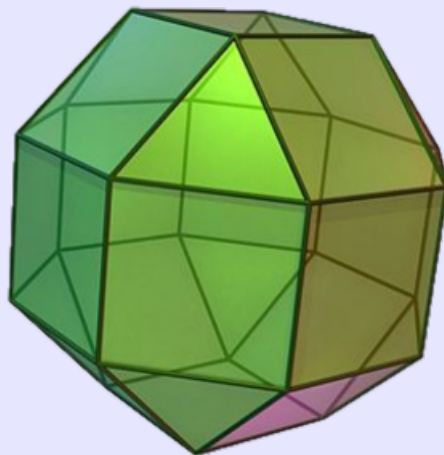


# Inleiding tot de groepentheorie

De studie van symmetrieën  
**Met oplossingen**



**Mathias Buckinx**  
2021-2022

# Inleiding

Je wiskundeleerkracht heeft misschien wel eens gezegd dat wiskunde overal aanwezig is en dit was zeker geen leugen! Denk bijvoorbeeld aan symmetrieën, die niet alleen door de mens gecreëerd zijn, maar zelfs in de onaangeraakte natuur voorkomen. Veel mensen vinden symmetrie mooi en rustgevend daarom is symmetrie bijvoorbeeld heel belangrijk in kunst. Wiskundigen zouden geen wiskundigen zijn als ze deze meetkundige fenomenen niet uitgebreid zouden bestuderen. Inderdaad, via groepentheorie worden symmetrieën bestudeerd in een abstracte, wiskundige context.



Symmetrie is niet alleen mooi, maar heeft ook praktische toepassingen. Dit zien we bijvoorbeeld in de sportwereld. Je weet misschien al dat voor ieder groot internationaal voetbaltornooi een nieuwe bal wordt ontworpen. Deze wordt dan over heel de wereld verkocht. Men moet dus een bal ontwerpen die snel en goedkoop te maken is. De bal bestaat uit verschillende lapjes geometrische figuren. Het is natuurlijk belangrijk dat een opgeblazen bal bolvormig is en dus op iedere plaats er ongeveer hetzelfde uit ziet. Daarom moet de bal zo symmetrisch mogelijk zijn.



De klassieke voetbal ontworpen door Adidas in 1970 bestaat uit vijf- en zeshoeken. <sup>1</sup>



2

Zo is bijvoorbeeld de bal, Uniforia, die gebruikt werd in het Europees kampioenschap van 2020 gebaseerd op een **romboëdrische kuboctaëder**. Deze complexe figuur heeft 26 vlakken waarvan acht gelijkzijdige driehoeken en 18 vierkanten. Ze heeft 24 hoekpunten en 48 ribben. Op het einde van deze lessenreeks kan je precies het aantal symmetrieën van deze figuur berekenen. Via groepentheorie kunnen we dus de verschillende ballen ontworpen voor verschillende internationale toernooien exact vergelijken met elkaar en met de klassieke voetbal.

<sup>1</sup>[https://commons.wikimedia.org/wiki/File:Comparison\\_of\\_truncated\\_icosahedron\\_and\\_soccer\\_ball.png](https://commons.wikimedia.org/wiki/File:Comparison_of_truncated_icosahedron_and_soccer_ball.png)

<sup>2</sup><https://commons.wikimedia.org/wiki/File:Rhombicuboctahedron.jpg>

Deze lessenreeks is een inleiding tot de abstracte algebra. Hierin bestuderen we wiskundige structuren. Dit zijn verzamelingen waarop bepaalde bewerkingen zijn gedefinieerd. Je kent vast en zeker al een wiskundige structuur, namelijk vectorruimten. Misschien komt de naam je niet bekend voor, maar toch werk je iedere dag met zo een structuur. De verzameling van de reële getallen ( $\mathbb{R}$ ) en van de complexe getallen ( $\mathbb{C}$ ) samen met de optelling en de vermenigvuldiging zijn voorbeelden van vectorruimten. Een vectorruimte is dus letterlijk een verzameling van vectoren.

In deze bundel zullen we niet spreken over vectorruimten, maar over een andere wiskundige structuur, groepen. Dit zijn verzamelingen waarop een bewerking is gedefinieerd die speciale regels volgt. Groepentheorie wordt ook wel 'de studie van symmetrieën' genoemd. Via groepen kunnen we de meetkundige eigenschappen van symmetrieën van een meetkundig object omzetten naar regels binnen de abstracte wiskunde. Dit laatste is precies wat er in bod zal komen in deze lessenreeks.

In deze lessenreeks ben jij zelf de leerkracht! De bundel is opgebouwd op een manier waarbij je zelf de leerstof ontdekt met behulp van invuloefeningen en voorbeelden. Je gaat op zoek naar de rekenregels en definities van de belangrijkste begrippen binnen de groepentheorie. Veel puzzelplezier!

