduidde. Deze groep heeft dus een natuurlijke representatie in termen van matrices. (Dat ik hier de woordkeuze ‘representatie’ gebruik is geen toeval, zoals ik zal uitleggen in het volgende artikel in deze serie!)

Deze matrixgroepen zijn voorbeelden van *Liegroepen*, een klasse van groepen die een heel belangrijke rol speelt in de natuur- en wiskunde. Hoewel ik er verder niet op in zal gaan, is een Liegroep een groep die tegelijkertijd ook een “gladde variëteit” is. Wat dit precies betekent is niet belangrijk voor het vervolg van deze serie, maar grofweg kunnen we zeggen dat een Liegroep een continue groep is, meestal weergegeven als een groep van matrices. Bepaalde eigenschappen van Liegroepen zullen in het vervolg op de achtergrond een belangrijke rol spelen.

Om dit artikel af te sluiten, zal ik een tipje van de sluier oplichten over hoe groepen een rol spelen in de natuurkunde, en in het bijzonder in de quantummechanica. We hebben gezien dat een symmetriegroep de mogelijke operaties bevat die kunnen worden uitgevoerd op een object zonder dat dat object verandert. Vervolgens is de vraag hoe zo’n operatie dan precies werkt op een quantumtoestand, zoals een golffunctie van een elektron. Zo’n golffunctie blijkt een vector te zijn in een (mogelijk oneindig-dimensionale) vectorruimte. Natuurkundigen zijn dus geïnteresseerd in werkingen van groepen op vectorruimtes. In het volgende artikel leg ik uit dat representatietheorie de studie is van groepswerkingen op vectorruimtes, wat verklaart waarom die theorie zo’n belangrijke rol speelt in de natuurkunde.

Antwoorden van opgaves:

1. Voor $g\in G$ geldt dat $e_H=f(e_G)=f(gg^{-1})=f(g)f(g^{-1})$ en $e_H=f(e_G)=f(g^{-1}g)=f(g^{-1})f(g)$. Hieruit kun je concluderen dat $f(g^{-1})=f(g)^{-1}$.
2. We hebben gezien dat $\psi(e_{G_1}) = e_{G_2}$ is, dus $\psi(G_1)$ bevat de identiteit. Ook geldt, met behulp van de vorige opgave, dat $\psi(g^{-1})=\psi(g)^{-1}$, dus $\psi(G_1)$ bevat inverses. Ten slotte geldt, voor $\psi(g),\psi(h)\in \psi(G_1)$ dat $\psi(g)\psi(h)=\psi(gh)\in \psi(G_1)$, omdat ψ een groepshomomorfisme is; als we de operatie toepassen op twee elementen van het beeld van ψ blijven we dus in het beeld van ψ. Daarmee is $\psi(G_1)$ dus inderdaad een ondergroep van G_2.

---

[1] Dit leidt nog wel eens tot verwarring: waarom is draaien over 360 graden “niets doen”, terwijl alle andere symmetrieën óók de eigenschap hebben dat ze “niets doen” met het vierkant? De clou zit in die laatste twee woorden: draaien over 90 graden doet niets met een vierkant (en is dus een symmetrie *van het vierkant*), maar doet wel iets met allerlei andere vormen. Draaien over 360 graden is *altijd* “niets doen”, voor elke vorm die je kunt bedenken.

[2] Hoewel we de operatie voor een groep in het algemeen als $\cdot$ schrijven, zien we aan dit voorbeeld dat het dus niet altijd om vermenigvuldiging hoeft te gaan! Om het nog iets verwarrender maken gebruiken wiskundigen voor de algemene operatie die bij een groep hoort vaak tóch de term “vermenigvuldiging”, maar in dit artikel zal ik steeds “operatie” zeggen.

[3] Misschien komt deze notatie onverwachts, omdat je bekend bent met de notatie $x^{-1}=1/x$. Voor groepen krijgt het inverse-symbool een meer algemene betekenis, waardoor a^{-1} in dit geval, voor de gehele getallen, dus niet $1/a$ betekent, maar

juist \(-a \).

[4] Iets preciezer: de elementen in een discrete groep kun je altijd “op een rijtje zeten”, of in wiskundige termen: ze zijn *aftelbaar* – zelfs als het er oneindig veel zijn. Continue groepen zijn juist niet aftelbaar.