

Groepen in de derde graad

Michel Roelens
Els Vanlommel

INHOUD

1 Inleiding 14
2 Symmetriegroepen van vlakke figuren 16
2.1 Herhaling transformaties van het vlak en isometrieën 16
2.2 Symmetrieën van een vlakke figuur 18
3 Groepen bij modulorekenen 25
3.1 Repeterende decimale vormen . 25
3.2 Modulorekenen 26
3.3 Groepen van restklassen 28
3.4 Opnieuw de repeterende decimale vormen. 35
4 Abstracte groepen 36
5 Symmetriegroepen van ruimtefiguren 41
5.1 De symmetriegroep van een regelmatig viervlak 42
5.2 Algemener 46
5.3 De symmetriegroep van een kubus en van een dodecaëder . . . 47
5.4 Algemener 49
5.5 Nog algemener: de stelling van Lagrange in een abstracte groep 50

1 Inleiding

Het belang van groepen

Groepen staan in verband met meetkundige transformaties, getallen, matrices, veeltermen... Een *groep* is een voorbeeld van een *algebraïsche structuur*. Een algebraïsche structuur is een verzameling voorzien van één of meer bewerkingen die aan bepaalde eigenschappen moeten voldoen. Andere voorbeelden van algebraïsche structuren zijn een ring, een vectorruimte, een algebra...

Als je iets berekent of bewijst in een abstracte algebraïsche structuur (bv. in een groep), dan geldt dit meteen in alle voorbeelden van deze structuur. Dit is de sterkte van de *abstracte algebra*. Op die manier ontstaan verbanden tussen meetkundige transformaties, getallen, matrices, veeltermen...

Als je één voorbeeld van een algebraïsche structuur moet bestuderen, is groepen volgens ons een goede keuze. Het is een eenvoudige structuur: er is maar één bewerking en de lijst van eigenschappen die in de definitie staan, is niet te lang. Bovendien is deze structuur heel belangrijk door de link met symmetrie, in de meetkunde en elders binnen en buiten de wiskunde.

Symmetrie gaat in essentie over *invarianten*: over iets dat behouden blijft wanneer iets verandert. Je past bv. een meetkundige transformatie toe en hierbij blijft een meetkundige figuur invariant. Alle transformaties die de figuur invariant laten,

horen samen en vormen een groep. Symmetrische figuren komen voor in de meetkunde maar ook in de natuur, in de chemie en in de kunst. Met groepen bestudeer je symmetrie.

Veel puzzels, zoals de Rubikskubus of het ontwarren van knopen, steunen op invarianten (wat blijft er hetzelfde als je aan de kubus draait, of als je aan een uiteinde van de knoop trekt?).

Het begrip groep is ingevoerd door Evariste Galois in de 19de eeuw, niet in meetkunde maar bij de studie van vergelijkingen en hun exacte oplosbaarheid. De galoistheorie is sindsdien een belangrijk vak in een universitaire wiskundeopleiding. Ook in andere vakken in de hogere zuivere wiskunde vormt het begrip groep een sleutelbegrip, bv. homotopiegroepen in de algebraïsche topologie (sta ons toe om dit hier niet uit te leggen). Hetzelfde geldt in de toegepaste wiskunde (bv. cryptografie) en in de natuurwetenschappen: kristallografie, kwantummechanica, stringtheorie ... Overal komen groepen voor, gelinkt aan invarianten en vormen van (niet noodzakelijk meetkundige) symmetrie.

Een korte, goed leesbare tekst over het belang van groepen binnen en buiten de wiskunde, vind je online (Conrad, 2005).

Modernisering: zijn de groepen terug?

Groepen duiken op in de nieuwe specifieke eindtermen voor de derde graad in studierichtingen met 'gevorderde wiskunde' (economie-wiskunde, Grieks-wiskunde, Latijn-wiskunde, wetenschappen-wiskunde en 'technologische wetenschappen en engineering'). Op dit moment is alles wat we over nieuwe eindtermen schrijven onder voorbehoud. Na de vernietiging door het grondwettelijk hof kunnen er eindtermen sneuvelen of wijzigen. Laten we ervan uitgaan dat de groepen overeind zullen blijven.

Het volgende staat in de nieuwe eindterm over groepen:

> *De leerlingen onderzoeken verzamelingen voorzien van een bewerking via groepentheorie.*
>
> - *groep, commutatieve groep*
> - *uniciteit van het neutrale element en van de inverse van een element*
> - *mogelijke voorbeelden van groepsstructuren: gehele getallen modulo n, symmetriegroep van een meetkundige figuur, getallenverzameling*
> - *cayleytabel van een eindige groep*
> - *bepalen of een verzameling voorzien van een bewerking een groep vormt*
> - *rekenen in groepen*

Groepen en andere algebraïsche structuren speelden een grote rol in de leerplannen ten tijde van de Moderne Wiskunde (zeg maar jaren 1970). Kunnen we zeggen dat de groepen terug zijn van weggeweest? Eigenlijk niet. Toen speelden groepen, ringen, velden en vectorruimten een hoofdrol in de leerstof vanaf de eerste jaren van het secundair, volgens ons veel te vroeg. Nu komen groepen op het einde van het secundair aan bod, enkel voor de leerlingen die het pakket 'gevorderde wiskunde' krijgen. Dit is volgens ons een geschikt moment en een goed doelpubliek om op een zinvolle manier de stap te zetten naar een algebraïsche structuur. De leerlingen hebben al kennis gemaakt met meetkundige symmetrie en met andere concrete voorbeelden van groepen zonder dat ze die zo genoemd hebben, zodat ze het gemeenschappelijke patroon kunnen herkennen en leren benoemen.

Tien jaar geleden: loep over symmetrie

Het is exact tien jaar geleden (de tijd gaat snel...) dat Uitwiskeling een loep uitbracht over symmetrie (Roelens en Schatteman, 2012). Het doel was toen de studie van symmetrie van vlakke figuren. Doelpubliek was de eerste en de tweede graad. Groepen kwamen in die loep aan bod, maar zonder de stap naar abstracte groepen. Nu liggen de kaarten omgekeerd: we richten ons op groepen en we gebruiken symmetrie als één van de opstappen naar het (abstracte) begrip groep.

Het stuk van toen over de rozetten en de friezen, waarbij aangetoond wordt dat er juist 7 symmetriegroepen van strookpatronen bestaan, blijft zeer interessant. Een tip: dit kan als opdracht binnen het nieuwe stuk groepen in de derde graad ingelast worden.

Wat je in deze loep mag verwachten

In paragraaf 2 brengen we symmetriegroepen van vlakke figuren en hun cayleytabellen aan. Vanuit die cayleytabellen hebben we het ook over deelgroepen en over eigenschappen die gelden in zo'n symmetriegroep.

In paragraaf 3 ontmoet je groepen in een totaal andere context: het modulorekenen (bv. het rekenen op een klok). Voor de optelling heb je altijd een groep, maar voor de vermenigvuldiging ligt het ingewikkelder: je krijgt pas een groep nadat je elementen hebt geschrapt.

Soms hebben cayleytabellen van verschillende groepen een zelfde patroon. Vanuit een abstract standpunt kunnen verschillende groepen eigenlijk hetzelfde zijn (isomorf). Dit motiveert het werken in een abstracte groep in paragraaf 4, waarbij we in het midden laten wat de elementen zijn en wat de bewerking betekent. We maken enkele kleine bewijsoefeningen en we bekijken voorbeelden en tegenvoorbeelden.

We keren in paragraaf 5 terug naar symmetrie, maar dan in de ruimte. We zoeken uit hoe symmetrisch bepaalde ruimtefiguren zijn, door te tellen hoeveel draaiingen, vlakspiegelingen, enz. deze figuren invariant laten. Een slimme manier om die te tellen, steunt op een stelling die we kunnen veralgemenen tot abstracte groepen: de stelling van Lagrange.

We proberen in deze loep de groepen op een zinvolle manier aan te brengen, vanuit hun rol bij de studie van meetkundige symmetrie en modulorekenen. Hierdoor, en dat beseffen we, gaan we een stuk verder dan wat door de nieuwe eindterm gevraagd wordt. Het is dus niet nodig om alles uit deze loep in alle klassen (met gevorderde wiskunde) te geven. Paragraaf 5 zou je bv. kunnen voorbehouden voor differentiatie of voor klassen met nog extra uren wiskunde.

2 Symmetriegroepen van vlakke figuren

2.1 Herhaling transformaties van het vlak en isometrieën

We houden het hier kort. Voor een uitgebreidere uitleg over transformaties verwijzen we onder andere naar de loep van Uitwiskeling 28/4. Daar lees je bv. wat de verschillen zijn tussen de wiskundige verschuiving, draaiing ... enerzijds en die van het dagelijkse leven anderzijds.

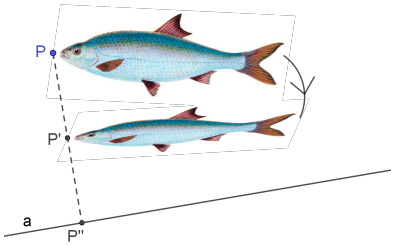
Eén van die verschillen willen we hier toch nog vermelden: bij een wiskundige transformatie blijft de figuur waar ze is en krijgt ze een beeld (een soort kloon). Dit zie je goed als je in GeoGebra een transformatie uitvoert. Als je in het dagelijks leven een figuur verschuift of draait, krijg je er geen tweede bij... Als het zo was, zou er nogal met geldbriefjes geschoven worden...

De leerlingen kennen verschuivingen, draaiingen en (lijn)spiegelingen van de eerste graad en homothetieën van de tweede graad. Wat hiervan meestal is bijgebleven, is hoe je het beeld van een figuur tekent. Transformaties die echt vervormen, hebben ze wellicht niet ontmoet.

Wiskundig gaat het over *transformaties van het vlak*. Dit betekent: elk punt van het vlak krijgt juist één beeld. Het beeld van een figuur is de meetkundige plaats (verzameling) van de beelden van de punten van de figuur. Om een transformatie wiskundig te definiëren, moet je vastleggen wat het beeld is van een willekeurig punt van het vlak. Je kunt dit vergelijken met het functievoorschrift van een reële functie: die definieer je ook door het beeld van een willekeurig getal x vast te leggen.

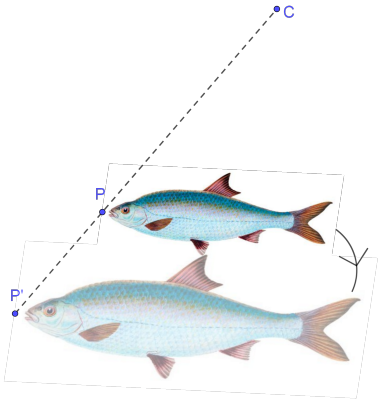
In de figuren hieronder zie je dat een figuur (een vis, te bekijken als een vlakke figuur, geen 3D-vis) onderworpen wordt aan verschillende transformaties. We geven ook telkens de definitie en het voorschrift voor het beeld van een willekeurig punt P van het vlak.

1. een samendrukking met factor $\frac{1}{2}$ naar een rechte a
   $d_{a,\frac{1}{2}} : P \mapsto P'$ zo dat $\overrightarrow{P''P'} = \frac{1}{2}\overrightarrow{P''P}$ (met P'' de loodrechte projectie van P op a)



Figuur 1 *– Samendrukking*

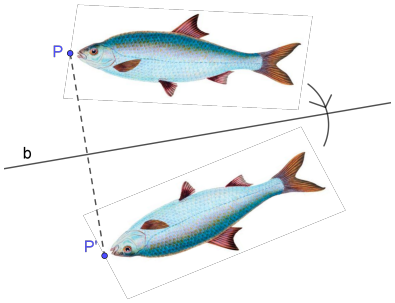
2. een vergroting (homothetie) met factor $\frac{3}{2}$ vanuit een punt C
   $h_{C,\frac{3}{2}} : P \mapsto P'$ zo dat $\overrightarrow{CP'} = \frac{3}{2}\overrightarrow{CP}$



***Figuur 2** – Homothetie*

3. een (lijn)spiegeling om een rechte b
   $s_b : P \mapsto P'$ zo dat

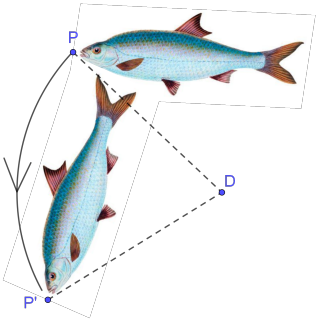
$$\begin{cases} b = \text{middelloodlijn}[PP'] & (\text{voor } P \notin b) \\ P' = P & (\text{voor } P \in b) \end{cases}$$



***Figuur 3** – Lijnspiegeling*

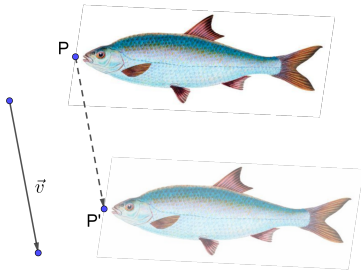
4. een draaiing (rotatie) rond een punt D over 75° in tegenwijzerzin
   $r_{D,+75°} : P \mapsto P'$ zo dat

$$\begin{cases} |DP'| = |DP| \text{ en } \angle PDP' = +75° & (\text{voor } P \neq D) \\ P' = D & (\text{voor } P = D) \end{cases}$$



***Figuur 4** – Draaiing*

5. een verschuiving (translatie) over een vector $\overrightarrow{v}$
   $t_{\overrightarrow{v}} : P \mapsto P'$ zo dat $\overrightarrow{PP'} = \overrightarrow{v}$



***Figuur 5** – Verschuiving*

De eerste transformatie verandert de vorm; de vis wordt dunner. De tweede behoudt de vorm maar niet de afmetingen; de vis wordt groter. De derde, vierde en vijfde transformaties behouden de afmetingen. Het zijn isometrieën.

Definitie • Isometrie

Een transformatie t is een *isometrie* als die de afstand bewaart, anders gezegd als $\forall P, Q$: $d(t(P), t(Q)) = d(P, Q)$.

Automatisch behoudt een isometrie ook de hoekgrootte; dat hoeft niet in de definitie te worden opgenomen. Immers, beschouw een hoek $B\hat{A}C$ en de beelden A', B', C' van A, B, C door een isometrie. Omdat de driehoeken ABC en $A'B'C'$ congruent zijn (zzz), geldt $B'\hat{A}'C' = B\hat{A}C$.

Bij de derde transformatie, de spiegeling, wordt de figuur 'omgekeerd'. Als de vis in karton uitgesneden is, dan wordt de kartonnen figuur buiten het vlak gedraaid om de spiegelas en terug in het vlak gelegd. Het spiegelbeeld toont de andere kant van de vis. Een lijnspiegeling keert de 'oriëntatie' om: wijzerzin wordt tegenwijzerzin en omgekeerd.

De vierde en de vijfde transformatie, de draaiing en de verschuiving, zijn verplaatsingen in het vlak. De kartonnen vis wordt niet omgedraaid; dezelfde kant blijft bovenaan. De oriëntatie blijft behouden. Een puntspiegeling hebben we hierboven niet apart opgenomen omdat we die als een draaiing over 180° kunnen bekijken. De identieke transformatie is nog een belangrijk speciaal geval. Ze beeldt elk punt op zichzelf af: $I : P \mapsto P$. De identieke toepassen betekent eigenlijk 'niets doen'. De identieke is een speciaal geval van een verschuiving, namelijk over de nulvector. De identieke is

ook een draaiing, namelijk over 0° (en rond om het even welk draaipunt). Dus: $I = t_{\overrightarrow{0}} = r_{D,0°}$

Transformaties kun je met elkaar *samenstellen*, na elkaar toepassen. De samengestelde van twee transformaties s en t, eerst s en dan t, noteren we als $t \circ s$ (lees: t na s). Deze op het eerste gezicht vreemde volgorde in de notatie zorgt ervoor dat we de volgorde kunnen behouden als we het beeld van een punt opschrijven:

$$(t \circ s)(P) = t(s(P)).$$

De *inverse* t^{-1} van een transformatie t is de transformatie die het beeld terugstuurt naar het origineel:

$$t^{-1}(Q) = P \Leftrightarrow t(P) = Q.$$

Deze inverse is enkel een goed gedefinieerde transformatie wanneer elk punt Q het t-beeld is van juist één punt P. De inverse van een transformatie t is ook de transformatie die t ongedaan maakt: als je eerst t toepast en dan t^{-1}, of andersom, dan is elk punt weer op zichzelf gestuurd. Anders gezegd: $t^{-1} \circ t = I = t \circ t^{-1}$.

In de loep van Uitwiskeling 28/4 worden samengestelde transformaties met GeoGebra onderzocht en worden resultaten bewezen over de samengestelde van twee spiegelingen, over de samengestelde van twee puntspiegelingen ... We zullen dit hier niet systematisch herhalen maar we bekijken dit wanneer we het nodig hebben voor symmetrie.

2.2 Symmetrieën van een vlakke figuur

Soms is een figuur 'immuun' voor een bepaalde transformatie. Spiegel je bv. een hartje (♡) om zijn symmetrieas, dan verandert het hartje niet (ook niet zijn plaats in het vlak). De figuur wordt 'op zichzelf afgebeeld'. Dit betekent niet dat elk punt van de figuur op zichzelf afgebeeld wordt, maar wel dat de figuur als geheel samenvalt met zijn beeld. We zeggen ook dat de figuur invariant blijft voor die transformaties.

In de eerste graad hebben leerlingen symmetrie leren herkennen bij figuren. Lijnsymmetrische figuren worden door een (lijn)spiegeling op zichzelf afgebeeld, puntsymmetrische door een puntspiegeling, draaisymmetrische door een niet-identieke draaiing ...