# Inhoudsopgave

<b>Inleiding</b> . . . . .	i
<b>1 Het begrip groep</b> . . . . .	1
1.1 De definitie van een groep . . . . .	1
1.2 Orde van een groep . . . . .	13
1.3 Eigenschappen van groepen . . . . .	14
1.4 Oefeningen . . . . .	15
<b>2 Voorbeelden van groepen</b> . . . . .	20
2.1 Symmetriegroepen . . . . .	20
2.2 Permutatiegroepen . . . . .	21
2.3 Oefeningen . . . . .	28
<b>3 Deelgroepen en de stelling van Lagrange</b> . . . . .	30
3.1 De regelmatige tetraëder . . . . .	30
3.2 Het deelgroepcriterium . . . . .	37
3.3 De stelling van Lagrange . . . . .	40
3.4 Oefeningen . . . . .	44

# 1 | Het begrip groep

## 1.1 De definitie van een groep

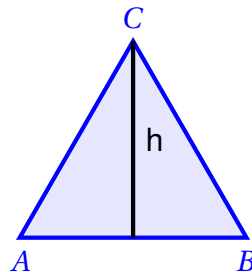
In dit hoofdstuk stellen we een definitie op voor het begrip groep.

### 1.1.1 Symmetrieën

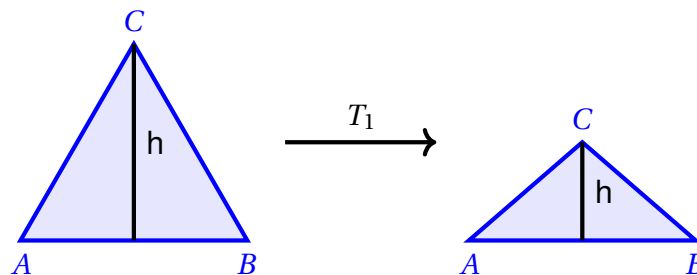
Groepentheorie wordt ook wel de studie van symmetrieën genoemd. We beginnen dus met een korte herhaling van het begrip symmetrie.

Transformaties van figuren, zoals symmetrieën, ken je al vanuit de lagere school. Een **transformatie** uitvoeren op een meetkundige figuur betekent dat we de figuur op een bepaalde manier veranderen. De vervormde figuur noemen we de **beeldfiguur**.

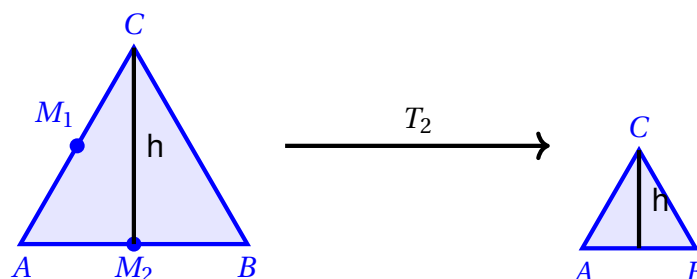
Onderstaande afbeelding geeft een gelijkzijdige driehoek weer met hoekpunten  $A, B$  en  $C$  en hoogtelijn  $h$ .



Transformatie  $T_1$  drukt de figuur samen zodat de lengte van de hoogtelijn ( $h$ ) gehalveerd is. Hiernaast zie je de beeldfiguur na deze transformatie. De vorm is duidelijk veranderd.

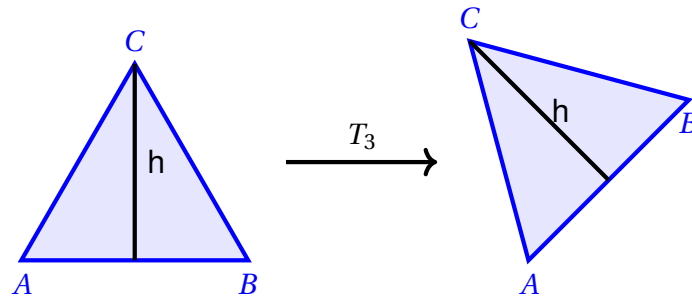


Transformatie  $T_2$  beeldt hoekpunt  $A$  af op zichzelf, maar hoekpunten  $C$  en  $B$  op respectievelijk  $M_1$  en  $M_2$  de middens van de zijdes  $AC$  en  $BC$ . We halveren dus de zijdes van de driehoek. Deze transformatie verandert de vorm van de driehoek niet, maar enkel de afstanden tussen punten op de driehoek. De beeldfiguur van deze transformatie is **gelijkvormig** met de oorspronkelijke driehoek.



Transformatie  $T_3$  roteert de driehoek met  $45^\circ$ . We zien hier weer dat de transformatie de vorm van de beeldfiguur niet verandert, maar in tegenstelling tot de vorige transformatie blijven de afstanden ook bewaard.

De beeldfiguur is **congruent** met de oorspronkelijke driehoek. Een transformatie die afstanden bewaart, noemen we een **isometrie**.



Nu we wat meer weten over transformaties, kunnen we ook nadenken over symmetrieën. In de afbeelding hiernaast zijn de drie verschillende symmetrieassen aangeduid. De figuur spiegelen over één van deze assen is een voorbeeld van een transformatie.