Definitie • Een symmetrie van een figuur

Een *symmetrie* van een figuur F is een isometrie die F op zichzelf afbeeldt.

De identieke is volgens deze definitie een symmetrie van elke denkbare figuur. We spreken pas van een symmetrische figuur als die bovendien nog één of meer niet-triviale symmetrieën heeft.

Vraag even aan de leerlingen of ze een figuur kunnen tekenen die op zichzelf wordt afgebeeld door twee spiegelingen met snijdende assen a en b, maar niet draaisymmetrisch is. Laat hen niet te lang zoeken, want het is niet mogelijk. Hoe komt dat? Als de spiegelingen s_a en s_b symmetrieën zijn van de (gezochte) figuur F, dan blijft de figuur ook invariant wanneer je die twee spiegelingen na elkaar uitvoert. De samengestelde $s_b \circ s_a$ is dus ook een symmetrie van F, en dat is, wanneer a en b elkaar snijden, een draaiing.

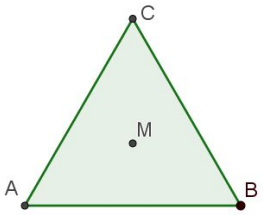
Als je symmetrieën van een figuur met elkaar samenstelt, blijf je 'binnen het groepje' van de symmetrieën van die figuur. We zeggen ook: de verzameling van de symmetrieën van F is *gesloten* voor het samenstellen. Door samen te stellen kun je dit groepje niet verlaten.

Dit is al één van de voorwaarden in de definitie van een *groep*. De andere voorwaarden zijn de associativiteit van de bewerking, het bestaan van een neutraal element en het bestaan van een inverse voor elk element. De symmetrieën van een figuur zullen altijd een groep vormen. Zie verderop.

LESACTIVITEIT

Symmetrieën van een gelijkzijdige driehoek

Gegeven: een gelijkzijdige driehoek ABC.



1 De gelijkzijdige driehoek is draaisymmetrisch. Welke draaiingen zijn symmetrieën van deze driehoek?

✓ *De draaiing rond het middelpunt M over $+120°$ ($120°$ in tegenwijzerzin dus). Een draaiing rond M over $-120°$ ($120°$ in wijzerzin, of nog: over $+240°$). En niet te vergeten: de identieke of de draaiing over $0°$. Er zijn er dus 3.*

2 Deze driehoek is ook lijnsymmetrisch. Welke spiegelingen zijn symmetrieën van deze driehoek?

✓ *Er zijn er drie, met als assen de zwaartelijnen (of hoogtelijnen of ...; bij een gelijkzijdige driehoek vallen die samen).*

Een symmetrie van de driehoek bepaalt automatisch een permutatie van de drie hoekpunten A, B, C. Zo kunnen we de draaiing rond M over $+120°$ noteren als de permutatie die A afbeeldt op B, B op C en C op A. Deze permutatie wordt ook met een matrix-achtig schema met twee rijen genoteerd; de originelen in de bovenste rij en hun beelden eronder:

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

Merk op: de namen van de punten draaien niet mee! Het beeld van punt A is het punt B (of $A' = B$) maar het punt A zelf blijft staan. Bij een wiskundige transformatie blijven de punten van het vlak staan waar ze stonden en krijgen ze een beeld. Dat is een belangrijk verschil met het draaien in het dagelijkse leven.

3 Is het mogelijk dat er nog meer symmetrieën zijn dan de draaiingen en de spiegelingen die je gevonden hebt?

✓ *Neen, we hebben ze allemaal. Elke symmetrie van de driehoek is volledig bepaald door de beelden van de drie hoekpunten, dus door een permutatie van A, B en C. Er zijn maar $3! = 6$ permutaties van drie elementen.*

Laten we de draaiing rond M over $+120°$ kortweg r noemen. De spiegeling om de zwaartelijn (hoogtelijn ...) uit C noteren we kortweg s.

4 Welke symmetrie van de driehoek is dan $s \circ r$?

✓ *Dit is de spiegeling om de zwaartelijn uit A. Leerlingen kunnen dit vinden door te tekenen. Als leraar kun je hen tonen dat dit ook gaat met de permutaties van de hoekpunten. In het schema*

hieronder staan de hoekpunten in de eerste rij. Van rij 1 naar rij 2 pas je r toe en van rij 2 naar rij 3 pas je s toe.

$$\begin{pmatrix} A & B & C \\ B & C & A \\ A & C & B \end{pmatrix}$$

Door de middelste rij (de tussenstap) weg te laten, zie je dat A op zichzelf wordt afgebeeld en B en C verwisseld worden.

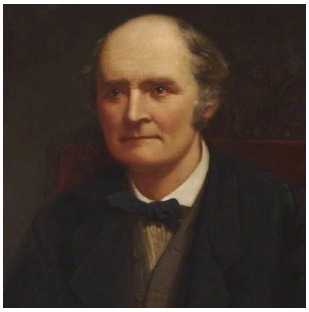
5 Welke symmetrie van de driehoek is $r \circ s$?

✓ *Dit is de spiegeling om de zwaartelijn uit B. Hier blijkt dat de volgorde belang heeft; de samenstelling is niet commutatief.*

6 Schrijf alle zes symmetrieën van de driehoek aan de hand van r en s.

✓ *De identieke is $s \circ s$. De draaiing rond M over $+120°$ is r. De draaiing rond M over $-120°$ is $r \circ r$. Uit de vorige opgaven weten we dat de drie spiegelingen te schrijven zijn als s, $s \circ r$ en $r \circ s$.*

Arthur Cayley (19de eeuw) was tegelijkertijd wiskundige en advocaat. Hij ijverde voor het toelaten van vrouwen in het hoger onderwijs, wat men in die tijd niet evident vond. De vermenigvuldiging van matrices is door hem bedacht, alsook de definitie van een abstracte groep (zie verderop in paragraaf 4). Naar hem zijn de cayleytabellen genoemd, een soort vermenigvuldigingstafels voor bewerkingen in (eindige) verzamelingen.



7 Vul de volgende 'cayleytabel' in voor de symmetrieën van de gelijkzijdige driehoek. In elk vakje komt de transformatie die je krijgt als je de transformatie van die rij uitvoert *na* ($\circ$) de transformatie van die kolom. In een dergelijke tabel is het de gewoonte om de symmetrieën kort te noteren. Behalve de identieke, die je kort met I noteert, noteer je alle symmetrieën in functie van r en s. Het samenstellingsteken $\circ$ mag je weglaten, dus $r \circ s = rs$, en $r \circ r = r^2$.

$\circ$	I	r	r^2	s	sr	rs
I						
r						
r^2						
s						
sr						
rs						

✓ *Hieronder is de ingevulde versie. Leerlingen kunnen meetkundig met de driehoek werken, of met de permutaties van de hoekpunten. Ze kunnen ook rekenen met r en s. Bv. $s \circ sr$ geeft r omdat $s^2 = I$. Of als je $r^2 \circ s$ al hebt gevonden, is $r \circ rs$ hetzelfde; associativiteit is bij het na elkaar toepassen van transformatie een evidentie. Na een tijd merken leerlingen ook dat elke symmetrie juist één keer voorkomt in elke rij en in elke kolom. Spontaan zullen ze dit gebruiken om de cayleytabel af te werken. Hier wordt in één van de volgende vragen op teruggekomen.*

$\circ$	I	r	r^2	s	sr	rs
I	I	r	r^2	s	sr	rs
r	r	r^2	I	rs	s	sr
r^2	r^2	I	r	sr	rs	s
s	s	sr	rs	I	r	r^2
sr	sr	rs	s	r^2	I	r
rs	rs	s	sr	r	r^2	I

8 Wat valt er op in de cayleytabel?

✔ *De vraag is bewust vaag geformuleerd. Sommige zaken die opvallen, komen later nog terug. Vermoedelijke antwoorden van de leerlingen:*

- *De rij en de kolom bij I zijn dezelfde als de donker gekleurde rij of kolom van de gegeven symmetrieën. Dit is natuurlijk niet verwonderlijk: de identieke I is niets doen, dus doet I ook niets als je die met een andere transformatie samenstelt. Wiskundig gezegd: I is neutraal.*
- *Elk element komt juist één keer voor in elke rij en in elke kolom. Men zegt dat de cayleytabel een 'Latijns vierkant' is. Sudoku's zijn speciale gevallen van Latijnse vierkanten met extra voorwaarden.*
- *Opvallend zijn de vier 'blokken' van drie bij drie in de cayleytabel. Je hebt een blok links boven van het samenstellen van de drie draaiingen onder elkaar. Het resultaat is weer een draaiing. Rechts onder heb je het blok van het samenstellen van twee spiegelingen. Je krijgt draaiingen. En dan heb je nog de twee blokken waarbij spiegelingen en draaiingen met elkaar worden samengesteld. De resultaten zijn spiegelingen. Dit is meetkundig allemaal goed te begrijpen.*

9 Waar of niet waar binnen de verzameling van deze zes symmetrieën? Leg uit op basis van de cayleytabel.

1. Deze verzameling is gesloten voor het samenstellen.
2. Het samenstellen is commutatief.
3. Het samenstellen is associatief.
4. Er is een neutraal element voor het samenstellen.
5. Voor elk element X bestaat er een element Y zo dat $Y \circ X = I = X \circ Y$. Wat zijn X en Y ten opzichte van elkaar?
6. Er zijn juist vier elementen X waarvoor geldt $X \circ X = I$.
7. Er zijn juist vier elementen X waarvoor geldt $X \circ X \circ X = I$.

✔

1. *Waar. We hebben dit vooraf al opgemerkt (met het voorbeeld van een figuur met twee snijdende symmetrieassen). In de cayleytabel: er verschijnen geen 'nieuwe' elementen in de tabel, enkel de zes symmetrieën.*
2. *Niet waar. We zien bv. dat $s \circ sr = r$ maar $sr \circ s = r^2$. Als het samenstellen commutatief was, zou de cayleytabel symmetrisch zijn ten opzichte van de diagonaal van links boven naar rechts onder.*
3. *Wel waar. Het is veel werk om dit volledig na te gaan op de cayleytabel. Je kunt een paar voorbeelden nemen. Meetkundig is het evident dat de associativiteit geldt. Drie keer na elkaar*

iets doen, daar maken haakjes geen verschil bij. Het samenstellen is van nature uit altijd associatief.

4. *Dit is waar: de identieke I is het neutraal element. In de cayleytabel zie je in de eerste rij en in de eerste kolom, dat samenstellen met I niets verandert.*
5. *Dit is waar. X en Y zijn elkaars inverse transformatie. In de cayleytabel: in elke kolom en in elke rij komt I voor. Bovendien liggen de I's symmetrisch ten opzichte van de diagonaal van linksboven naar rechtsonder. Dit betekent dat als $Y \circ X = I$, ook $X \circ Y = I$. (X en Y kunnen hierbij ook gelijk zijn, zoals bij de spiegelingen en bij I zelf.)*
6. *Dit is waar: I en de drie spiegelingen voldoen. De twee niet triviale draaiingen niet.*
7. *Niet waar. Dit geldt voor de drie draaiingen, maar voor geen enkele spiegeling.*

De vier eigenschappen 1, 3, 4 en 5 (zie vorige vraag) zorgen ervoor dat de symmetrieën van de gelijkzijdige driehoek een 'groep' vormen.

Definitie • Een groep van transformaties

Een verzameling G van transformaties is een *groep* van transformaties als de volgende voorwaarden vervuld zijn:

- G is gesloten voor het samenstellen.
- Het samenstellen is associatief in G.
- De identieke I, die neutraal is voor het samenstellen, zit in G.
- Voor elk element t van G zit de inverse transformatie t^{-1} ook in G.

De associativiteit geldt altijd voor het samenstellen. Om te onderzoeken of je een groep van transformaties hebt, hoef je die niet te controleren. Dat zal wel nodig zijn wanneer we het begrip groep zullen uitbreiden tot andere verzamelingen en andere bewerkingen dan het samenstellen.

10 Hieronder wordt bewezen dat de symmetrieën van een willekeurige figuur een groep vormen. Leg bij elke gelijkheid uit waarop gesteund wordt.

Stelling • Symmetriegroep van een figuur

Alle symmetrieën van een figuur F vormen een groep.

Bewijs •

- Eerst moeten we bewijzen dat de verzameling van alle symmetrieën van F gesloten is voor het samenstellen. Beschouw twee symmetrieën s en t van figuur F. We bewijzen dat $t \circ s$ dan ook een symmetrie is van F:

$$\begin{aligned}(t \circ s)(F) &= t(s(F)) \\ &= t(F) \\ &= F\end{aligned}$$

- De samenstelling is altijd associatief.

- De identieke is een symmetrie van F, want $I(F) = F$.
- Beschouw een symmetrie t van F. We bewijzen dat de inverse t^{-1} ook een symmetrie is van F:

$$\begin{aligned} t^{-1}(F) &= t^{-1}(t(F)) \\ &= (t^{-1} \circ t)(F) \\ &= I(F) \\ &= F \end{aligned}$$

✔ *Gesloten: de eerste gelijkheid steunt op de definitie van het samenstellen. De tweede geldt omdat s een symmetrie is van F en de derde omdat t een symmetrie is van F.*

Inverse: de eerste gelijkheid geldt omdat t een symmetrie is van F. De tweede gelijkheid steunt op de definitie van het samenstellen. De derde op een eigenschap van de inverse transformatie en de vierde op de betekenis van de identieke ('niets doen' doet niets).

Een notatie voor de symmetriegroep van figuur F is $\text{Sym}(F), \circ$ (maar vaak blijven we het voluit schrijven).

Als een deelverzameling van een groep van transformaties zelf een groep vormt voor de samenstelling, dan spreken we van een *deelgroep* van die groep.

11 Vormen de draaiingen van de gelijkzijdige driehoek een deelgroep?

✔ *Ja. De samengestelde van twee draaiingen is weer een draaiing; je ziet dit ook aan het blok linksboven in de cayleytabel. De identieke is erbij en de inverse van een draaiing is de draaiing over de tegengestelde hoek en die zit er telkens bij.*

12 Vormen de spiegelingen van de gelijkzijdige driehoek een deelgroep?

✔ *Neen. De samengestelde van twee spiegelingen is geen spiegeling. Of een ander argument (maar één reden volstaat): de identieke is geen spiegeling.*

Na de opgave over de symmetrieën van de gelijkzijdige driehoek, maken de leerlingen best de cayleytabel van een andere symmetriegroep. We stellen voor dat ze dit voor de rechthoek doen. Dit is eenvoudiger, waardoor ze het na de vorige opdracht vlot zelf zullen kunnen.



***Figuur 6** – Rechthoek*

De leerlingen zoeken alle symmetrieën en vinden twee draaiingen: I en de draaiing rond het middelpunt over 180°. Ze vinden ook twee spiegelingen, ten opzichte van de rechten die de middens van overstaande zijden verbinden. Als ze de draaiing r noemen en de twee spiegelingen s en s' dan wordt dit de cayleytabel. Eventueel kunnen ze opmerken dat $s' = r \circ s = s \circ r$, zodat ze alle elementen met r en s kunnen noteren. We hebben dat hieronder niet gedaan.

Hier is de cayleytabel van $\text{Sym}(\square), \circ$.

$\circ$	I	r	s	s'
I	I	r	s	s'
r	r	I	s'	s
s	s	s'	I	r
s'	s'	s	r	I

Wat valt er nu op? Hetzelfde als bij de gelijkzijdige driehoek: het neutrale karakter van I, het Latijnse vierkant, en ook hier de vier blokken.

Deze symmetriegroep is wel commutatief: de cayleytabel is perfect symmetrisch ten opzichte van de diagonaal van links boven naar rechts onder.

Nog een belangrijk verschil met Sym(△),∘: niet elke permutatie van de vier hoekpunten komt overeen met een symmetrie van de rechthoek. De hoekpunten mogen niet gelijk hoe afgebeeld worden: bv. twee hoekpunten verbonden door een lange zijde, moeten afgebeeld worden op twee hoekpunten verbonden door een lange zijde. Slechts vier van de $4! = 24$ permutaties van de hoekpunten leveren symmetrieën op.

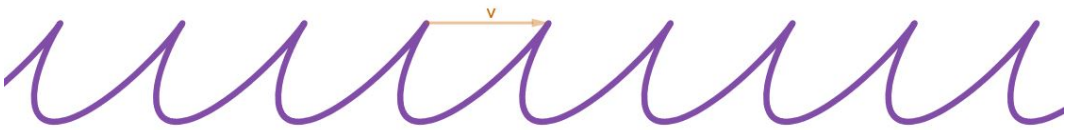
Ook hier vormen de draaiingen een deelgroep.

In de loep van tien jaar geleden (Roelens en Schatteman, 2012) hadden we het uitgebreid over strookpatronen (friezen). Hier willen we maar één voorbeeld aanhalen om te laten zien dat een symmetriegroep ook oneindig kan zijn. Uiteraard is het dan onmogelijk om een volledige cayleytabel te maken.

LESACTIVITEIT

Symmetriegroep van een strookpatroon

Veronderstel dat deze figuur links en rechts onbegrensd verder gaat. Het is een eenvoudig voorbeeld van een strookpatroon of fries.



1 Welke symmetrieën heeft deze fries?

✔ *De verschuivingen over gehele veelvouden van de getekende vector* $\overrightarrow{v}$.

Noem $t = t_{\overrightarrow{v}}$.

2 Wat is de inverse t^{-1}?

✔ $t^{-1} = t_{-\overrightarrow{v}}$.