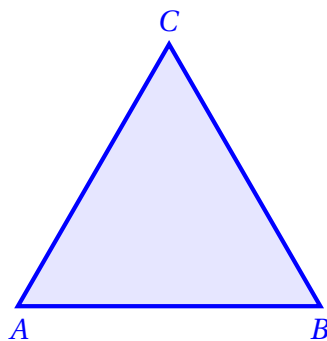
In dit geval spreken we van een **symmetrie**, want de beeldfiguur valt perfect samen met de oorspronkelijke figuur.

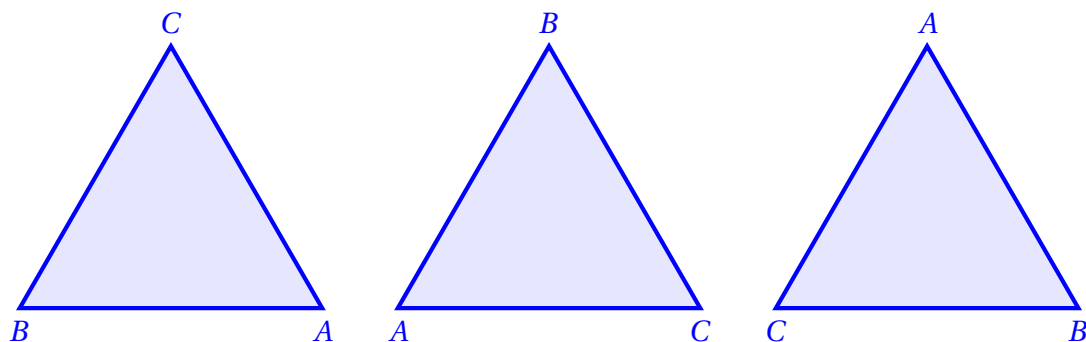


Een **symmetrie** van een figuur is een transformatie die **afstanden behoudt** en de figuur **op zichzelf afbeeldt**.

In deze paragraaf zullen we dieper ingaan op de symmetrieën van een gelijkzijdige driehoek.

- I** Beschrijf nauwkeurig welke symmetrieën je moet uitvoeren op gelijkzijdige driehoek  $ABC$  om onderstaande beeldfiguren te krijgen.

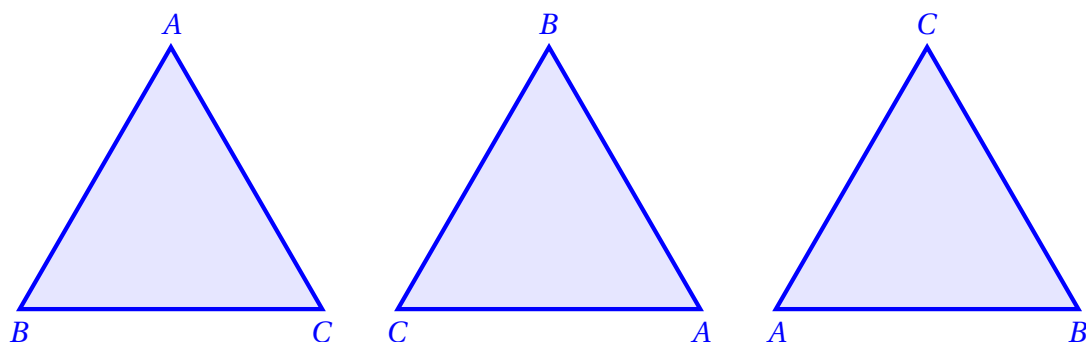




Driehoek  $BAC$  is de beeldfiguur van een spiegeling over de hoogtelijn uit  $C$ .

Driehoek  $ACB$  is de beeldfiguur van een spiegeling over de hoogtelijn uit  $A$ .

Driehoek  $CBA$  is de beeldfiguur van een spiegeling over de hoogtelijn uit  $B$ .



Driehoek  $BCA$  is de beeldfiguur van een rotatie over  $120^\circ$  in wijzerzin.

Driehoek  $CAB$  is de beeldfiguur van een rotatie over  $240^\circ$  in wijzerzin.

Driehoek  $ABC$  is de beeldfiguur van de transformatie die helemaal niets verandert.

Een gelijkzijdige driehoek heeft dus 6 symmetrieën.

— 1

De verzameling die alle symmetrieën van de gelijkzijdige driehoek bevat, noemen we  $G$ . De verzameling  $G$  bestaat dus uit 6 elementen.

### 1.1.2 Combinaties van symmetrieën

We kunnen transformaties combineren door ze na elkaar uit te voeren.

Bijvoorbeeld, de combinatie van  $T_1$  met  $T_2$  is de transformatie die je krijgt door *eerst transformatie  $T_1$  en daarna transformatie  $T_2$  uit te voeren*.

De combinatie van twee symmetrieën is opnieuw een symmetrie, want de driehoek twee keer transformeren naar zichzelf na elkaar is ook een transformatie van de driehoek naar zichzelf.

In de vorige oefening hebben we **alle** 6 symmetrieën van de driehoek al opgesomd. **Twee symmetrieën combineren geeft dus opnieuw één van deze 6 symmetrieën.**

- 2 Schrap wat niet past in volgende uitspraken over symmetrieën van de gelijkzijdige driehoek. Probeer zelf enkele combinaties van symmetrieën van een gelijkzijdige driehoek uit. Gebruik oefening 1.

- De combinatie van twee rotaties is **altijd** een rotatie.

Wanneer we eerst een rotatie over  $x$  graden uitvoeren en daarna een rotatie over  $y$  graden. Dan hebben we in totaal geroteerd over  $x + y$  graden. De combinatie is dus **altijd een rotatie**.

- De combinatie van twee spiegelingen is **nooit** een spiegeling.

Als we twee keer spiegelen om dezelfde as, dan voeren we de identieke transformatie uit. Als we na een spiegeling, een tweede spiegeling uitvoeren, dan bekomen we **altijd een rotatie**. Probeer dit!

- De combinatie van een spiegeling met een rotatie is **nooit** een rotatie.

Als we eerst de driehoek over een bepaalde spiegelas spiegelen en daarna roteren hebben we eigenlijk een spiegeling uitgevoerd over één van de andere twee assen. — 2

We gebruiken het symbool 'o' wanneer we de bewerking uitvoeren om symmetrieën te combineren.

Herinner je dat als  $f(x)$  en  $g(x)$  functies zijn, dan is  $f \circ g = f(g(x))$ . We voeren dus functie  $f$  uit **na** functie  $g$ .



Als  $T_2$  en  $T_1$  transformaties zijn, betekent  $T_2 \circ T_1$  dus dat we transformatie  $T_2$  **na** transformatie  $T_1$  uitvoeren.

We gebruiken vaak de volgende notatie:

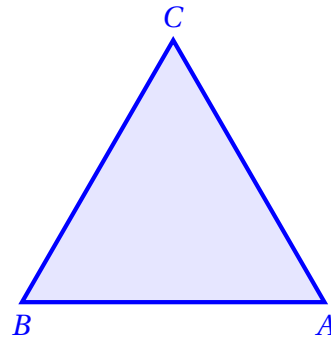
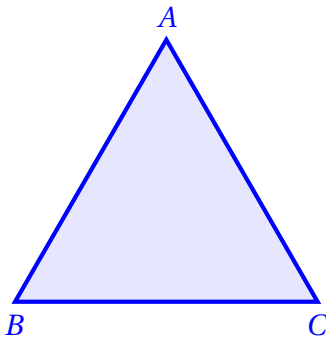
- $T_2 \circ T_1 = T_2 T_1$
- $T_1 \circ T_1 = T_1^2$

### 1.1.3 Algebraïsche voorstelling van symmetrieën van de gelijkzijdige driehoek

In deze paragraaf zullen we de symmetrieën van de driehoek algebraïsch voorstellen. Dit wil zeggen dat we aan iedere symmetrie een symbool toekennen en hiermee kunnen rekenen. Als we de symbolen en de (reken)regels hiertussen goed begrijpen moeten we niet telkens opnieuw teruggrijpen naar de visuele voorstelling van de symmetrieën van de driehoek.

Uit oefening 1 en 2 herkennen we twee soorten symmetrieën. We kiezen van beide soorten één symmetrie en ken aan deze de symbolen **R** en **S** toe.

Onderstaande driehoeken zijn de beeldfiguren van de gekozen symmetrieën. Kijk eens terug naar oefening 1 en schrijf de juiste symmetrie bij de gekozen driehoeken.



De rotatie over  $120^\circ$  (in wijzerzin) (**R**)    De spiegeling over de verticale hoogtelijn (**S**)

Binnenkort zullen alle symmetrieën van de regelmatige driehoek een algebraïsche voorstelling krijgen.  $R$  en  $S$  zijn voorstellingen van specifieke symmetrieën.

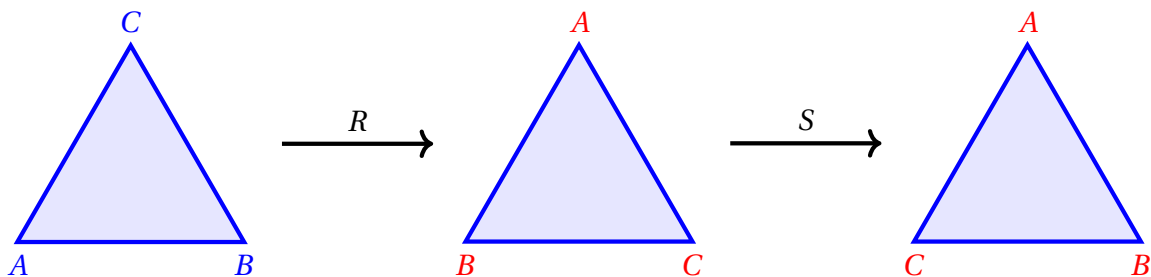
Natuurlijk is 'niets doen' ook een symmetrie, want als we niets doen transformeren we de driehoek ook naar zichzelf.



We kennen het symbool 'e' toe aan de transformatie die helemaal niets aan de driehoek verandert. We noemen deze symmetrie de **identieke transformatie**.