3 Wat krijg je als je $t_{4\overrightarrow{v}}$ samenstelt met $t_{-7\overrightarrow{v}}$?

✔ $t_{-7\overrightarrow{v}} \circ t_{4\overrightarrow{v}} = t_{-3\overrightarrow{v}}$

4 Wat is t^3?

✔ $t^3 = t_{3\overrightarrow{v}}$

5 Maak een stuk van de (oneindige) cayleytabel. Je mag je beperken tot het stuk waarbij t^{-1}, I, t, t^2 met elkaar samengesteld worden.

∘	…	t^{-1}	I	t	t^2	…
…	…	…	…	…	…	…
t^{-1}	…	t^{-2}	t^{-1}	I	t	…
I	…	t^{-1}	I	t	t^2	…
t	…	I	t	t^2	t^3	…
t^2	…	t	t^2	t^3	t^4	…
…	…	…	…	…	…	…

6 Is $\{t, t^2, t^3, t^4, \ldots\}$ gesloten voor de samenstelling? Is het een deelgroep van de symmetriegroep van de fries?

✔ *Ja, deze verzameling is gesloten maar het is geen deelgroep, bv. omdat de identieke er niet in zit.*

7 Is $\{I, t, t^2, t^3, \ldots\}$ gesloten voor de samenstelling? Is het een deelgroep?

✔ *Ja, deze verzameling is gesloten, de identieke is er wel bij. Maar het is geen deelgroep want de inverse van bv. t is er niet bij.*

8 Geef een eindige deelgroep.

✔ *De enige eindige deelgroep is $\{I\}$.*

9 Geef een oneindige deelgroep die niet de hele symmetriegroep van de fries is.

✔ *Bijvoorbeeld de verschuivingen over de even gehele veelvouden van $\overrightarrow{v}$.*

Opmerking die niet voor de leerlingen bedoeld is.

Hoewel deze loep niet over strookpatronen gaat, wilden we toch één eenvoudig voorbeeld opnemen van een symmetriegroep die oneindig is. Voor eindige groepen van transformaties is niet alleen de associativiteit een overbodige voorwaarde (omdat die altijd geldt) maar is dat ook het geval met het bestaan van een neutraal element en van inversen. Om na te gaan of een eindige verzameling transformaties een groep vormt voor de samenstelling, volstaat het na te gaan dat die verzameling gesloten is voor de samenstelling.

Iets algemener: een eindige (maar niet lege) deelverzameling van een groep vormt een deelgroep als die gesloten is voor de bewerking. In het geval van een eindige verzameling van transformaties gaat het over een deelverzameling van de groep van alle transformaties.

Met deze oneindige groep laten we zien dat je, om na te gaan of een deelverzameling een deelgroep vormt, wel degelijk moet nagaan dat de identieke erin zit en dat de inverse van elk element erin zit. (Enkel inversen is ook al goed want als een element en zijn inverse in de deelverzameling zitten, dan ook de samengestelde en dat is de identieke.)

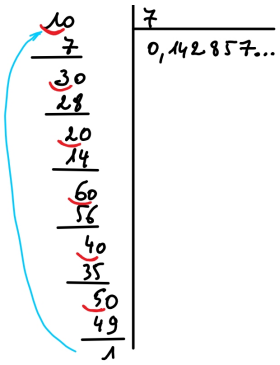
3 Groepen bij modulorekenen

Via de symmetrieën van vlakke figuren komen we op een heel natuurlijke manier bij groepen. Daarom zijn die symmetriegroepen een uitstekende manier om groepentheorie in te leiden. Ook in rekenkundige en algebraïsche contexten duiken groepen op. Daar gaat het in deze paragraaf over. We bekijken hierbij opnieuw voornamelijk eindige groepen omdat we via eindige groepen in eerste instantie gemakkelijker intuïtie kunnen opbouwen voor de theorie. Eens je de patronen kent voor eindige groepen, vormen oneindige groepen een relatief eenvoudige uitbreiding. Al zijn er belangrijke verschillen: na de lesactiviteit van de strookpatronen merkten we bijvoorbeeld op dat het pas bij oneindige deelgroepen nodig is om aan te tonen dat het neutraal en invers element ook tot de groep behoren.

We starten hieronder met een probleem waarbij ook in een rekenkundige context op een natuurlijke manier groepen opduiken, dit keer groepen van gehele getallen.

3.1 Repeterende decimale vormen

In de lagere jaren leerden de leerlingen dat echte breuken altijd kunnen geschreven worden als repeterende decimale vormen. Om het repeterend deel te vinden, kunnen ze een staartdeling uitvoeren. In Figuur 7 zie je die deling voor de breuk $\frac{1}{7} = 0{,}142857142\ldots$



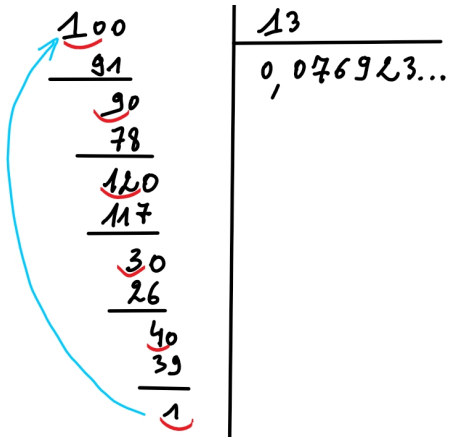
Figuur 7 *– De staartdeling voor $\frac{1}{7}$*

Op dezelfde manier berekenen we $\frac{2}{7}$, $\frac{3}{7}$ … $\frac{6}{7}$:

$$\frac{2}{7} = 0{,}285714285\ldots \qquad \frac{3}{7} = 0{,}428571428\ldots$$
$$\frac{4}{7} = 0{,}571428571\ldots \qquad \frac{5}{7} = 0{,}714285714\ldots$$
$$\frac{6}{7} = 0{,}857142857\ldots$$

We zien dat steeds dezelfde zes decimalen terugkomen, in dezelfde volgorde, maar telkens wel startend op een andere plaats in het rijtje. Dat groepje decimalen hoort blijkbaar op een bepaalde manier samen. Een mooie goocheltruc die steunt op dit principe wordt beschreven in Uitwiskeling 31/4 (2015).

We onderzoeken een tweede voorbeeld, met noemer 13. In Figuur 8 zie je de staartdeling voor de breuk $\frac{1}{13} = 0{,}076923076\ldots$



***Figuur 8** – De staartdeling voor $\frac{1}{13}$*

We berekenen ook de decimale schrijfwijze van $\frac{2}{13}$, $\frac{3}{13}$ … $\frac{12}{13}$:

$$\frac{1}{13} = 0{,}076923076\ldots \qquad \frac{2}{13} = 0{,}153846153\ldots$$
$$\frac{3}{13} = 0{,}230769230\ldots \qquad \frac{5}{13} = 0{,}384615384\ldots$$
$$\frac{4}{13} = 0{,}307692307\ldots \qquad \frac{6}{13} = 0{,}461538461\ldots$$
$$\frac{9}{13} = 0{,}692307692\ldots \qquad \frac{7}{13} = 0{,}538461538\ldots$$
$$\frac{10}{13} = 0{,}769230769\ldots \qquad \frac{8}{13} = 0{,}615384615\ldots$$
$$\frac{12}{13} = 0{,}923076923\ldots \qquad \frac{11}{13} = 0{,}846153846\ldots$$

Hier is iets anders aan de hand: blijkbaar zijn er nu twee groepen van repeterende decimalen die elk de helft van de breuken $\frac{1}{13}$, $\frac{2}{13}$ … $\frac{12}{13}$ voorstellen.

Waarom zijn het net de breuken $\frac{1}{13}$, $\frac{3}{13}$, $\frac{4}{13}$, $\frac{9}{13}$, $\frac{10}{13}$ en $\frac{12}{13}$ die samen een groepje vormen en idem voor de breuken $\frac{2}{13}$, $\frac{5}{13}$, $\frac{6}{13}$, $\frac{7}{13}$, $\frac{8}{13}$ en $\frac{11}{13}$? Waarom die onderverdeling? Deze vragen kunnen beantwoord worden vanuit de getaltheorie, maar we kunnen ze ook bekijken vanuit het perspectief van groepentheorie. Om dat te doen, hebben we eerst enkele nieuwe begrippen en eigenschappen nodig.

3.2 Modulorekenen

De rood onderlijnde getallen in de staartdelingen van Figuur 7 en Figuur 8 zijn telkens resten bij deling door respectievelijk 7 en 13. Dit brengt ons bij modulorekenen. In de loep van Uitwiskeling 24/3 (2008) gingen we hier al dieper op in. Daar vind je nauwkeurige definities, eigenschappen en suggesties om dit aan te brengen in de klas. In de loep van Uitwiskeling 28/3 (2012) vind je toepassingen van modulorekenen in cryptografie. Omdat we in de loep die je nu leest modulorekenen enkel als context gebruiken voor groepen, overlopen we kort en eerder informeel de nodige begrippen.

Bij modulorekenen bekijken we van een geheel getal niet langer zijn waarde maar enkel zijn rest bij deling door een vooraf bepaald natuurlijk getal n (met $n \geq 1$). We groeperen dan de gehele getallen met dezelfde rest. In Tabel 1 deden we dit voor $n = 7$. De mogelijke resten bij deling door 7 zijn 0, 1…6. In elke kolom zie je de gehele getallen met die specifieke rest.

0	1	2	3	4	5	6
⋮	⋮	⋮	⋮	⋮	⋮	⋮
−7	−6	−5	−4	−3	−2	−1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
⋮	⋮	⋮	⋮	⋮	⋮	⋮

***Tabel 1** – De gehele getallen gerangschikt naar hun rest bij deling door 7*

Getallen uit dezelfde kolom staan in verband met elkaar omdat ze dezelfde rest hebben na deling door 7.

De volgende definitie legt dit concept vast voor willekeurige n.

Definitie • Congruent modulo n

Twee gehele getallen x en y met dezelfde rest bij deling door n (met $n \in \mathbb{N}_0$) worden congruent modulo n genoemd. We noteren dit als

$$x \equiv y \pmod{n}.$$

De relatie 'congruent modulo n' verdeelt de verzameling $\mathbb{Z}$ in *restklassen*. Voor $n = 7$ zijn er zeven restklassen, die overeen komen met de zeven verzamelingen van getallen in de kolommen van Tabel 1. Elke verzameling krijgt een naam, bijvoorbeeld de verzameling van alle gehele getallen die rest 3 hebben bij deling door 7:

$$\begin{aligned}\overline{3} &= \{b \in \mathbb{Z} \mid b \equiv 3 \pmod{7}\} \\ &= \{\ldots -4, 3, 10, 17, 24 \ldots\}.\end{aligned}$$

Voor een willekeurige n geldt dan de volgende definitie:

Definitie • Restklasse

$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$

Er zijn bij deling door n precies n verschillende resten $0, 1, 2 \ldots n-1$ mogelijk. Om die reden zijn er ook precies n restklassen. De verzameling van die restklassen noteren we als $\mathbb{Z}_n$. Er geldt dus:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2} \ldots \overline{n-1}\}.$$

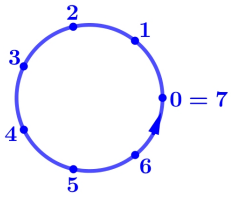
Merk op dat we ook andere gehele getallen kunnen nemen om de restklassen voor te stellen. Zo is bijvoorbeeld $\overline{156} = \overline{148} = \overline{4} = \overline{-12}$ in $\mathbb{Z}_8$ omdat 156, 148, 4 en -12 dezelfde rest hebben bij deling door 8.

Als uit de context duidelijk is dat je met restklassen rekent, laat men na verloop van tijd soms de streepjes weg in de notatie en noteert men de restklasse $\overline{3}$ gewoon als 3. Zo ook noteert men dan $\mathbb{Z}_n = \{0, 1, 2 \ldots n-1\}$. Verderop in deze paragraaf zullen we dat ook doen.

Dankzij het modulorekenen kun je een willekeurig geheel getal steeds reduceren tot een getal tussen 0 en $n-1$ en kunnen we dus steeds werken met eindige getallenverzamelingen $\mathbb{Z}_n$. Je kunt dit 'zien' als werken op een getallenas die je oprolt tot een cirkel i.p.v. op een rechte as (zie Figuur 9 en Figuur 10)



***Figuur 9** – De getallenas van de gehele getallen*



***Figuur 10** – De getallenas opgerold, voor het rekenen in $\mathbb{Z}_7$*

Een heel gekende en natuurlijke context waarin we het principe van modulorekenen gebruiken, is het kloklezen. Daarbij werken we in $\mathbb{Z}_{12}$ of in $\mathbb{Z}_{24}$. Als je bijvoorbeeld om 23u begint te kijken naar een film die 3 uur duurt dan eindigt deze film om 2 uur. We rekenen modulo 24: $23 + 3 = 26 \equiv 2 \pmod{24}$ of nog $\overline{23} + \overline{3} = \overline{26} = \overline{2}$ in $\mathbb{Z}_{24}$. Een ander voorbeeld is het rekenen in $\mathbb{Z}_{12}$ met de maanden van een jaar. Stel dat het nu september is, welke maand is het dan binnen 27 maanden? Om het antwoord te vinden, hoef je niet te starten bij september en dan 27 maanden stap voor stap verder te tellen. Het volstaat om de rest te berekenen bij deling van 27 door 12, $27 \equiv 3 \pmod{12}$, en dus moet je 3 maanden verder tellen vanaf september om het antwoord te vinden. 27 maanden later zitten we in de maand december. Op dezelfde manier weet je dat als het nu woensdag is, het binnen 23 dagen vrijdag is. We weten immers: $\overline{23} = \overline{2}$ in $\mathbb{Z}_7$ en dus moet je twee dagen verder tellen vanaf woensdag.

We kunnen nu de bewerkingen met gehele getallen overdragen op restklassen als volgt:

Definitie • Som en product van restklassen

Voor twee restklassen $\overline{a}$ en $\overline{b}$ in $\mathbb{Z}_n$ geldt:

$$\overline{a} + \overline{b} = \overline{a + b}$$

en

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

De optelling van restklassen komt regelmatig voor in alledaagse contexten, zoals het voorbeeld van de film hierboven: $\overline{23} + \overline{3} = \overline{23 + 3} = \overline{26} = \overline{2}$ in $\mathbb{Z}_{24}$.

We illustreren ook de vermenigvuldiging van restklassen. In $\mathbb{Z}_{26}$ geldt: $\overline{57} \cdot \overline{100} = \overline{57 \cdot 100} = \overline{5700} = \overline{6}$. Merk op dat je hetzelfde resultaat vindt met andere representanten: $\overline{57} \cdot \overline{100} = \overline{5} \cdot \overline{22} = \overline{110} = \overline{6}$.

Algemeen kun je aantonen dat de definities van de optelling en de vermenigvuldiging van restklassen niet afhangen van de gekozen representanten voor die restklassen.

De + en de · in het linkerlid van deze definitie zijn de nieuwe optelling en de nieuwe vermenigvuldiging van restklassen. In het rechterlid staan de gewone som en het gewone product in $\mathbb{Z}$. Toch schrijven we voor de eenvoud twee keer hetzelfde symbool.

Wanneer je in de klas groepen centraal stelt, kun je misschien best informeel omgaan met modulorekenen. Het risico bestaat immers dat je anders teveel tijd 'verliest'. Het zou zelfs informeler kunnen dan wij hier nu doen. In plaats van de overgang te maken naar restklassen modulo n, zou je enkel kunnen blijven werken met de getallen die als rest voorkomen bij de deling door n (dus niet rekenen met verzamelingen maar met getallen). Als je dan bij optellen of vermenigvuldigen een te groot getal uitkomt, trek je een aantal keer n af om weer bij een rest uit te komen.

3.3 Groepen van restklassen

Net zoals we dat voor samenstellingen van transformaties deden, kunnen we nu cayleytabellen maken voor de optelling en vermenigvuldiging van restklassen. In wat volgt, noteren we restklassen niet langer met de streepjes boven de getallen. De cayleytabel voor de optelling in $\mathbb{Z}_7$ ziet er dan als volgt uit (we gebruiken dezelfde conventies als voorheen):

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

We herkennen het typische Latijns vierkant dat we ook al vonden bij de symmetriegroepen van vlakke figuren. We onderzoeken nu enkele eigenschappen van het optellen in $\mathbb{Z}_7$.

1. $\mathbb{Z}_7$ is gesloten voor het optellen.
   Er verschijnen geen nieuwe restklassen in de cayleytabel.
2. Om sommen te kunnen maken met meer dan twee termen is het relevant om associativiteit van de nieuwe bewerking te onderzoeken. We stellen vast dat het optellen in $\mathbb{Z}_7$ associatief is. Het vraagt te veel rekenwerk om dat uit de tabel af te leiden. Wel zien we eenvoudig in dat de associativiteit van de optelling in $\mathbb{Z}_7$ rechtstreeks volgt uit de associativiteit van het optellen in $\mathbb{Z}$. De definitie van de optelling in $\mathbb{Z}_7$ is immers gebaseerd op de optelling in $\mathbb{Z}$.
3. Er is een neutraal element voor de optelling in $\mathbb{Z}_7$, namelijk 0.
   Je ziet in de eerste rij en de eerste kolom van de cayleytabel dat 0 optellen bij een getal (een restklasse!) niets verandert aan dat getal.
4. Elk element heeft een invers element voor de optelling in $\mathbb{Z}_7$.
   We zien immers dat in elke rij en kolom van de cayleytabel 0 voorkomt. Het invers element (het tegengestelde) van 3 bijvoorbeeld is 4 en we noteren dit op de gebruikelijke manier als $-3 = 4$.
5. Het optellen in $\mathbb{Z}_7$ is commutatief.
   We zien dat er in de cayleytabel symmetrie is tegenover de diagonaal die van links boven naar rechts onder gaat. Dit betekent dat $a+b = b+a$ voor elk paar elementen uit $\mathbb{Z}_7$.

De kenmerken 1, 2, 3 en 4 die we hierboven onderzochten, vatten we samen door te zeggen dat $\mathbb{Z}_7$ een groep vormt voor de optelling. Wegens de commutativiteit spreken we van een commutatieve groep.

We veralgemenen voor $\mathbb{Z}_n$:

Eigenschap • Een groep van restklassen

De verzameling $\mathbb{Z}_n$ van restklassen modulo n vormt een groep voor de optelling van restklassen. Anders geformuleerd: $\mathbb{Z}_n$,+ is een groep. Dit betekent:

- $\mathbb{Z}_n$ is gesloten voor de optelling.
  $\forall a,b \in \mathbb{Z}_n : a + b \in \mathbb{Z}_n$
- De optelling is associatief in $\mathbb{Z}_n$.
  $\forall a,b,c \in \mathbb{Z}_n : (a + b) + c = a + (b + c)$

- Er is een neutraal element voor de optelling in $\mathbb{Z}_n$, namelijk 0.
  $\forall a \in \mathbb{Z}_n : a + 0 = a = 0 + a$ met $0 \in \mathbb{Z}_n$
- Elk element heeft een invers element voor de optelling in $\mathbb{Z}_n$.
  $\forall a \in \mathbb{Z}_n, \exists b \in \mathbb{Z}_n : a + b = 0 = b + a$

We noteren: $b = -a$ en noemen b het tegengestelde element van a.

In de volgende lesactiviteit onderzoeken we andere groepen van restklassen, onder andere voor het vermenigvuldigen van restklassen.

LESACTIVITEIT

Groepen van restklassen

We weten al dat $\mathbb{Z}_n$ (voor $n \in \mathbb{N}_0$) een groep vormt voor de optelling van restklassen. Zijn er nog andere groepen van restklassen, eventueel voor het product?

We spreken van een groep G van restklassen voor een bewerking ($+$ of $\cdot$) als er voldaan is aan de vier eigenschappen die we ook bij $\mathbb{Z}_7$,$+$ tegenkwamen:

- G is gesloten voor die bewerking.
- De bewerking is associatief in G.
- Er is een neutraal element voor de bewerking in G.
- Elk element heeft een invers element voor de bewerking in G.

1 Vormt $\mathbb{Z}_n$ een groep voor de vermenigvuldiging van restklassen? Maak om dit te onderzoeken de cayleytabel voor $\mathbb{Z}_4$ en die voor $\mathbb{Z}_7$.

✔ *De gevraagde cayleytabellen:*

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

We kunnen duidelijk niet veralgemenen dat $\mathbb{Z}_n$ een groep vormt voor de vermenigvuldiging van restklassen. Er is namelijk een probleem met de eerste rij en de eerste kolom uit de cayleytabellen. Die bestaan enkel uit nullen. 0 heeft dus geen invers element voor de vermenigvuldiging. Het neutraal element voor de vermenigvuldiging van restklassen is immers 1 en dit komt niet voor in de eerste rij of de eerste kolom. We zeggen dat 0 een opslorpend element is voor de vermenigvuldiging van restklassen.

2 Kun je uit $\mathbb{Z}_7$ een element verwijderen zó dat een groep overblijft voor de vermenigvuldiging?

✔ *Ja, je kunt eenvoudig nagaan dat $\mathbb{Z}_7 \setminus \{0\}$ een groep vormt voor de vermenigvuldiging. De cayleytabel ziet er uit als volgt:*

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Er worden geen nieuwe elementen gevormd in de cayleytabel en dus is $\mathbb{Z}_7 \setminus \{0\}$ gesloten voor de vermenigvuldiging. Associativiteit van de vermenigvuldiging van restklassen volgt rechtstreeks uit de associativiteit van de vermenigvuldiging in $\mathbb{Z}$. De eerste rij en de eerste kolom in de tabel leren ons dat 1 het neutraal element is voor de vermenigvuldiging. Verder zien we dat 1 voorkomt in elke rij en elke kolom. Elk element heeft een invers element voor de vermenigvuldiging.

3 Bepaal van elk element uit $\mathbb{Z}_7 \setminus \{0\}$ het invers element voor de vermenigvuldiging.

✔ *Het invers element van 1 is 1. We noteren dit als $1^{-1} = 1$. Het invers element van 2 is 4 of nog $2^{-1} = 4$. Verder geldt: $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$ en $6^{-1} = 6$. Niet alleen 1, maar ook 6 heeft dus zichzelf als inverse. We noemen deze inverse elementen voor de vermenigvuldiging ook de omgekeerde elementen.*

4 Kun je op dezelfde manier uit $\mathbb{Z}_4$ element(en) verwijderen zó dat een groep overblijft voor de vermenigvuldiging? Verklaar.

✔ *Ja. Je moet al zeker het opslorpend element 0 verwijderen. $\mathbb{Z}_4 \setminus \{0\}$ is dan echter niet meer gesloten voor de vermenigvuldiging want in de rij van de 2 komt nog een 0 voor. Dat is opmerkelijk: blijkbaar is $2 \cdot 2 = 0$ terwijl $2 \neq 0$. We noemen 2 daarom een nuldeler. Algemeen zijn nuldelers getallen die zelf geen nul zijn maar waarvoor het product wél nul is. Als we ook 2 verwijderen uit $\mathbb{Z}_4$, ziet de cayleytabel met de overblijvende restklassen 1 en 3 er uit als volgt:*

·	1	3
1	1	3
3	3	1

We stellen vast: $\mathbb{Z}_4 \setminus \{0,2\}$ vormt een groep voor de vermenigvuldiging.

5 Als n een priemgetal is dan vormt $Z_n \setminus \{0\}$ een groep voor de vermenigvuldiging. Verklaar dit intuïtief.

✔ *Het probleem in de cayleytabel van $\mathbb{Z}_4 \setminus \{0\}$ is dat er een 0 voorkomt in de rij van de 2 waardoor de verzameling niet meer gesloten is voor de vermenigvuldiging. Wanneer krijgen we zulke rijen met een 0 er in? Algemeen geldt voor $n > 1$: $a \cdot b \equiv 0 \pmod{n}$ als $a \cdot b$ een veelvoud is van n. Dan geldt $ggd(a,n) \neq 1$ of $ggd(b,n) \neq 1$ voor $a, b \in \mathbb{Z}_n$. Als n priem is, sluit je deze situatie sowieso uit. We besluiten: als n een priemgetal is, dan is $\mathbb{Z}_n \setminus \{0\}$ een groep voor de vermenigvuldiging.*

Eigenschap • Een groep van restklassen

De verzameling $\mathbb{Z}_p \setminus \{0\}$ met p priem vormt een groep voor de vermenigvuldiging van restklassen. Anders geformuleerd: $\mathbb{Z}_p \setminus \{0\}, \cdot$ is een groep. Dit betekent:

- $\mathbb{Z}_p \setminus \{0\}$ is gesloten voor de vermenigvuldiging.
  $\forall a,b \in \mathbb{Z}_p \setminus \{0\} : a \cdot b \in \mathbb{Z}_p \setminus \{0\}$
- De vermenigvuldiging is associatief in $\mathbb{Z}_p \setminus \{0\}$.
  $\forall a,b,c \in \mathbb{Z}_p \setminus \{0\} : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Er is een neutraal element voor de vermenigvuldiging in $\mathbb{Z}_p \setminus \{0\}$, namelijk 1.
  $\forall a \in \mathbb{Z}_p \setminus \{0\} : a \cdot 1 = a = 1 \cdot a$ met $1 \in \mathbb{Z}_p \setminus \{0\}$
- Elk element heeft een invers element voor de vermenigvuldiging in $\mathbb{Z}_p \setminus \{0\}$.
  $\forall a \in \mathbb{Z}_p \setminus \{0\}, \exists b \in \mathbb{Z}_p \setminus \{0\} : a \cdot b = 1 = b \cdot a$
  We noteren: $b = a^{-1}$ en noemen b de omgekeerde van a.

Merk op dat we hier snel over begrippen en eigenschappen gaan m.b.t. deelbaarheid en dergelijke. Voor een meer rigoureuze behandeling van de theorie verwijzen we naar Uitwiskeling 24/3 (2008). Daar vind je ook een nauwkeurig bewijs van de vorige eigenschap.

6 Hieronder zie je de vermenigvuldigingstabel voor $\mathbb{Z}_{12}$ die we vonden via Wolfram Demonstrations Project (Muradian). De bewerking is hier vermenigvuldigen modulo 12. Welke restklassen moet je uit $\mathbb{Z}_{12}$ schrappen zó dat er een groep overblijft voor de vermenigvuldiging?

⊗	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

✔ *We schrappen al zeker* 0 *en gaan verder na welke elementen geen inverse hebben. Dat zijn* 2, 3, 4, 6, 8, 9 *en* 10. *Dit zijn niet toevallig ook de elementen die nuldelers zijn: er komen nullen voor in hun rijen of kolommen. We schrappen al deze elementen uit* $\mathbb{Z}_{12}$. *De overblijvende elementen vormen de verzameling van alle elementen die wél een inverse hebben voor de vermenigvuldiging in* $\mathbb{Z}_{12}$ *en we noteren deze verzameling als* $\mathbb{Z}_{12}^* = \{1,5,7,11\}$. *Merk op dat deze verzameling bestaat uit alle getallen uit de verzameling* $\{0,1,2 \ldots 11\}$ *die relatief priem zijn met* 12. *Ze hebben geen gemeenschappelijke delers met* 12 *(buiten* 1*). Merk bovendien op dat voor elk van de elementen* a *van* $\mathbb{Z}_{12}^*$ $a^2 = 1$. *Elk element is zijn eigen invers. De cayleytabel ziet er voor deze verzameling uit als volgt:*

·	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

We kunnen nu nagaan dat $\mathbb{Z}_{12}^*$ een groep vormt voor de vermenigvuldiging in $\mathbb{Z}_{12}$. Er worden geen nieuwe elementen gevormd in de cayleytabel en dus is $\mathbb{Z}_{12}^*$ gesloten voor de vermenigvuldiging. Associativiteit van de vermenigvuldiging van restklassen volgt rechtstreeks uit de associativiteit van de vermenigvuldiging in $\mathbb{Z}$. De eerste rij en de eerste kolom in de tabel leren ons dat 1 het neutraal element is voor de vermenigvuldiging. Verder zien we dat 1 voorkomt in elke rij en elke kolom. Dit betekent dat elk element een invers element heeft voor de vermenigvuldiging.

Algemeen gelden de volgende eigenschappen:

Eigenschap • Inverse voor de vermenigvuldiging in $\mathbb{Z}_n$

a heeft een inverse voor de vermenigvuldiging in $\mathbb{Z}_n$ als en slechts als a en n relatief priem zijn of nog als en slechts als $\text{ggd}(a,n) = 1$.

Eigenschap • De groep van de inverteerbare elementen voor de vermenigvuldiging in $\mathbb{Z}_n$

Stel $\mathbb{Z}_n^*$ de verzameling van alle restklassen a met $1 \leq a \leq n-1$ en a relatief priem met n. Deze verzameling is een groep voor de vermenigvuldiging in $\mathbb{Z}_n$, de groep van alle inverteerbare elementen voor die vermenigvuldiging.

Voor bewijzen van deze eigenschappen verwijzen we naar Uitwiskeling 24/3 (2008) en naar Gallian (2017).

7 We weten ondertussen dat $\mathbb{Z}_9$,+ een groep vormt. Via Wolfram Demonstrations Project (Muradian) vinden we de cayleytabel:

$\oplus$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

We bekijken de deelverzameling $H = \{0,3,6\}$ van $\mathbb{Z}_9$. Maak een cayleytabel voor de optelling in H en onderzoek de groepseigenschappen. Wat stel je vast?

✔ *De cayleytabel voor H is*

+	0	3	6
0	0	3	6
3	3	6	0
6	6	0	3

We zien weer het Latijns vierkant opduiken. H is een groep voor de optelling in $\mathbb{Z}_9$. Het is een deelgroep van $\mathbb{Z}_9$ en we noteren dit als $H,+ \subset \mathbb{Z}_9,+$.

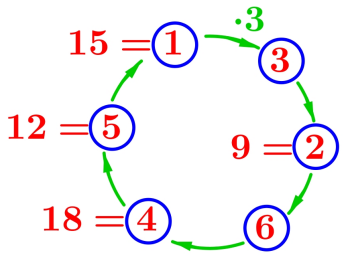
8 Bekijk de verzameling $H+1 = \{1,4,7\}$ die je vindt door bij elk element van de deelgroep H 1 op te tellen. We noemen dit een nevenklasse van H. Is deze nevenklasse een groep voor de optelling in $\mathbb{Z}_9$? Verklaar je antwoord.

✔ *Nee, dit is geen groep want het neutraal element 0 behoort niet tot $H+1$. Meestal zijn nevenklassen geen deelgroepen.*

9 Zoek alle mogelijke deelgroepen van $\mathbb{Z}_6,+$.

✔ *Met wat puzzel- en zoekwerk in de cayleytabel vinden we dat $\{0,3\}$ en $\{0,2,4\}$ deelgroepen zijn van $\mathbb{Z}_6,+$. Natuurlijk zijn er daarnaast nog de triviale deelgroepen, $\{0\}$ en $\mathbb{Z}_6$.*

Er zijn manieren om meer gestructureerd deelgroepen te zoeken in $\mathbb{Z}_n$. Bekijken we bijvoorbeeld opnieuw de groep $\mathbb{Z}_7 \setminus \{0\}$, uitgerust met de vermenigvuldiging. Als 3 in een deelgroep zit, dan moeten ook alle machten van 3 in die deelgroep zitten. Dit levert het rijtje $3^0 = 1$, 3, $3^2 = 9 = 2$, $3^3 = 3^2 \cdot 3 = 2 \cdot 3 = 6$, $3^4 = 3^3 \cdot 3 = 6 \cdot 3 = 18 = 4$, $3^5 = 3^4 \cdot 3 = 4 \cdot 3 = 12 = 5$, $3^6 = 3^5 \cdot 3 = 5 \cdot 3 = 15 = 1$. Omdat we 1 vinden, weten we dat $3^7 = 3$ en dit brengt ons terug bij de start van het rijtje. Dit wordt gevisualiseerd in de figuur hieronder.



Het rijtje vormt de verzameling $\{1,2,3,4,5,6\}$ en we noteren deze met $\langle 3 \rangle$. Het valt op dat $\langle 3 \rangle = \mathbb{Z}_7 \setminus \{0\}$. We zeggen daarom dat 3 de verzameling $\mathbb{Z}_7 \setminus \{0\}$ voortbrengt of dat het een generator is van $\mathbb{Z}_7 \setminus \{0\}$.

10 Geldt dit ook voor de andere elementen? Zijn dat allemaal generatoren van $\mathbb{Z}_7 \setminus \{0\}$?

✔ *We rekenen het na voor de verschillende elementen:*

- $\langle 2 \rangle = \{1,2,4\}$ *want na drie stappen ben je terug bij* 1: $2^3 = 8 = 1$. *Bijgevolg is* 2 *geen voortbrengend element van* $\mathbb{Z}_7 \setminus \{0\}$. *Omdat* $2^3 = 1$ *zeggen we dat de orde van* $\langle 2 \rangle$ *gelijk is aan* 3. *Merk op dat die orde logischerwijs gelijk is aan het aantal elementen van* $\langle 2 \rangle$.
- *Je kunt narekenen dat ook* $\langle 4 \rangle = \{1,2,4\}$. *De orde van* $\langle 4 \rangle$ *is dus ook* 3.
- 5 *brengt wel heel* $\mathbb{Z}_7 \setminus \{0\}$ *voort:* $\langle 5 \rangle = \mathbb{Z}_7 \setminus \{0\}$.
- $\langle 6 \rangle = \{1,6\}$ *omdat* $6^2 = 1$. *De orde van* $\langle 6 \rangle$ *is dus* 2.

11 Maak de cayleytabellen voor $\langle 2 \rangle$ en voor $\langle 6 \rangle$ met de vermenigvuldiging in $\mathbb{Z}_7 \setminus \{0\}$. Wat stel je vast?

✔ *De gevraagde cayleytabellen:*

·	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

·	1	6
1	1	6
6	6	1

We stellen vast dat zowel $\langle 2\rangle$ als $\langle 6\rangle$ deelgroepen vormen voor de vermenigvuldiging modulo 7. Dit kun je ook intuïtief inzien: als je twee machten van 2 met elkaar vermenigvuldigt, dan krijg je opnieuw een macht van 2.

Door opeenvolgende machten te nemen van elementen (verschillend van 1) van $\mathbb{Z}_7 \setminus \{0\}$ vinden we op een meer gestructureerde manier deelgroepen van $\mathbb{Z}_7 \setminus \{0\},\cdot$. Merk op dat we hierbij slechts de deelgroepen vinden met één generator. Dat zijn in het algemeen niet alle deelgroepen.

Deze oefening illustreert een algemene eigenschap van groepen.

Eigenschap • $\langle a\rangle$ is een deelgroep

Stel gegeven een groep G en stel dat a een element is van G. Dan is $\langle a\rangle$ altijd een deelgroep van G.