3

We hebben in de vorige paragraaf gezien dat de combinatie van symmetrieën van de driehoek opnieuw een symmetrie van de driehoek zal zijn. Probeer  $S \circ R$  te berekenen. De combinatie van **S na R** staat voorgesteld via de beeldfiguren van deze symmetrieën. Vul de hoekpunten van de beeldfiguren correct aan.



Welke symmetrie (in woorden) is de combinatie  $S \circ R$ ? **De spiegeling over de hoogtelijn uit B.**

We geven deze symmetrie van de gelijkzijdige driehoek dus het symbool  $S \circ R$  of  $SR$ . Probeer in de tabel alle 6 symmetrieën voor te stellen als combinaties van  $R$  en  $S$ .

Schrijf alle 6 symmetrieën van de driehoek (uit oefening 1) in woorden in kolom 1. Schrijf in kolom 2 de transformaties uit kolom 1 algebraïsch, dus in symbolen als combinaties van  $R$  en  $S$ .

Transformatie	Algebraïsch
niets doen	$e$
rotatie over $120^\circ$	$R$
rotatie over $240^\circ$	$R^2$
spiegeling over de verticale hoogtelijn (uit $C$ )	$S$
spiegeling over de hoogtelijn uit $A$	$RS$ (of $SR^2$ )
spiegeling over de hoogtelijn uit $B$	$SR$ (of $R^2S$ )

— 3

4 Vul onderstaande tabel verder aan:

- In de eerste rij schrijf je de symmetrieën uit de tabel van oefening 3 in symbolen.
- In de eerste kolom doe je hetzelfde.
- Combineer nu de symmetrieën, schrijf in iedere cel de symmetrie die je krijgt als je de transformatie uit de corresponderende kolom uitvoert **na** de transformatie uit de corresponderende rij.
- Denk eraan dat de combinatie van symmetrieën opnieuw een symmetrie van de driehoek is. Je moet dus opnieuw één van de 6 symbolen uit oefening 3 invullen.

$\circ$	$e$	$R$	$R^2$	$S$	$RS$	$SR$
$e$	$e$	$R$	$R^2$	$S$	$RS$	$SR$
$R$	$R$	$R^2$	$e$	$RS$	$SR$	$S$
$R^2$	$R^2$	$e$	$R$	$SR$	$S$	$RS$
$S$	$S$	$SR$	$RS$	$e$	$R^2$	$R$
$RS$	$RS$	$S$	$SR$	$R$	$e$	$R^2$
$SR$	$SR$	$RS$	$S$	$R^2$	$R$	$e$

Vul de rekenregels voor de  $\circ$ -bewerking aan.

Voor alle transformaties ( $X$ ), geldt  $e \circ X = X \circ e = X$

$R \circ R \circ R = R^3 = e$  en  $S \circ S = S^2 = e$

\* $S \circ R = SR = \dots \circ S$   $SR = R^2 S$  en  $R \circ S = RS = S \circ \dots$   $RS = SR^2$

We merken dat ieder element maar één keer voorkomt in iedere rij en kolom. — 4

5 In deze oefeningen ontdekken we enkele eigenschappen van verzameling  $G$ .

- Zijn volgende uitspraken waar of niet waar voor de verzameling  $G$  (schrap wat niet past).
- Beargumenteer je antwoord door gebruik te maken van de tabel uit oefening 4.

1) Er zijn precies vier symmetrieën  $X$  waarvoor geldt dat  $X \circ X = e$ . **Waar.**

In de tabel zien we dat  $e \circ e = S \circ S = RS \circ RS = SR \circ SR = e$ .

2) Er zijn precies vier symmetrieën  $X$  waarvoor geldt  $X \circ X \circ X = e$ . **Niet waar.**

Dit vereist wat rekenwerk, maar we zien dat enkel  $e \circ e \circ e = e$ ,  $R \circ R \circ R = e$ ,  $R^2 \circ \underbrace{R^2 \circ R^2}_{=R} = R^2 \circ R = e$ . Voor spiegelingen ( $S, SR$  en  $RS$ ) geldt dit niet. Bijvoorbeeld  $RS \circ \underbrace{RS \circ RS}_{=e} = RS \circ e = RS$ .

3) Het combineren van symmetrieën is commutatief. **Niet waar.**

Bijvoorbeeld  $RS \circ S = R$ , maar  $S \circ RS = R^2$ . Dit betekent dat  $RS \circ S \neq S \circ RS$ .

4) Het combineren van symmetrieën is associatief. **Waar.**

Inderdaad, het combineren van symmetrieën is een associatieve operatie. We kunnen transformaties ook voorstellen als functies en we weten dat de compositie van functies associatief is. Als  $f, g$  en  $h$  functies zijn van de driehoek naar driehoek, dan is  $(h \circ (f \circ g))(x) = h((g \circ f)(x)) = h(g(f(x)))$  en  $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$ .