Merk op dat dit zowel om groepen met de optelling van restklassen als bewerking kan gaan als om groepen met de vermenigvuldiging als bewerking. Kijken we bijvoorbeeld naar oefening 7. Je kunt daar narekenen dat de groep H uit die oefening gelijk is aan $\langle 3\rangle$. De bewerking bij die groep is de optelling en dus berekenen we $\langle 3\rangle$ door opeenvolgende veelvouden van 3 te berekenen: we starten bij 0 en tellen daar 3 bij op. Doen we dat nog eens dan vinden we 6 en doen we dat dan nog eens dan vinden we $9 = 0$. Het cirkeltje is rond en $\langle 3\rangle = \{0,3,6\}$. Het is dus geen verrassing dat H een deelgroep is van $\mathbb{Z}_9,+$.

Stel dat G de groep $\mathbb{Z}_n,+$ is (additieve groep) of de groep $\mathbb{Z}_n \setminus \{0\},\cdot$ (multiplicatieve groep). Je kunt dan aantonen dat de orde van een element van G altijd een deler is van de orde van G. Dit klopt met de concrete gevallen die we hebben nagerekend: de orde van 2 in $\mathbb{Z}_7 \setminus \{0\}$ is 3 en dat is een deler van 6, de orde van $\mathbb{Z}_7 \setminus \{0\}$. Bovendien: als de grootste gemene deler van een element a van G en de orde van G gelijk is aan 1, dan is $\langle a\rangle = G$. Ook dat klopt met onze bevindingen.

12 Bereken $\langle a\rangle$ voor elk element a van $\mathbb{Z}_9,+$ dat niet gelijk is aan 0.

✓ $\langle 1\rangle = \langle 2\rangle = \langle 4\rangle = \langle 5\rangle = \langle 7\rangle = \langle 8\rangle = \mathbb{Z}_9$. *Dit weten we zonder rekenwerk uit de eigenschap die hierboven is beschreven: zowel voor 1, 2, 4, 5, 7 als 8 geldt dat ze onderling ondeelbaar zijn met 9, de orde van $\mathbb{Z}_9$. Verder kunnen we narekenen dat $\langle 6\rangle = \langle 3\rangle$.*

13 Is de verzameling $G = \{5,15,25,35\}$ een groep voor de vermenigvuldiging in $\mathbb{Z}_{40}$? Verklaar je antwoord.

✓ *We maken de cayleytabel:*

·	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

Als je deze tabel goed bestudeert, zie je dat 25 het neutraal element is voor deze vermenigvuldiging. We kunnen de cayleytabel herschikken om dit duidelijker te tonen.

·	25	5	15	35
25	25	5	15	35
5	5	25	35	15
15	15	35	25	5
35	35	15	5	25

Ook de andere groepsvoorwaarden zijn voldaan. Dus: ja, G vormt een groep voor de vermenigvuldiging in $\mathbb{Z}_{40}$. Het neutraal element is dus niet altijd 1. Merk op dat G geen deelgroep is van de multiplicatieve groep $\mathbb{Z}_{40}^*$ (de elementen van G behoren niet tot $\mathbb{Z}_{40}^*$).

Merk op dat we hierboven bij de formulering van de eigenschappen rond de inverse voor de vermenigvuldiging in $\mathbb{Z}_n$ niet meer expliciet het onderscheid maken tussen een geheel getal a en de restklasse waartoe a behoort. Bovendien noteren we deze restklasse ook gewoon met a. Deze mate van abstractie is misschien voor sommige leerlingen moeilijk. Zoals al gezegd: als je puur de nadruk wilt leggen op groepen, kun je het werken met restklassen weglaten en enkel spreken van delers en gehele getallen.

Om af te ronden, komen we terug op de vragen die we stelden bij de repeterende decimale vormen.

3.4 Opnieuw de repeterende decimale vormen

Met de kennis die we nu hebben, kunnen we een antwoord geven op die vragen. Bekijken we opnieuw de deling in Figuur 7. We weten dat de rij van de decimalen zich herhaalt doordat de rest die we telkens berekenen op een bepaald moment opnieuw 1 is. De rij van de resten (rood onderlijnd in Figuur 7 en Figuur 8) is dus belangrijk en niet zozeer de decimalen in de ontwikkeling zelf. De rij van de resten die zich steeds herhalen, is bij de deling met noemer 7 gelijk aan 1, 3, 2, 6, 4, 5. De 0 komt hierin niet voor omdat het gaat om een repeterende decimale vorm. Dit zijn de elementen van $\mathbb{Z}_7 \setminus \{0\}$ en we weten ondertussen dat deze verzameling een groep vormt voor de vermenigvuldiging. Maar wat is dan het verschil met de breuken met noemer 13? Waarom zijn er daar twee verschillende repeterende delen?

Bekijken we goed de rood onderlijnde resten. Die vinden we door in de staartdeling telkens de vorige rest met 10 te vermenigvuldigen (we zetten er een nul bij) en daar de rest van te berekenen bij deling door 7 respectievelijk 13. Stel dat in een bepaalde stap in de deling de rest r is, dan is de volgende rest $10r \pmod 7$ respectievelijk $10r \pmod{13}$. Als we dit herhalen, krijgen we opeenvolgende machten van 10. We berekenen hierbij dus eigenlijk telkens $\langle 10 \rangle$.

Wanneer we starten met k (voor de berekening van $\frac{k}{7}$ met $k = 1, 2, 3 \ldots 6$), vormen de opeenvolgende resten het rijtje getallen k vermenigvuldigd met de opeenvolgende machten van 10. De opeenvolgende resten vormen bijgevolg een meetkundige rij met beginterm k en quotiënt 10. Voor $k = 1$ in $\mathbb{Z}_7$, krijg je dan het rijtje 1, 3, 2, 6, 4, 5, dat heel $\mathbb{Z}_7 \setminus \{0\}$ doorloopt. Voor andere waarden van k start je elders in het rijtje maar houd je verder dezelfde volgorde aan, waarbij je op het einde naar het begin springt. Alle breuken $\frac{k}{7}$ hebben dus hetzelfde groepje van decimalen in hun ontwikkeling.

Als je in $\mathbb{Z}_{13}$ rekent, krijg je voor $k = 1$ na vermenigvuldigen met de opeenvolgende machten van 10 het rijtje 1, 10, 9, 12, 3, 4. Omdat er al herhaling optreedt na 6 elementen, doorloopt het rijtje nu niet heel $\mathbb{Z}_{13} \setminus \{0\}$. Omdat 2 niet tot dat

rijtje behoort, krijg je voor $k = 2$ een ander rijtje: 2, 7, 5, 11, 6, 8. Het is geen toeval dat de beide rijtjes even lang zijn: elk element van het eerste rijtje wordt afgebeeld op juist één overeenkomstig element van het tweede rijtje door te vermenigvuldigen met 2 (een bijectie). Het is ook geen toeval dat de rijtjes geen elementen gemeen hebben. Verder is de unie van beide rijtjes heel $\mathbb{Z}_{13} \setminus \{0\}$. Voor alle andere waarden van k kom je daardoor ofwel in het eerste ofwel in het tweede rijtje terecht. Je start daarbij telkens wel elders in dat rijtje maar je houdt verder dezelfde volgorde aan, waarbij je op het einde naar het begin springt. De elementen van het eerste rijtje vormen de verzameling $\langle 10 \rangle = \{1,10,9,12,3,4\}$. Dit is een deelgroep van $\mathbb{Z}_{13} \setminus \{0\}$. De verzameling $2\langle 10 \rangle = \{2, 7, 5, 11, 6, 8\}$ is geen deelgroep, maar ontstaat door elk element van de deelgroep te vermenigvuldigen met een getal buiten die deelgroep. Zo'n verzameling hebben we eerder al een nevenklasse genoemd.

Dit alles vormt een mooie aanzet naar de stelling van Lagrange die we achteraan in deze loep bewijzen. Het feit dat $k\langle 10 \rangle$ even veel elementen heeft als $\langle 10 \rangle$ is een rechtstreekse toepassing van die stelling.

Stel dat we met noemers 41 werken. In $\mathbb{Z}_{41} \setminus \{0\}$ is $\langle 10 \rangle = \{1,10,18,16,37\}$. De nevenklassen zijn $k\langle 10 \rangle$. Je kunt gemakkelijk inzien dat die ook telkens 5 elementen tellen en onderling disjunct zijn. We weten dat $\mathbb{Z}_{41} \setminus \{0\}$ orde 40 heeft en dus zullen er 8 verschillende rijtjes van resten ontstaan. Je kunt narekenen dat dit de rijtjes zijn met $k = 1, 2, 3, 4, 5, 6, 11, 15$. We weten zo bijvoorbeeld dat de decimale ontwikkeling van $\frac{26}{41}$ een repeterend deel van 5 decimalen bevat. Bovendien kunnen we narekenen dat 26 in de nevenklasse $6\langle 10 \rangle = \{19,26,14,17,6\}$ zit. De resten in de staartdeling zullen dus beginnen bij 26, gevolgd door 14, 17, 6, 19, dan terug 26… Het repeterende rijtje decimalen is dan 63414.

Bij deze voorbeelden zijn de noemers priemgetallen. Wat als dat niet het geval is en de noemer bijvoorbeeld 39 is met teller k voor $k = 1, 2 \ldots 38$? Uit deze verzameling breuken kunnen we de vereenvoudigbare breuken, zoals $\frac{3}{39} = \frac{1}{13}$ schrappen omdat we die al tegenkwamen. Welke tellers blijven over? Dat is niet zomaar een verzameling getallen: het is de verzameling van alle elementen van $\mathbb{Z}_{39} \setminus \{0\}$ die onderling ondeelbaar of relatief priem zijn met 39. Deze verzameling kennen we al: het is de groep van de inverteerbare elementen voor de vermenigvuldiging modulo 39. Met de ϕ-functie van Euler kun je de orde van deze groep berekenen. Het is voor leerlingen die geïnteresseerd zijn in abstracte leerstof een mooie opdracht om hier verder op door te bomen en de achterliggende theorie te doorgronden.

4 Abstracte groepen

In de vorige paragrafen kwamen we groepen tegen in heel verschillende contexten. Een symmetriegroep van een vlakke figuur is iets helemaal anders dan een groep die we bij het modulorekenen tegenkwamen. En toch voldoen ze aan dezelfde regels. Meer nog: soms lijken twee groepen uit verschillende contexten wel dezelfde groep te zijn. Je ziet hier de cayleytabel van de groep $\mathbb{Z}_4, +$ en die van Rot(□),∘, de rotaties van een vierkant.

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

∘	I	r	r^2	r^3
I	I	r	r^2	r^3
r	r	r^2	r^3	I
r^2	r^2	r^3	I	r
r^3	r^3	I	r	r^2

Op de betekenis van de elementen en van de bewerking na, is het eigenlijk twee keer dezelfde tabel. Elk element van $\mathbb{Z}_4$ komt overeen met juist één element van Rot(□) (en omgekeerd), op zo'n manier dat op elke plaats in de tabellen (bv. tweede rij, derde kolom) overeenkomstige elementen staan. We zeggen dat beide groepen *isomorf* zijn (van het Grieks: $\iota\sigma o\varsigma$ = gelijk en $\mu o\rho\varphi\eta$ = vorm), notatie:

$$\mathbb{Z}_4, + \cong \text{Rot}(\square), \circ\,.$$

Algebraïsch bekeken is er eigenlijk geen verschil tussen het optellen modulo 4 en het samenstellen van rotaties rond een punt over veelvouden van 90°.

Let op als je twee cayleytabellen vergelijkt: hier stonden de overeenkomstige elementen op dezelfde plaats in de volgorde (0, 1, 2, 3 en I, r, r^2, r^3). Maar als de elementen van de tweede groep bv. als $r, r^2, r^3, r^4 = I$ in de tabel stonden, zou het

minder evident zijn om op de cayleytabellen het isomorfisme te zien. Indien nodig moet je eerst de volgorde van de elementen herschikken.

LESACTIVITEIT

Nog enkele isomorfe groepen

1 Ook Sym(▭), ∘, de symmetriegroep van een rechthoek, heeft vier elementen. Is die ook isomorf met $\mathbb{Z}_4, +$ en met Rot(□)?

✔ *Neen. Hier zie je de cayleytabel van Sym(▭), ∘. Beide groepen zijn commutatief. In de symmetriegroep van de rechthoek is elk element zijn eigen inverse (want I is op de diagonaal), wat niet geldt bij de andere. Dus: ook na herschikking zullen deze cayleytabellen nooit overeenkomen.*

∘	I	r	s	s'
I	I	r	s	s'
r	r	I	s'	s
s	s	s'	I	r
s'	s'	s	r	I

2 Neem de verzameling

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\right\}$$

met de matrixvermenigvuldiging. Maak de cayleytabel. Controleer dat dit een groep is. Met welke vorige groepen is deze groep wel of niet isomorf?

✔ *De leerlingen zullen vaststellen dat deze groep isomorf is met Sym(▭), ∘. Ter informatie: men kan bewijzen dat er op isomorfisme na maar twee verschillende groepen van vier elementen bestaan. We hebben ze hier allebei, telkens onder twee gedaanten, ontmoet.*

3 Zelfde vraag voor $\{1, -1, i, -i\}$ voor de vermenigvuldiging van complexe getallen.

✔ *Opnieuw een groep, isomorf met $\mathbb{Z}_4, +$. Om dit te zien, kunnen de leerlingen deze vier complexe getallen voor de cayleytabel in de volgorde $1, i, -1, -i$ zetten.*

4 Met welke groep is de symmetriegroep van de strook isomorf (zie vorige lesactiviteit)?

✔ *Met $\mathbb{Z}, +$. Elk element t^z van de symmetriegroep van de fries komt overeen met het geheel getal z, en er geldt $t^{z_2} \circ t^{z_1} = t^{z_1+z_2}$. Het samenstellen van deze verschuivingen komt algebraïsch op hetzelfde neer als het optellen van de exponenten bij de basisverschuiving t.*

Het feit dat een 'zelfde groep' ontmoet wordt in verschillende context, leidt tot het idee om een groep te bekijken als een abstracte structuur, waarbij het niet belangrijk is wat de elementen zijn of hoe de bewerking in zijn werk gaat.

Vooraf: als we zeggen dat $*$ een *bewerking* is in G, dan veronderstellen we hierbij dat $a * b$ bestaat en uniek is, voor elke a en b. Dit wordt in de definitie hieronder niet uitdrukkelijk vermeld, maar zit inbegrepen in het woord bewerking. (Voor wie vertrouwd is met de terminologie van verzamelingen en relaties: $*$ is een *afbeelding* van $G \times G$ naar G.)

Definitie • Abstracte groep

Een verzameling G voorzien van een bewerking $*$ vormt een groep als de volgende voorwaarden voldaan zijn:

$\forall a, b \in G : a * b \in G$

(G is gesloten voor $*$)

$\forall a, b, c \in G : (a * b) * c = a * (b * c)$

($*$ is associatief in G)

$\exists e \in G : \forall a \in G : e * a = a = a * e$

(* heeft een neutraal element in G)

$\forall a \in G : \exists a^{-1} \in G : a^{-1} * a = e = a * a^{-1}$

(elk element heeft een invers voor $*$ in G)

In plaats van 'G voorzien van de bewerking $*$' gebruiken we vaak de korte notatie $G,*$.

Merk op dat de commutativiteit er niet bij staat. Het samenstellen van symmetrieën van een figuur is trouwens in het algemeen niet commutatief. Er zijn commutatieve en niet-commutatieve groepen.

De associativiteit was bij het samenstellen van isometrieën evident en hoefde niet gecontroleerd te worden. Bij het modulorekenen was deze voorwaarde wel relevanter. Misschien vraag je je af of er niet-associatieve bewerkingen bestaan. Wel, neem bv. in $\mathbb{R}$ de bewerking $r * s = \frac{r+s}{2}$, het nemen van het rekenkundig gemiddelde van twee reële getallen. Als je $(1 * 3) * 8$ berekent, kom je 5 uit, maar $1 * (3 * 8) = 3{,}25$. (Je geeft minder 'gewicht' aan de getallen die tussen de haakjes staan...) Merk op: $1 * 3 * 8$ bestaat niet en is dus niet het gemiddelde van de drie getallen 1, 3, en 8. We hebben hier een bewerking ingevoerd voor twee getallen en omdat de associativiteit niet geldt, mag je de haakjes niet weglaten.

Bij groepen van transformaties had het neutraal element een vaste betekenis (de identieke) en hadden de inverse elementen ook een vaste betekenis (de inverse transformaties, die de beelden terugsturen naar hun originelen). Hier is dat niet meer zo, en moeten neutraal element en inversen 'bestaan' als elementen van de groep.

Het voordeel van abstracte groepen is dat je als het ware tegelijkertijd in gelijk welke groep werkt. In de volgende lesactiviteit bewijs je eigenschappen in een abstracte groep. Je weet niet wat de elementen voorstellen; het enige waar je gebruik van kunt maken, zijn de voorwaarden uit de definities. En wat je bewezen hebt, is meteen geldig in gelijk welke groep.

LESACTIVITEIT

Abstracte bewijsjes

1 Bewijs dat het neutraal element in een groep uniek is.

✓ *Veronderstel dat e en e' twee verschillende neutrale elementen zijn van de groep $G,*$. Dan is $e * e' = e$ omdat e' neutraal is. Maar ook $e * e' = e'$ omdat e neutraal is. Bijgevolg: $e=e'$, in tegenspraak met de veronderstelling. Dus kunnen er geen twee verschillende zijn.*

2 Bewijs dat in een groep $G,*$ elk element *juist* één invers heeft.

✓ *Veronderstel dat a' en a'' twee verschillende inversen zijn van $a \in G$. Dan:*

$$a' * a * a'' = a' * (a * a'') = a' * e = a'$$
$$a' * a * a'' = (a' * a) * a'' = e * a'' = a''$$

Bijgevolg: $a' = a''$.