5) Voor iedere symmetrie  $X_1$  bestaat er een tweede symmetrie  $X_2$  zodat  $X_2 \circ X_1 = e$ . **Waar.**

Dit zien we in de tabel. In de kolom van een willekeurige symmetrie  $X_1$  staan de combinaties van alle symmetrieën met deze  $X_1$ . In iedere kolom komt symmetrie  $e$  voor, dus de combinatie van de symmetrie van de juiste rij met  $X_1$  geeft  $X_2 \circ X_1 = e$ . — 5

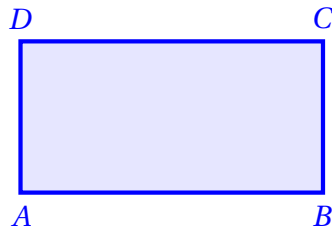
### 1.1.4 De symmetrieën van een rechthoek

In deze paragraaf bekijken we een nieuwe verzameling  $H$ , die alle symmetrieën van een rechthoek bevat. We onderzoeken de verschillen en gelijkenissen met de verzameling  $G$  uit de vorige paragrafen.

- 6 Beschrijf alle symmetrieën van onderstaande rechthoek nauwkeurig en ken aan ze allemaal een ander symbool toe (bv:  $a, b, c, \dots$ ).

Tip: Vergeet de identieke transformatie niet!

Hoeveel symmetrieën zijn er? 4.



- de identieke transformatie ( $e$ )
- een spiegeling over de rechte door het midden van zijde  $AB$  en zijde  $CD$  ( $a$ )
- een spiegeling over de rechte door het midden van zijde  $AD$  en zijde  $BC$  ( $b$ )
- een rotatie over  $180^\circ$  ( $c$ )

Combineer de symmetrieën volgens de  $\circ$ -bewerking uit de vorige oefeningen. Je hebt misschien niet de volledige tabel nodig!

$\circ$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

- 7 In deze oefeningen ontdekken we enkele eigenschappen van verzameling  $H$ .
- Zijn volgende uitspraken waar of niet waar voor de verzameling  $H$  (schrap wat niet past). Beargumenteer je antwoord met combinaties uit oefening 6.
  - Welke stellingen gelden voor alle groepen denk je? Duid deze aan!

1) Er zijn precies vier symmetrieën  $X$  waarvoor geldt dat  $X \circ X = e$ . **Waar.**

In de tabel zien we dat een symmetrie combineren met zichzelf altijd de identieke transformatie is:  $a \circ a = b \circ b = c \circ c = e \circ e = e$ .

2) Er zijn precies vier symmetrieën  $X$  waarvoor geldt  $X \circ X \circ X = e$ . **Niet waar.**

Enkel  $X = e$  voldoet hieraan, want  $e \circ e \circ e = e$ .

Er bestaat geen enkele andere symmetrie die hieraan voldoet, want  $X \circ X$  is altijd gelijk aan  $e$  en dus is  $X \circ X \circ X$  altijd gelijk aan  $X$ .

3) Het combineren van symmetrieën is commutatief. **Waar.**

In de tabel kunnen we zien dat  $X_1 \circ X_2 = X_2 \circ X_1$  altijd waar is. Bijvoorbeeld  $a \circ b = b \circ a = c$ .

4) Het combineren van symmetrieën is associatief. **Waar.**

Inderdaad, het combineren van symmetrieën is een associatieve operatie. We kunnen transformaties ook voorstellen als functies en we weten dat de compositie van functies associatief is. Als  $f, g$  en  $h$  functies zijn van de rechthoek naar de rechthoek, dan is  $(h \circ (f \circ g))(x) = h((g \circ f)(x)) = h(g(f(x)))$  en  $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$ .

5) Voor iedere symmetrie  $X_1$  bestaat er een tweede symmetrie  $X_2$  zo dat  $X_2 \circ X_1 = e$ . **Waar.**

Dit zien we in de tabel. In de kolom van  $X_1$  staan de combinaties van alle symmetrieën met  $X_1$ . In iedere kolom komt symmetrie  $e$  voor, dus de combinatie van de symmetrie van de juiste rij met  $X_1$  geeft  $X_2 \circ X_1 = e$ .

### 1.1.5 De definitie van een groep

De verzamelingen  $G$  en  $H$  die alle symmetrieën bevatten van een meetkundige figuur samen met de bewerking  $\circ$  zijn voorbeelden van **groepen**.

Groepen zijn wiskundige structuren die we noteren als  $(G, \circ)$  en  $(H, \circ)$ .

De identieke transformatie (het element 'e') noemen we het **identiteitselement** van deze verzamelingen.



We noemen een tabel waarin de bewerkingen tussen de elementen van een eindige groep weergegeven staan, de **Cayleytabel** van de groep. Ieder element van de groep komt exact één keer voor in iedere kolom en rij van de tabel.

Uit de Cayleytabel van een groep kunnen we meteen belangrijke eigenschappen van de groep zien zoals het identiteitselement en of de groep commutatief is.

8 Met behulp van de vorige oefeningen kan je nu zelf de basisregels heruitvinden.

- Welke basisregels gelden voor alle groepen denk je?  
Kijk bijvoorbeeld ook eens naar de uitspraken uit oefeningen 5 en 7.
- Hoe komen ze voor in onze groepen  $G$  en  $H$ .  
Om je te helpen, geven we in regels 1 en 3 zelf het antwoord op deze vraag.
- Beschrijf deze eigenschappen voor een willekeurige groep met bewerking  $\circ$ .