3 Bewijs dat $(x * y)^{-1} = y^{-1} * x^{-1}$, voor alle $x, y \in G$. Waarom noemt men deze eigenschap de 'broek-onderbroek-eigenschap'?

✔ *We tonen aan dat $y^{-1} * x^{-1}$ inderdaad de inverse is van $x * y$:*

$$(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = y^{-1} * y = e$$

En analoog: $(x * y) * (y^{-1} * x^{-1}) = e$

De naam 'broek-onderbroek' voor deze eigenschap komt omdat net als bij het aan- en uitkleden de volgorde wordt omgekeerd: 's morgens (of op een ander moment) doe je eerst je onderbroek aan en dan je broek. Om dit ongedaan te maken doe je eerst je broek uit en dan je onderbroek. De situatie 'rok-onderbroek' komt overeen met commutatieve situaties in de wiskunde, daar maakt de volgorde niet uit.

4 Bewijs dat in een groep $G, *$ een vergelijking van de vorm $a * x = b$, met x als onbekende en $a, b \in G$, altijd juist één oplossing heeft.

✔ *Eerst: als die x bestaat, dan moet:*

$$a * x = b \Rightarrow a^{-1} * (a * x) = a^{-1} * b \Rightarrow (a^{-1} * a) * x = a^{-1} * b \Rightarrow e * x = a^{-1} * b \Rightarrow x = a^{-1} * b.$$

We controleren dat de gevonden x effectief een oplossing is:

$$a * (a^{-1} * b) = (a * a^{-1}) * b = b.$$

Als je het eerste deel van dit bewijs nog eens overloopt, kun je vaststellen dat we werkelijk alle voorwaarden voor een groep nodig hebben. Bij de eerste implicatie het feit dat een bewerking een uniek resultaat geeft. Dan de associativiteit. Dan het invers en ten slotte het neutraal element. Je kunt zeggen: een groep is de structuur waarin je zo'n vergelijking kunt oplossen.



In een tweede lesactiviteit onderzoeken de leerlingen voorbeelden en tegenvoorbeelden van groepen. Om aan te tonen dat het een groep is, moet je in principe alle voorwaarden nagaan, maar als je wilt bewijzen dat het geen groep is, is het genoeg de vinger te leggen op één voorwaarde die niet geldt.

LESACTIVITEIT

Een groep of geen groep, that's the question.

Is het een groep of niet? Leg uit waarom.

1 $\mathbb{N}, +$

✓ *Neen: de natuurlijke getallen verschillend van* 0 *hebben geen inverse voor* $+$ *binnen* $\mathbb{N}$. *Omdat* 0 *neutraal is, zouden de inversen in dit geval de tegengestelde getallen moeten zijn, maar die zitten niet in* $\mathbb{N}$.

2 $\mathbb{Z}, +$

✓ *Ja.*

3 $\mathbb{Z}, -$

✓ *Neen: de bewerking is niet associatief. Of nog (maar één reden volstaat): er is geen (tweezijdig) neutraal element.*

4 $\mathbb{Z}, \cdot$

✓ *Neen: behalve* 1 *en* -1 *hebben de gehele getallen geen inverse voor* $\cdot$ *binnen* $\mathbb{Z}$.

5 $\mathbb{Q}, +$

✓ *Ja.*

6 $\mathbb{Q}, \cdot$

✓ *Neen: het getal* 0 *heeft binnen* $\mathbb{Q}$ *geen inverse voor* $\cdot$.

7 $\mathbb{Q}_0, \cdot$

✓ *Ja.*

8 $\mathbb{R}^{2\times 2}, +$

✓ *Ja.*

9 $\mathbb{R}^{2\times 2}, \cdot$

✓ *Neen: er zijn ook niet-inverteerbare* 2×2*-matrices, bv.* $\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$.

10 De inverteerbare 2×2-matrices (van reële getallen) met de vermenigvuldiging

✓ *Ja. Merk op: eens je weet dat dit een groep is, gelden eigenschappen over inverteerbare matrices, zoals* $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$, *automatisch zonder dat je die nog met matrixberekening moet bewijzen.*

11 De spiegelingen die een gegeven lijnsymmetrische figuur op zichzelf afbeelden

✓ *Neen. Er is in deze verzameling geen neutraal element, want de identieke is geen spiegeling. Of nog: als je twee spiegelingen samenstelt, krijg je geen spiegeling; de verzameling is dus niet gesloten voor het samenstellen.*

12 De draaiingen die een gegeven begrensde vlakke figuur op zichzelf afbeelden, met de samenstelling

✔ *Ja.*

13 De draaiingen die een gegeven strookpatroon op zichzelf afbeelden

✔ *Tja, het hangt ervan af. Als de symmetriegroep van de fries enkel uit verschuivingen bestaat, dan is er één draaiing die de fries op zichzelf afbeeldt, namelijk de identieke. Dan is het antwoord ja, want de identieke vormt een (oninteressante) groep van één element. Maar als er andere draaiingen in zitten, dan zijn dat draaiingen over* 180°*, dus puntspiegelingen (zie Roelens en Schatteman, 2012). De samengestelde van twee verschillende puntspiegelingen is geen draaiing maar een verschuiving, en valt dus buiten deze verzameling. In dat geval is het antwoord dus neen omdat de verzameling niet gesloten is voor het samenstellen.*

14 $\mathbb{N}$ met als bewerking het nemen van het maximum

✔ $\mathbb{N}$ *is gesloten voor het maximum, de associativiteit geldt en* 0 *is neutraal. Maar behalve* 0 *heeft geen enkel element een invers. Geen groep dus.*

5 Symmetriegroepen van ruimtefiguren

Ook driedimensionale lichamen kunnen symmetrie vertonen. In de ruimte kun je spiegelen ten opzichte van een vlak, een rechte of een punt. Je hebt dan ook vlaksymmetrische, lijnsymmetrische en puntsymmetrische figuren. Er zijn ook draaisymmetrische figuren. Draaien gebeurt in de ruimte niet rond een punt maar rond een rechte. Een lijnspiegeling is hetzelfde als een draaiing over 180°.

Merk op dat het slechts zin heeft te spreken over wijzerzin of tegenwijzerzin als je de draaias hebt georiënteerd. Stel bv. dat je rond een verticale as draait: wijzerzin van boven uit gezien (draaias naar onder gericht) komt neer op tegenwijzerzin van onder uit gezien (draaias naar boven gericht). Daarom kun je in de ruimte geen 'oriëntatie' vastleggen door enkel te spreken over wijzer- of tegenwijzerzin, want dit hangt af hoe je ernaar kijkt. Een hand is wel geschikt om een oriëntatie in de ruimte te bepalen: er is een duim die aangeeft hoe je moet kijken (met de duim mee) en de (gekromde) vingers tonen een draaizin. Op die manier bepaalt de rechterhand ´wijzerzin' en de linkerhand ´tegenwijzerzin' (Figuur 11).



***Figuur 11** – Rechterhand*

Stelling • Classificatie symmetrieën van een begrensd lichaam

- Oriëntatie-behoudende → **draaiing** rond een georiënteerde rechte
  Speciale gevallen:
  - Draaihoek = 0° → **identieke**
  - Draaihoek = 180° → **lijnspiegeling**
- Oriëntatie-omkerende: **draaispiegeling** (draaiing gevolgd door vlakspiegeling om een vlak loodrecht op de draaias)
  Speciale gevallen:
  - Draaihoek = 0° → **vlakspiegeling**
  - Draaihoek = 180° → **puntspiegeling**

Een begrensde ruimtefiguur kan behalve vlaksymmetrisch, lijnsymmetrisch, puntsymmetrisch of draaisymmetrisch ook *draaispiegelsymmetrisch* zijn. Een *draaispiegeling* is de samengestelde van een draaiing en een vlakspiegeling waarbij de as van de draaiing loodrecht staat op het spiegelvlak. Een concreet voorbeeld komt in de lesactiviteit over de tetraëder, vraag 8. Vlakspiegelingen en puntspiegelingen zijn speciale gevallen van draaispiegelingen, met als draaihoek respectievelijk 0° en 180°.

Een vlakspiegeling verandert de oriëntatie: een linkerhand wordt afgebeeld op een rechterhand. Ook de draaispiegelingen doen dat (en dus ook de puntspiegelingen, anders dan in het vlak waar

de puntspiegelingen draaiingen zijn!). Draaiingen (en dus ook lijnspiegelingen) behouden de oriëntatie.

Men kan bewijzen (maar we doen het hier niet) dat er voor een begrensd lichaam geen andere mogelijkheden zijn. Dat is ver van evident.

Voor onbegrensde ruimtelichamen zijn nog andere symmetrieën mogelijk, verschuivingen en samengestelden van verschuivingen met draaiingen of met vlakspiegelingen, maar die hebben we hier niet nodig omdat we ons beperken tot begrensde lichamen.

Laten we oriëntatie-omkerende isometrieën kortweg *omkeringen* noemen, en oriëntatie-omkerende symmetrieën van een figuur kortweg *omkeersymmetrieën* van die figuur.

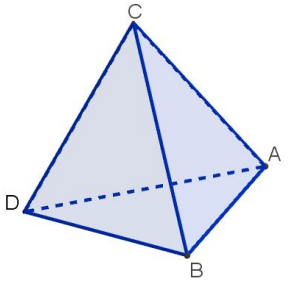
5.1 De symmetriegroep van een regelmatig viervlak

Voor deze lesactiviteit heb je per groepje een regelmatig viervlak nodig (in karton of polydron). Polydron kan door de school aangekocht worden maar is eigenlijk te duur om het als leraar persoonlijk aan te schaffen. Een regelmatig viervlak is natuurlijk snel in karton gemaakt. Voor ingewikkeldere veelvlakken kun je vlakke ontwikkelingen afdrukken van www.polyhedra.net/nl/.

LESACTIVITEIT

Symmetriegroep van een regelmatig viervlak

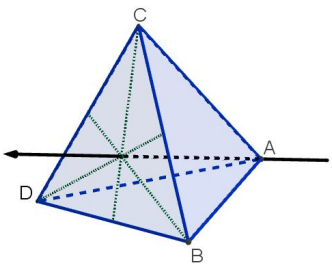
Je krijgt een regelmatig viervlak (tetraëder), dat je voor deze opgave kunt vastnemen en manipuleren.

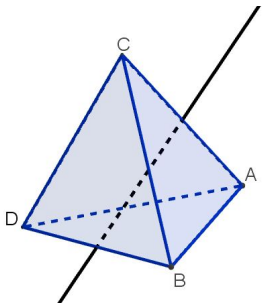


1 Bepaal alle draaisymmetrieassen van dit veelvlak.

✓ *Er zijn twee soorten draaisymmetrieassen. De eerste soort: telkens door een hoekpunt en het midden van het overstaande zijvlak. Hierrond kun je de tetraëder op zichzelf draaien over hoeken van* 120° *of* 240° *(of* −120°*, wat op hetzelfde neerkomt als* 240°*). Omdat er vier hoekpunten zijn, zijn er vier draaisymmetrieassen van deze soort.*

Er is nog een tweede soort: de verbindingslijnen tussen de middens van overstaande ribben. Hierrond kun je de tetraëder op zichzelf draaien over 180°*. Omdat er zes ribben zijn, zijn er drie paren van overstaande ribben en dus drie dergelijke draaisymmetrieassen.*



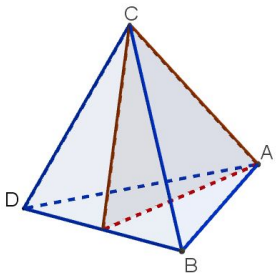


2 Een draaisymmetrieas kan overeenkomen met verschillende draaiingen die de figuur op zichzelf afbeelden, anders gezegd met verschillende draaisymmetrieën van de figuur. Hoeveel draaisymmetrieën heeft het regelmatig viervlak? (Tip: de identieke draaiing mag je maar één keer meetellen, want over 0° draaien rond de ene as of rond de andere as is hetzelfde: niets doen.)

✔ *Start met de identieke te tellen:* 1. *Voor elke as van de eerste soort zijn er twee draaiingen in de symmetriegroep, over* 120° *en over* 240°. *Dus:* $1+4\cdot 2$. *Voor elke as van de tweede soort is er één draaiing, over* 180°. *We vervolgen onze telling:* $1+4\cdot 2+3\cdot 1=12$. *De tetraëder heeft dus* 12 *draaisymmetrieën.*

3 Bepaal alle symmetrievlakken van het regelmatig viervlak. Hoeveel vlakspiegelingen zijn er in de symmetriegroep?

✔ *Elk symmetrievlak is bepaald door een ribbe en het midden van de overstaande ribbe. Omdat er zes ribben zijn, zijn er dus zes symmetrievlakken. Elk symmetrievlak komt overeen met* 1 *vlakspiegeling. Er zijn dus* 6 *vlakspiegelingen in de symmetriegroep.*



4 Denk je dat je alle symmetrieën van de tetraëder gevonden hebt?

✔ *Er zijn* 12 *draaiingen gevonden en* 6 *vlakspiegelingen, samen* 18 *symmetrieën. Er zijn nog* 6 *symmetrieën die niet ontdekt zijn. Dat zijn draaispiegelingen. Het is weinig waarschijnlijk dat de leerlingen die vinden door de tetraëder te manipuleren. Maar er zijn twee manieren waarop ze, met hulp van de leraar, kunnen achterhalen dat er nog* 6 *tekort zijn.*

Elke symmetrie van de tetraëder levert juist één permutatie van de hoekpunten A, B, C *en* D *op, want de hoekpunten moeten uiteraard op de hoekpunten afgebeeld worden. Ook omgekeerd: elke permutatie van de hoekpunten levert juist één symmetrie op. Dat komt omdat elk hoekpunt zich op dezelfde manier verhoudt tot elk ander hoekpunt. (Bij bv. een kubus is dat niet zo: een hoekpunt kan met een ander hoekpunt een ribbe vormen, of een zijvlaksdiagonaal, of een ruimtediagonaal.) Welnu: het aantal permutaties van* 4 *elementen is* $4! = 24$, *dat is* 6 *meer dan het aantal gevonden symmetrieën tot nu toe.*

Een andere redenering om te vinden dat er nog 6 *onontdekte symmetrieën zijn, gaat als volgt. Het regelmatig viervlak kan op* 12 *manieren op zichzelf gedraaid worden. Stel nu dat we het viervlak vlakspiegelen om één van zijn symmetrievlakken. Dat gespiegelde viervlak is natuurlijk juist even draaisymmetrisch als het niet-gespiegelde. Er zijn dus* 12 *draaiingen die het op zichzelf afbeelden. Dit levert* 12 *omkeersymmetrieën op, namelijk die vlakspiegeling gevolgd door één van de* 12 *draaiingen. Verderop wordt bewezen dat die* 12 *allemaal verschillend zijn en dat er geen andere omkeersymmetrieën zijn, met een redenering die volop thuis hoort in de groepentheorie.*

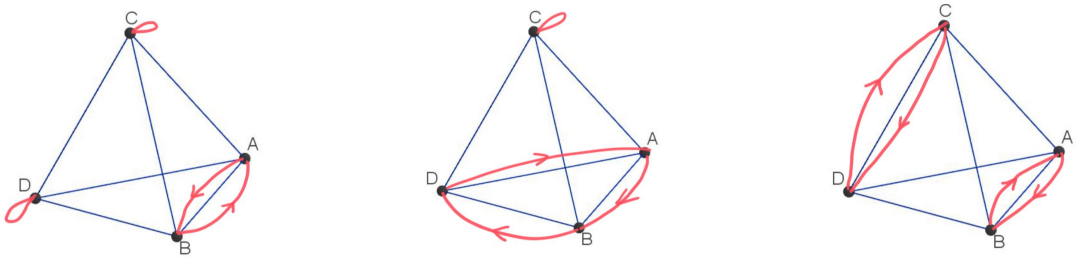
Laten we het hebben over de permutaties van de hoekpunten A, B, C en D.

We voeren enkele notaties in. Daarna zal het aan jou zijn om de 24 permutaties van de hoekpunten te associëren met de juiste symmetrieën van de tetraëder.

Een eerste notatie zijn we in het vlak al tegengekomen. Bv. de permutatie waarbij A en B met elkaar verwisseld worden en C en D op zichzelf afgebeeld worden, kunnen we noteren als

$$\begin{pmatrix} A & B & C & D \\ B & A & C & D \end{pmatrix}$$

Een nog kortere notatie is $(A\,B)$, want de permutatie verwisselt A en B. De punten die op zichzelf afgebeeld worden, noteren we niet. In deze notatie is $(A\,B) = (B\,A)$



Nog enkele voorbeelden

- $(A\,B\,D)$ is de draaiing die C op zichzelf afbeeldt, A afbeeldt op B, B op D en D op A. Men zegt dat $(A\,B\,D)$ een *cykel* is. Merk op dat $(A\,B\,D) = (B\,D\,A) = (D\,A\,B) \neq (D\,B\,A)$. We mogen de drie punten in deze notatie cyclisch permuteren, want de draaizin is belangrijk maar niet waar je begint.
- $(A\,B)(C\,D)$ is de permutatie die A met B verwisselt en C met D. Deze permutatie bestaat uit twee disjuncte cykels (disjunct omdat er geen punt is dat in meer dan één cykel terugkomt).

Men kan (vrij gemakkelijk) aantonen dat elke permutatie kan worden geschreven als een combinatie van disjuncte cykels. Men moet dan wel ook de lege cykel van 0 elementen toelaten, voor de identieke permutatie. Die noteert men als ( ).