#### Basisregel 1: *Geslotenheid:*

De combinatie van twee symmetrieën die een figuur op zichzelf afbeelden is opnieuw een **symmetrie** van die figuur.

Als  $S_1$  en  $S_2$  elementen zijn van verzameling  $G$ , dan is  $S_2 \circ S_1$  ook een element van  $G$ .

#### Basisregel 2: *Associativiteit:*

Als  $S_1, S_2$  en  $S_3$  elementen zijn van verzameling  $G$ , dan is  $(S_1 \circ S_2) \circ S_3 = S_1 \circ (S_2 \circ S_3)$ .  
In een willekeurige groep is de groepsbewerking associatief.

#### Basisregel 3: *Identiteitselement*

De identieke transformatie (niets doen) is het identiteitselement in groepen  $G$  en  $H$ .

Er bestaat een identiteitselement  $e$  van  $G$  zodat voor alle  $S \in G$ ,  $e \circ S = S$  en  $S \circ e = S$ .

#### Basisregel 4: *Invers element*

Voor ieder element  $S_1$  bestaat er een invers element  $S_2$  zodat  $S_1 \circ S_2 = e = S_2 \circ S_1$ . Dit wil zeggen dat het uitvoeren van een symmetrie altijd omkeerbaar is door deze te combineren met een bepaalde symmetrie.

— 8



Iedere groep moet voldoen aan de vier basisregels.  
We noemen deze basisregels de **groepsaxioma's**.

We zijn nu klaar om een goede definitie te geven voor het begrip groep.

### De definitie van een groep

Een groep  $(G, *)$  is een wiskundige structuur die bestaat uit een niet-lege verzameling  $G$ , samen met een bewerking die we voorstellen met een  $*$ . De verzameling samen met de bewerking moeten voldoen aan vier eisen die samen bekendstaan als de groepsaxioma's:

#### 1) Geslotenheid

Voor alle  $a, b \in G$  geldt  $a * b \in G$ .

#### 2) Associativiteit

Voor alle  $a, b, c \in G$  geldt de relatie:  $(a * b) * c = a * (b * c)$ .

#### 3) Identiteitselement

Er bestaat een element  $e \in G$ , zodat voor alle elementen  $a \in G$  geldt dat  $e * a = a * e = a$ .

#### 4) Invers element

Voor elke  $a \in G$  bestaat er een element  $a^{-1} \in G$ , waarvoor geldt:  
 $a * a^{-1} = a^{-1} * a = e$ .

⚠ In groepsaxioma 4 veronderstellen we eigenlijk dat er exact 1 identiteitselement  $e \in G$  bestaat. We zullen in paragraaf 1.3 ontdekken dat als er een identiteitselement  $e$  bestaat dit element ook het enige identiteitselement (*uniek*) is.

We noemen deze eigenschap de **uniciteit van het identiteitselement**.

⚠ Niet elke groep heeft de commutativiteitseigenschap! We noemen een groep  $G$  **commutatief** als voor elk element  $a, b$  in  $G$  geldt:  $a * b = b * a$  of equivalent als de Cayleytabel van groep  $G$  symmetrisch is rond de hoofddiagonaal.

### Voorbeeld

De verzameling  $G$  samen met de operatie  $\circ$  uit 1.1.1 is een voorbeeld van een groep. In deze groep zitten 6 verschillende symmetrieën van de gelijkzijdige driehoek.

We kennen het symbool  $R$  toe aan een rotatie van  $120^\circ$

en het symbool  $S$  aan de spiegeling over de verticale hoogtelijn.

Tenslotte definiëren ook een groepsoperatie  $\circ$  via volgende rekenregels:

- $R \circ R \circ R = R^3 = e$ , want drie keer roteren over  $120^\circ$  is een rotatie over  $360^\circ$ .
- $S \circ S = S^2 = e$ .
- $R \circ S = RS = SR^2$ , want eerst spiegeling en daarna roteren is hetzelfde als twee keer roteren en daarna spiegelen.  
(of analoog  $S \circ R = SR = R^2S$ )

We kunnen nu de 6 symmetrieën in groep  $G$  schrijven als:

$$\{e, R, R^2, S, RS, R^2S\} \text{ of } \{e, R, R^2, S, SR, SR^2\}$$

We weten al uit paragraaf 1.1 dat deze groep voldoet aan de groepsaxioma's.

We zullen regelmatig de notatie voor een groep niet voluit schrijven.



We schrijven dan groep  $G$  in plaats van groep  $(G, *)$  als uit de context duidelijk is wat de groepsbewerking  $*$  is.

### 1.1.6 Oneindige groepen

Nu we een definitie hebben gevormd van het begrip groep proberen we groepen beter te begrijpen. Eigenlijk zijn groepen geen nieuwe structuren.

Je kent zelf al veel groepen zonder dat je dit weet!

Zo is bijvoorbeeld  $(\mathbb{Z}, +)$  de verzameling van de gehele getallen samen met de optelling een groep.