5 Welke symmetrie van de tetraëder hoort bij $(A\,B)$?

✔ *De spiegeling om het vlak door DC en het midden van $[AB]$.*

6 Zelfde vraag voor $(A\,B\,D)$.

✔ *De draaiing over $-120°$ rond de as door C en het midden van het zijvlak ABD. De draaiing is in wijzerzin op voorwaarde dat je kijkt van C naar het midden van het overstaande zijvlak. Als je in de andere 'zin' kijkt, is het tegenwijzerzin en dus $+120°$.*

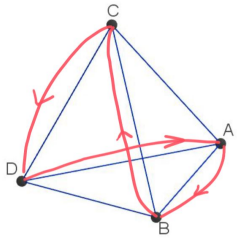
7 Zelfde vraag voor $(A\,B)(C\,D)$.

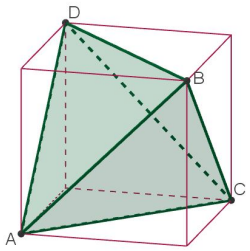
✔ *De lijnspiegeling (of: draaiing over $180°$) rond de as die de middens van $[AB]$ en $[CD]$ verbindt.*

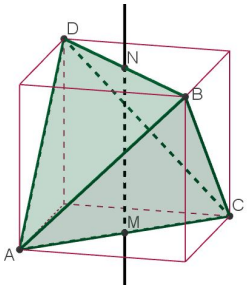
8 Welke 'soort' permutaties (in termen van cykels) hebben we nog niet gehad? Geef voor één voorbeeld van deze soort aan met welke symmetrie die overeenkomt.

✔ *We hebben nog geen cykels van lengte 4 ontmoet. Neem bv. $(A\,B\,C\,D)$. Het zal wel een draaispiegeling zijn, want dat is de overblijvende soort bij de mogelijke symmetrieën van een begrensde figuur zoals de tetraëder. Het is niet zo gemakkelijk om te 'zien' over welke draaiing gevolgd door welke vlakspiegeling het gaat.*

Om de leerlingen hierbij te helpen, kun je de tetraëder voorstellen in een kubus, bepaald door een diagonaal van het grondvlak en de 'andere' diagonaal van het bovenvlak.







Het antwoord is: eerst een draaiing rond de 'verticale' as door de middens M en N van de ribben $[AC]$ en $[BD]$, over 90° in tegenwijzerzin als je van boven naar beneden kijkt. Deze draaiing is geen symmetrie van de tetraëder. Het beeld is de andere tetraëder die je in de kubus kunt inschrijven. Na de draaiing ligt het beeld van B recht boven C, het beeld van D recht boven A, het beeld van A recht onder B en het beeld van C recht onder D. Nu kunnen de leerlingen wellicht zien dat er enkel nog moet worden gespiegeld ten opzichte van het 'horizontale' vlak op halve hoogte (anders gezegd: door de middens van de vier andere ribben van de tetraëder). De draaias en het spiegelvlak staan loodrecht op elkaar; we hebben wel degelijk een draaispiegeling.

De permutaties van vier elementen vormen een groep, genoteerd als $\mathscr{S}_4, \circ$, die isomorf is met de symmetriegroep van de tetraëder. Met elke permutatie van de vier hoekpunten komt juist één symmetrie van de tetraëder overeen en omgekeerd. Bovendien komt het op hetzelfde neer of je de permutaties samenstelt of de symmetrieën.

9 Vul in de onderstaande tabel alle permutaties van de hoekpunten van de tetraëder in. Gebruik de cykelnotatie.

Soort symmetrie	Permutaties van de hoekpunten
Identieke = draaiing over 0°	
Draaiingen over ±120°	
Lijnspiegelingen = draaiingen over 180°	
Vlakspiegelingen	
Draaispiegelingen	

✔ *Hier is de ingevulde tabel.*

Soort symmetrie	Permutaties van de hoekpunten
Identieke = draaiing over 0°	$()$
Draaiingen over ±120°	$(ABC), (ACB), (BCD), (BDC), (ACD), (ADC), (ABD), (ADB)$
Lijnspiegelingen = draaiingen over 180°	$(AB)(CD), (AC)(BD), (AD)(BC)$
Vlakspiegelingen	$(AB), (AC), (AD), (BC), (BD), (CD)$
Draaispiegelingen	$(ABCD), (ACBD), (ACDB), (BADC), (BCAD), (BDCA)$

Het meetkundig vinden van de draaiingen, gaat nog, maar het zien van alle omkeersymmetrieën is niet evident. Als het enkel gaat over het 'aantal' symmetrieën om te bepalen hoe symmetrisch het

ruimtelichaam is, dan is er een andere redenering mogelijk. Merk op dat het aantal omkeersymmetrieën van de tetraëder ook 12 is, net zoals het aantal draaiingen.

10 Zou dit altijd zo zijn? Waarom?

✔ *Het vlakgespiegelde (of puntgespiegelde of draaigespiegelde) lichaam is even draaisymmetrisch als het oorspronkelijke lichaam... (We verwachten hier geen nauwkeurig bewijs. Dat komt hieronder, buiten de lesactiviteit.)*

11 Bestaan er ook ruimtelichamen die geen enkele omkeersymmetrie hebben? Verfijn je antwoord op de vorige vraag, door een voorwaarde toe te voegen.

✔ *Jazeker. Bijvoorbeeld mijn rechterhand. Of een draaimolen voorzien van stoeltjes met leuningen (waarbij we geen rekening houden met de kleur van de stoeltjes). Een dergelijk voorwerp heeft wel draaiingen in de symmetriegroep: mijn hand heeft er één, de identieke; de molen kan op zichzelf gedraaid worden rond de centrale verticale as, over hoeken van veelvouden van 60°. Maar die hebben geen enkele omkeersymmetrie.*



Verfijning: als een ruimtelichaam minstens één omkeersymmetrie heeft, dan heeft het er evenveel als het aantal draaisymmetrieën.

5.2 Algemener

De draaisymmetrieën van een begrensd ruimtelichaam vormen altijd een deelgroep van de symmetriegroep van dat lichaam. Immers, als je twee keer na elkaar de oriëntatie bewaart, dan bewaar je de oriëntatie. En oriëntatie-bewarende symmetrieën van een begrensd lichaam zijn draaiingen. Bovendien: de identieke is een draaiing (over 0°) en de inverse van een draaiing is een draaiing.

In de vorige lesactiviteit kwam op het einde de stelling ter sprake over het aantal omkeersymmetrieën, als er zijn. We bewijzen deze stelling in het algemeen, niet enkel voor de tetraëder.

Stelling • Gegeven: een begrensde ruimtefiguur F met een eindig aantal draaisymmetrieën.

Als F minstens één omkeersymmetrie heeft, dan zijn er juist evenveel omkeersymmetrieën als draaisymmetrieën.

Bewijs •

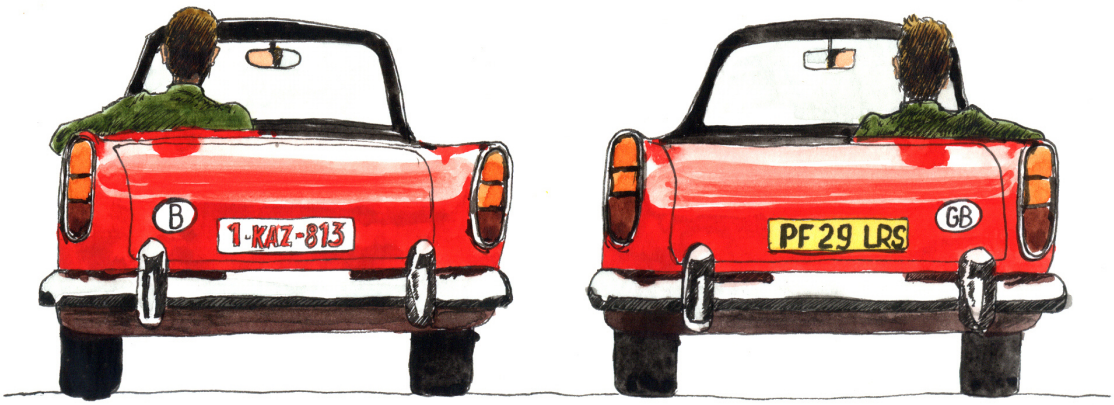
Veronderstel dat er juist n draaisymmetrieën $r_1, r_2, ...r_n$ van F zijn.

Gegeven is dat er een omkeersymmetrie is. Noem die i.

Dan zijn $r_1 \circ i, r_2 \circ i, ..., r_n \circ i$ omkeersymmetrieën van F. We bewijzen dat hier geen gelijke tussen zitten en dat er geen ontbreken. Als dat lukt, dan weten we dat er ook n zijn en is de stelling bewezen.

Veronderstel dat twee daarvan gelijk zijn, bv. $r_k \circ i = r_l \circ i$ met $k \neq l$. Door i te schrappen (we zitten in een groep) krijgen we $r_k = r_l$, tegenspraak.

Veronderstel dat we een omkeersymmetrie j vergeten zijn. Dan is $j \circ i^{-1}$ een symmetrie van F (we zitten in een groep...), die de oriëntatie behoudt, dus een draaiing. Dus bestaat er een $m \in \{1,...n\}$ zodat $j \circ i^{-1} = r_m$. Hieruit volgt $j = r_m \circ i$. Tegenspraak met de veronderstelling dat we die vergeten waren.



5.3 De symmetriegroep van een kubus en van een dodecaëder

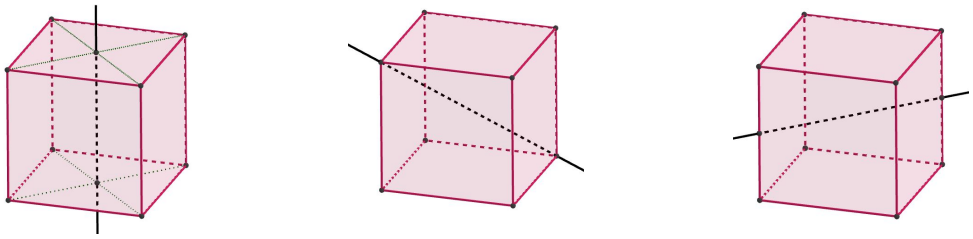
Zet de leerlingen nu aan het werk rond de symmetriegroep van de kubus. Door de vorige stelling weten ze dat ze enkel de draaiingen moeten tellen en dan met twee vermenigvuldigen.

LESACTIVITEIT

Symmetriegroep van een kubus

1 Bepaal alle draaisymmetrieën van de kubus.

✓ *Er zijn drie soorten draaisymmetrie-assen.*



- *Door de middens van twee overstaande zijvlakken (draaihoeken: veelvouden van 90°). Er zijn er 3 en als we de identieke vooraf tellen, tellen ze elk voor 3 draaiingen. Telling:* $1 + 3 \cdot 3$.
- *Door twee overstaande hoekpunten (draaihoeken: veelvouden van 120°). Er zijn er 4 en ze tellen elk voor 2 draaiingen. Vervolg telling:* $1 + 3 \cdot 3 + 4 \cdot 2$.
- *Door de middens van overstaande ribben (draaihoek: 180°). Er zijn er 6 en ze tellen elk voor 1. Vervolg telling:* $1 + 3 \cdot 3 + 4 \cdot 2 + 6 \cdot 1 = 24$.

2 Hoeveel symmetrieën heeft de kubus?

✓ *Er zijn 24 draaiingen in de symmetriegroep van de kubus. Bovendien is er minstens één omkeersymmetrie in deze symmetriegroep, bv. een vlakspiegeling, of de puntspiegeling ten opzichte*

van het middelpunt van de kubus. Door de vorige stelling mogen we dus besluiten dat er ook 24 *omkeersymmetrieën zijn. Totaal:* 48 *symmetrieën.*

3 Kun je het verband tussen het aantal symmetrieën van een kubus en van een tetraëder verklaren?

✔ *Je kunt twee tetraëders inschrijven in een kubus. De helft van de symmetrieën van de kubus bewaren deze tetraëders, de andere helft beelden deze tetraëders op elkaar af. We beschouwen deze korte, informele uitleg hier als voldoende.*

Merk op dat hier, in tegenstelling met de tetraëder, niet elke permutatie van de 8 hoekpunten overeenkomt met een symmetrie van de kubus. Twee buren (eindpunten van een zelfde ribbe) kunnen bv. door een isometrie bv. nooit afgebeeld worden op de twee uiteinden van een diagonaal. Er zijn dus heus geen 40320 symmetrieën van de kubus. De symmetriegroep van de kubus is zeker niet isomorf met $\mathscr{S}_8, \circ$.

Dan geef je de leerlingen een dodecaëder (regelmatig twaalfvlak). Hoeveel symmetrieën zijn er? Hoewel het mogelijk is om alle draaisymmetrieassen te vinden en hiermee het aantal draaiingen (en dan maal twee voor het aantal symmetrieën), is het probleem voldoende complex om een eenvoudigere manier te motiveren.

LESACTIVITEIT

Symmetriegroep van de dodecaëder

1 Mag je ook bij de dodecaëder het aantal draaiingen verdubbelen om het aantal symmetrieën te verkrijgen?

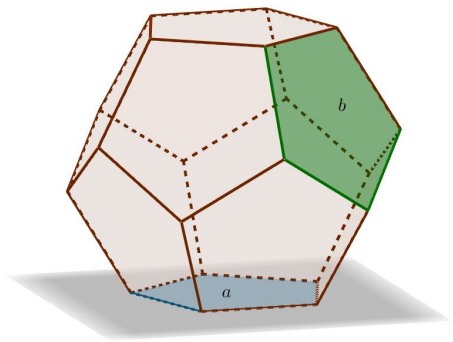
✔ *Ja, want er zijn vlakspiegelingen die de dodecaëder invariant laten. (Twee overstaande ribben bepalen telkens een symmetrievlak...) De dodecaëder is ook puntsymmetrisch. L'embarras du choix: er zijn zeker omkeersymmetrieën.*

Het aantal draaiingen tellen is hier een hele klus. Daarom gaan we op een slimme manier tellen, typisch voor groepentheorie.

Leg een zijvlak a op de tafel.

2 Hoeveel draaisymmetrieën van de dodecaëder zijn zo dat dit zijvlak op de tafel blijft liggen?

✔ *Er zijn er vijf, rond de centrale verticale as, over de veelvouden van* 72°. *Zowel de vijfhoek a op de tafel als de dodecaëder als geheel worden hierbij op zichzelf afgebeeld.*



3 Kies een ander zijvlak, bijvoorbeeld b. Hoeveel draaisymmetrieën van de dodecaëder brengen dit zijvlak naar het zijvlak a op de tafel?

✓ *Het is niet nodig om deze draaiingen concreet te zoeken om te weten hoeveel er zijn. Immers, er is er zeker één want de dodecaëder kan verplaatst worden zodat b op de tafel komt, en een verplaatsing is een oriëntatie-behoudende isometrie, dus een draaiing. Noem die ene draaiing r. Als je r samenstelt met de vijf draaiingen die het zijvlak op de tafel laten liggen, dan heb je er* 5.

4 Hoeveel draaisymmetrieën zijn er in totaal?

✓ *Wat voor zijvlak b geldt, geldt analoog voor elk ander zijvlak. Voor elk van de* 12 *(dodeca) zijvlakken zijn er dus vijf symmetrieën van de dodecaëder die ze naar de tafel brengen (of, in het geval van a, houden). Besluit: er zijn* $12 \cdot 5 = 60$ *draaisymmetrieën.*

5 Hoeveel elementen telt de symmetriegroep van de dodecaëder?

✓ *Twee keer* 60*, dus* 120*.*

6 Pas dit zelfde principe toe op de kubus om het aantal symmetrieën te vinden zonder alle draaisymmetrieassen te moeten zoeken.

✓ *Een zijvlak op de tafel:* 4 *draaiingen. Maal het aantal zijvlakken die naar de tafel gedraaid kunnen worden:* $6 \cdot 4 = 24$ *draaiingen. Maal* 2 *dus* 48 *symmetrieën. Als het enkel om het aantal gaat, is dit zeker gemakkelijker dan alle draaiingen concreet te omschrijven.*

5.4 Algemener

We veralgemenen de redenering met een zijvlak 'op de tafel' tot willekeurige veelvlakken. Bij deze wiskundige versie wordt niet meer over een tafel gesproken.

Stelling •

Als er bij een veelvlak F minstens één draaisymmetrie is die zijvlak b afbeeldt op zijvlak a, dan zijn er juist evenveel draaisymmetrieën die dit doen als draaisymmetrieën die zijvlak a op zichzelf afbeelden.

Bewijs •

Veronderstel dat er juist n draaisymmetrieën $r_1, r_2, ..., r_n$ zijn die a behouden.

Gegeven is dat er een draaisymmetrie is die b naar a brengt. Noem die r.

Dan zijn $r_1 \circ r, r_2 \circ r, ...r_n \circ r$ draaisymmetrieën van F die b naar a brengen. We bewijzen dat hier geen gelijke tussen zitten en dat er geen ontbreken. Als dat lukt, dan weten we dat er ook n zijn en is de stelling bewezen.

Veronderstel dat twee daarvan gelijk zijn, bv. $r_k \circ r = r_l \circ r$ met $k \neq l$. Door r te schrappen (we zitten in een groep) krijgen we $r_k = r_l$, tegenspraak.

Veronderstel dat we een draaisymmetrie s vergeten zijn. Dan is $s \circ r^{-1}$ een draaiing van F (we zitten in een groep...), die de a behoudt (a wordt eerst naar b gestuurd en terug naar a.) Dus bestaat er een $m \in \{1,...n\}$ zodat $s \circ r^{-1} = r_m$. Hieruit volgt $s = r_m \circ r$. Tegenspraak met de veronderstelling dat we die vergeten waren.

"Er zijn evenveel omkeersymmetrieën als draaisymmetrieën." en "Er zijn evenveel draaisymmetrieën die zijvlak b naar zijvlak a brengen, als draaisymmetrieën die a behouden." Deze stellingen hebben wiskundig hetzelfde patroon. Je ziet ook dat het bewijs helemaal op hetzelfde neerkomt. Hier zit een diepere, algemenere wiskundige waarheid achter. Als je iets 'behoudt' (de oriëntatie, een zijvlak, ...) dan heb je een deelgroep. Een deelgroep van een groep zorgt voor nevenklassen die allemaal evenveel elementen hebben als de deelgroep.

Je hebt telkens een deelgroep (de oriëntatie-behoudende; de 'zijvlak-a-behoudende'...) en je hebt nevenklassen (in het eerste geval één nevenklasse: de omkeersymmetrieën; in het tweede ge-

val evenveel nevenklassen als zijvlakken verschillend van a die door een draaisymmetrie de plaats van a kunnen innemen.) En de nevenklassen hebben evenveel elementen als de deelgroep.

Je kunt ook iets anders dan de oriëntatie of een zijvlak behouden. Neem bv. de kubus en begin met een ribbe: er zijn 2 draaiingen die deze ribben behouden. Maal 12, het aantal ribben dat je naar die ene ribbe kunt draaien, geeft 24 draaiingen, maal 2 geeft 48 symmetrieën. Of als je begint met een hoekpunt: 3, maal 8 geeft 24, maal 2 geeft 48. Je zou zelfs kunnen werken met de twee ingeschreven tetraëders: er zijn 12 draaisymmetrieën die deze tetraëders op zichzelf afbeelden, maal 2 geeft 24 draaiingen, maal 2 geeft 48 symmetrieën

Het is ook niet noodzakelijk om eerst de draaiingen te tellen en dan met 2 te vermenigvuldigen. In plaats van eerst met een deelgroep van de groep van de draaisymmetrieën te starten, kun je ook meteen een deelgroep van de symmetriegroep nemen. Bv. bij een kubus en beginnend met een zijvlak: er zijn 8 symmetrieën die dat zijvlak behouden (vier draaiingen en vier vlakspiegelingen). Maal 6 is meteen 48.

5.5 Nog algemener: de stelling van Lagrange in een abstracte groep

We verlaten de meetkunde en werken in een abstracte groep.

Definitie • Gegeven een groep $G,*$. Een *deelgroep* van G is een deelverzameling H die zelf een groep vormt voor dezelfde bewerking $*$.

Notatie: $H,* \subset G,*$.

De notatie is dezelfde als voor een deelverzameling maar met de bewerking erbij.

We hebben al heel wat voorbeelden ontmoet. We zetten er drie van op een rij.

- De draaisymmetrieën van een begrensde vlakke of ruimtelijke figuur F vormen een deelgroep van de symmetriegroep van F.

$$\text{Rot}(F),\circ \subset \text{Sym}(F),\circ$$

- De symmetrieën van een veelvlak die een bepaald zijvlak a invariant laten, vormen een deelgroep van de symmetriegroep van het veelvlak.
- In $\mathbb{Z}_{13} \setminus \{0\}$ vormen de elementen voortgebracht door 10 een deelgroep.

$$\langle 10\rangle,\cdot = \{1,10,9,12,3,4\},\cdot \subset \mathbb{Z}_{13} \setminus \{0\},\cdot$$

We definiëren nu wat nevenklassen zijn.

Definitie •

Gegeven een groep $G,*$ met hierin een deelgroep $H,*$. Voor elk element $a \in G$ definiëren we de *nevenklasse* $H * a$ als volgt:

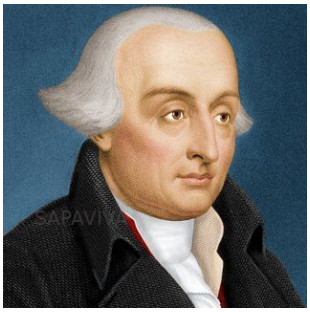
$$H * a = \{h * a | h \in H\}$$

De deelgroep H is zelf ook een nevenklasse want je kunt het element a in H kiezen. We geven bij de drie voorbeelden van deelgroepen hierboven telkens een voorbeeld van een nevenklasse.

- De omkeersymmetrieën van een begrensde figuur F vormen in de symmetriegroep van F de nevenklasse $\text{Rot}(F) \circ i$ (met i een omkeersymmetrie van F).
- De symmetrieën van een veelvlak die zijvlak b op zijvlak a afbeelden, vormen een nevenklasse in de symmetriegroep van het veelvlak.
- $\langle 10\rangle \cdot 2 = \{2,7,5,11,6,8\}$ is een nevenklasse in $\mathbb{Z}_{13} \setminus \{0\},\cdot$.

We bewijzen twee eigenschappen van nevenklassen vooraleer we de stelling van Lagrange bewijzen. We zullen deze twee eigenschappen nodig hebben om de stelling van Lagrange te bewijzen.

De eerste eigenschap betekent dat het niet uitmaakt welk element van de nevenklasse je neemt om de nevenklasse ermee te bepalen. De tweede eigenschap zegt dat nevenklassen elkaar niet overlappen.



Figuur 12 *– Joseph-Louis Lagrange, 18de eeuw, Franse wiskundige, natuurkundige en astronoom van Italiaanse afkomst*

De leerlingen kunnen deze eigenschappen interpreteren in de verschillende voorbeelden. Ze kunnen de tussenstappen van de bewijzen ook verantwoorden met de definitie van een abstracte groep.

Eigenschap • Gegeven $H,* \subset G,*$.

Voor elk element $a' \in H * a : H * a' = H * a$.

Bewijs •

Neem een willekeurig element van het linkerlid: $h * a'$, met $h \in H$. Omdat a' in $H * a$ zit, kan a' geschreven worden als $h' * a$ met $h' \in H$. Dus

$$h * a' = h * (h' * a) = (h * h') * a \in H * a.$$

Neem een willekeurig element van het rechterlid: $h * a$ met $h \in H$. Omdat $a' = h' * a$ met $h' \in H$ is $h'^{-1} * a' = a$ en $h'^{-1} \in H$ (want H is een deelgroep). Dus:

$$h * a = h * (h'^{-1} * a) = (h * h'^{-1}) * a' \in H * a'.$$

Hiermee is de eigenschap bewezen.

Eigenschap •

De doorsnede van twee nevenklassen is leeg.

Bewijs •

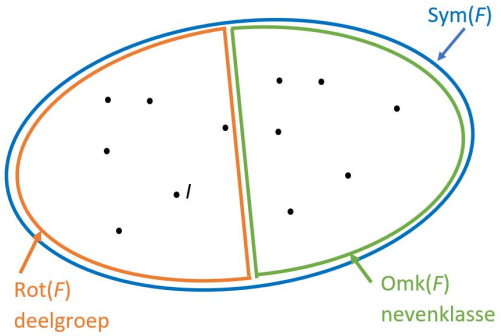
Neem twee verschillende nevenklassen $H * a$ en $H * b$.

Veronderstel dat x zowel in $H * a$ als in $H * b$ zit. Dan bestaan er elementen h en h' zo dat $x = h * a = h' * b$. Maar dan is $h'^{-1} * h * a = b$ waardoor b in $H * a$ zit. Uit de vorige eigenschap volgt dat de nevenklassen gelijk zijn. we hebben een tegenspraak en de eigenschap is bewezen.

De groep G wordt dus 'opgedeeld' in nevenklassen die elkaar niet overlappen (als we ook de deelgroep zelf als een nevenklasse bekijken). Men zegt dat de nevenklassen een 'partitie' van de groep vormen.

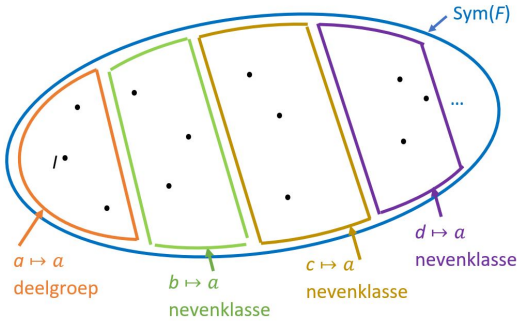
We passen dit weer toe op dezelfde voorbeelden.

- De symmetriegroep van een begrensde figuur is opgedeeld in de deelgroep van de draaiingen en de nevenklasse van de omkeersymmetrieën (Figuur 13).



Figuur 13 *– Partitie draaisymmetrieën en omkeersymmetrieën*

- De symmetriegroep van de dodecaëder is opgedeeld in de deelgroep van de symmetrieën die zijvlak a op zichzelf afbeelden, de nevenklasse van de symmetrieën die zijvlak b op zijvlak a afbeelden, de nevenklasse van de symmetrieën die zijvlak c op zichzelf afbeelden...(Figuur 14).



Figuur 14 *– Partitie welk zijvlak naar zijvlak a*

- $\mathbb{Z}_{13} \setminus \{0\}$ is opgedeeld in de deelgroep $\langle 10 \rangle = \{1, 10, 9, 12, 3, 4\}$ en de nevenklasse $\langle 10 \rangle \cdot 2 = \{2, 7, 5, 11, 6, 8\}$.

Stelling van Lagrange •

In een eindige groep $G,*$ geldt:

Elke nevenklasse van een deelgroep H heeft juist evenveel elementen als de deelgroep H.

Bewijs • Als $H = G$, is er niets te bewijzen. We veronderstellen dus dat er een element a bestaat dat in G zit maar niet in H.

Veronderstel dat er juist n elementen $h_1, h_2, \ldots h_n$ in H zijn.

Dan is het duidelijk dat $h_1 * a, h_2 * a, \ldots h_n * a$ alle elementen van $H * a$ zijn. We bewijzen dat er geen gelijke tussen zitten. Als dat lukt, dan weten we dat er in de nevenklasse $H * a$ ook juist n elementen zijn.

Veronderstel dat twee daarvan gelijk zijn, bv. $h_k * a = h_l * a$ met $k \neq l$. Door a te schrappen (we zitten in een groep) krijgen we $h_k = h_l$, tegenspraak.

Hiermee is de stelling bewezen.

Gevolg: het aantal elementen van de eindige groep is het product van het aantal elementen van de deelgroep en het aantal nevenklassen. Het is zo dat we het aantal symmetrieën van figuren slim telden.

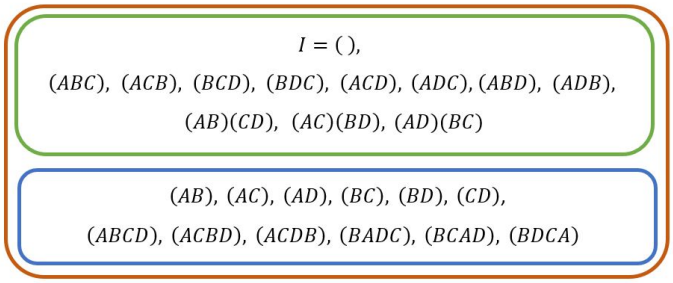
Nog een gevolg is dat het aantal elementen van een deelgroep van een eindige groep altijd een deler is van het aantal elementen van de groep.

Om te eindigen keren we terug naar de symmetriegroep van de tetraëder, of – wat op hetzelfde neerkomt want isomorf – de permutatiegroep van vier elementen $\mathscr{S}_4, \circ$. De leerlingen kennen deze groep al van een vorige activiteit; nu kunnen ze hiermee heel concreet de stelling van Lagrange illustreren.

LESACTIVITEIT

Deelgroepen en nevenklassen van $\mathscr{S}_4, \circ$

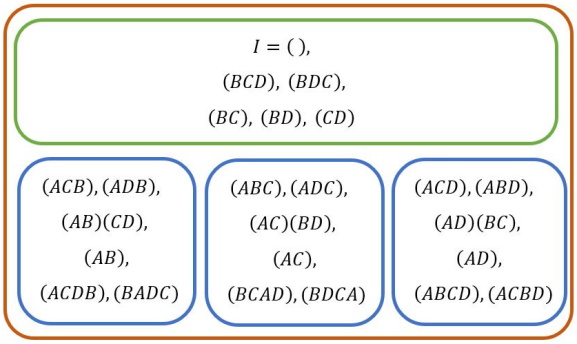
In een vorige lesactiviteit somde je alle symmetrieën van de tetraëder op, genoteerd als permutaties van de hoekpunten A, B, C, D (in cykelnotatie) en ingedeeld volgens soort transformatie. Hieronder zie je een venndiagram (of eerder een mengvorm tussen venndiagram en opsomming) van deze symmetriegroep, met de deelgroep van de draaisymmetrieën en (dus) de nevenklasse van de omkeersymmetrieën.



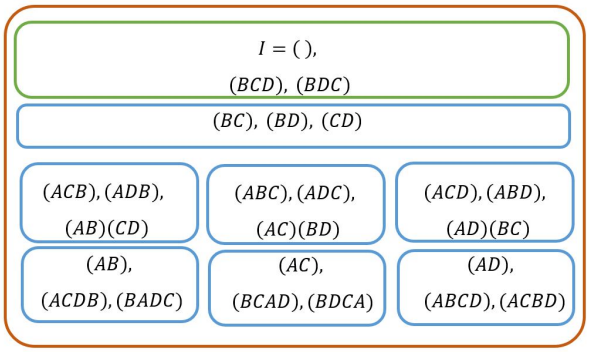
1 Kies een andere deelgroep dan die van de draaisymmetrieën en maak een venndiagram van de opdeling in deelgroep en nevenklassen.

✓ *We geven enkele mogelijke antwoorden.*

- *De leerlingen kunnen de deelgroep kiezen van de symmetrieën die een zijvlak, bv. BCD, invariant laten. De deelgroep heeft 6 elementen en er zijn 4 klassen (want vier zijvlakken of, volgens de stelling van Lagrange, $24 : 6 = 4$). Elke nevenklasse bestaat uit de symmetrieën die een bepaald ander zijvlak afbeelden op BCD. Het is handig om te beseffen dat bv. 'zijvlak ACD afbeelden op zijvlak BCD' op hetzelfde neerkomt als 'hoekpunt B afbeelden op hoekpunt A'.*



- *Ze kunnen de deelgroep kiezen van de draaisymmetrieën die een zijvlak BCD, invariant laten. Nu heeft de deelgroep 3 elementen en zijn er 8 klassen. Elke klasse van de vorige figuur is nu in twee helften verdeeld, de draaisymmetrieën en de omkeersymmetrieën van die klasse.*



- *Ze kunnen de deelgroep kiezen van de symmetrieën die een ribbe invariant laten. De deelgroep heeft 4 elementen en er zijn 6 klassen.* Enzovoort.

2 Controleer bij één van je nevenklassen dat je die inderdaad verkrijgt als $H \circ a$, met a een element van die klasse en H de deelgroep.

✔ *Het is mogelijk dat de leerlingen op deze manier de nevenklassen hebben bepaald. Maar als ze meetkundig hebben gewerkt, kan dit nog een interessante controle zijn. Bv. neem de nevenklasse van de symmetrieën die zijvlak ACD afbeelden op zijvlak BCD (of nog: die B afbeelden op A.*

We tonen aan dat deze nevenklasse verkregen wordt door alle elementen van de deelgroep H met één element van de nevenklasse, bv. (AB) samen te stellen.

$$\begin{aligned}
( ) \circ (AB) &= (AB) \\
(BCD)(AB) &= (ACDB) \\
(BDC)(AB) &= (BADC) \\
(BC)(AB) &= (ACB) \\
(BD)(AB) &= (ADB) \\
(CD)(AB) &= (AB)(CD).
\end{aligned}$$

De leerlingen kunnen meetkundig werken ofwel met de matrixnotatie voor opeenvolgende permutaties. Bv. voor $(BCD)(AB)$:

$$\begin{pmatrix} A & B & C & D \\ B & A & C & D \\ C & A & D & B \end{pmatrix}$$

Door de tweede rij (tussenstap) weg te laten, lezen zij het resultaat af: A naar C, B naar A, C naar D en D naar B.

BRONNEN

Brenton, L. (2008). Remainder wheels and group theory. *The College Mathematics Journal*. Vol.39, No.2, pp.129-135.

Buckinx, M. (2022). *Introductie van groepentheorie in de derde graad van doorstroomrichtingen in het Vlaamse secundair wiskundeonderwijs. De studie van symmetrieën.* Ongepubliceerd materiaal in het kader van een masterthesis aan de KU Leuven.

Conrad, K. (2005). *Why is group theory important?*, https://kconrad.math.uconn.edu/math216/whygroups.html

Deprez, J., Symens, S., Tytgat, P. (2008). Naar de abstracte algebra? *Uitwiskeling 24/3*.

Eggermont, H., Vanlommel, E. (2012). Priemgetallen. *Uitwiskeling 28/3*.

Gallian, J.A. (2017). *Contemporary Abstract Algebra*. Cengage Learning, Boston USA. ISBN 978-1-305-65796-0.

Muradian, R. (2011). *Modular Arithmetic Tables*. Wolfram Demonstrations Project, https://demonstrations.wolfram.com/ModularArithmeticTables/

Roelens, M. (2004). Symmetrische figuren. *Uitwiskeling 20/2.*

Roelens, M., Schatteman, A. (2012). Symmetrie. *Uitwiskeling 28/4.*

Roelens, M. (2015). Het rekenwonder. *Uitwiskeling 31/4*.

Sanderson, G. (2020). *Group theory, abstraction and the 196,883-dimensional monster.*, https://www.3blue1brown.com/lessons/groups-and-monsters

Vos, B. (2022). *Herintroductie van groepentheorie in het Vlaamse secundair wiskundeonderwijs. Interventieonderzoek gebaseerd op een algebraïsch perspectief*. Ongepubliceerd materiaal in het kader van een masterthesis aan de KU Leuven.