9 Controleer dat  $(\mathbb{Z}, +)$  inderdaad een groep is door de groepsaxioma's na te gaan.

**Geslotenheid:** De som van twee gehele getallen is opnieuw een geheel getal.

Bijvoorbeeld:  $(-10) + 2 = -8$  en  $-8$  is een geheel getal.

In symbolen:  $\forall a, b \in \mathbb{Z} : a + b \in \mathbb{Z}$ .

**Associativiteit:** De optelling is altijd associatief.

In symbolen:  $\forall a, b, c \in \mathbb{Z} : (a + b) + c = a + (b + c)$ .

**Identiteitselement:** Het identiteitselement is 0, want 0 optellen bij een getal geeft opnieuw dat getal.

In symbolen:  $\forall a \in \mathbb{Z} : a + 0 = a = 0 + a$ .

**Invers element:** Het invers element van een getal is zijn tegengestelde, want de som van een getal en zijn tegengestelde is altijd gelijk aan 0.

In symbolen:  $\forall a \in \mathbb{Z} : a + (-a) = 0 = (-a) + a$ .

Is  $(\mathbb{N}, +)$  ook een groep? Waarom wel/niet?

Nee, het invers element van een getal in  $\mathbb{N}$  onder de optelling is zijn tegengestelde, maar de negatieve getallen zitten niet in deze verzameling.

— 9



$(\mathbb{Z}, +)$  is een voorbeeld van een **oneindige groep**, want de verzameling  $\mathbb{Z}$  heeft oneindig veel elementen.

Inderdaad, er bestaan oneindig veel gehele getallen: 1, 2, 100, 9999, ...

## 1.2 Orde van een groep

In deze korte paragraaf bespreken we een belangrijk begrip gerelateerd aan groepen. We beginnen met een voorbeeld.

### Voorbeeld

Beschouw de groep ( $G$ ) van alle symmetrieën van een gelijkzijdige driehoek zoals in paragraaf (1.1.1).

We weten al dat  $G = \{e, R, R^2, S, RS, R^2S\}$ , waarbij  $R$  een rotatie is en  $S$  een spiegeling. We zien dus dat  $G$  zes verschillende elementen (symmetrieën) bevat. We zeggen dan dat **de orde van de groep**  $G$  gelijk is aan zes.

Denk nog eens na over de rekenregels binnen deze groep.

We weten al dat  $S^2 = e$  en ook  $R^3 = e$ . We zeggen dan dat **de orde van het element**  $S$  gelijk is aan 2 en de orde van het element  $R$  gelijk is aan 3.

Natuurlijk is  $S^4 = S^{2^2} = e^2 = e$ , maar toch is de orde van het element  $S$  gelijk aan 2 en niet gelijk aan 4. We zoeken dus naar het **kleinste** getal  $n$  waarvoor  $b^n = e$ .

Wat is de orde van  $R^2$  in  $G$ ? **De orde is 3,  $R^2 \circ R^2 \circ R^2 = R^6 = (R^3)^2 = e^2 = e$ .**

Wat is de orde van  $RS$  in  $G$ ? **De orde is 2,  $RS \circ RS = RSRS = R(R^2S)S = e$ .**

### Orde van een groep

Het aantal elementen in een groep  $G$  noemen we de **orde van de groep** en we noteren dit met  $\#G$  of  $\text{ord}(G)$ .

De **orde van het element**  $a$  in een groep met bewerking  $*$  is het **kleinste** getal  $n$  zodat  $a^n = \underbrace{a * a * a * \dots}_{n \text{ keer}} = e$  en we noteren dit met  $\text{ord}(a)$ .

De orde van het identiteitselement  $e$  is dus altijd gelijk aan 1.

*In bovenstaand voorbeeld is  $\#G = 6$  en  $\text{ord}(R) = 3$ .*



De orde van een element is **altijd** een deler van de orde van een groep. We tonen dit aan in oefening 50 met behulp van de stelling van Lagrange (HF3).



Een oneindige groep heeft oneindig veel elementen. Deze groepen hebben dus ook een oneindige orde.

Bijvoorbeeld in de groep  $(\mathbb{Z}, +)$ , de gehele getallen onder de optelling, hebben alle getallen (behalve het identiteitselement 0) een oneindig orde. Het is dus meestal niet zinvol om te spreken over ordes in oneindige groepen.

### 1.3 Eigenschappen van groepen

In deze paragraaf bekijken we enkele algemene eigenschappen.

We beginnen telkens met de eigenschappen te bekijken in de groep  $(\mathbb{Z}, +)$ , maar zullen daarna zelf een algemeen bewijs vormen.

**10** Kunnen er in een groep  $(G, *)$  twee identiteitselementen bestaan?

Wat is het identiteitselement in  $(\mathbb{Z}, +)$ ? **0.**

Bewijs de uniciteit van het identiteitselement voor alle groepen.

- Stel dat een groep  $(G, *)$  twee identiteitselementen heeft  $e_1$  en  $e_2$ .
- Stel dat  $x$  nu een willekeurig element uit  $G$  is.
- Wat is  $e_1 * x (= x * e_1)$ ?  **$x$ .** Wat is  $x * e_2 (= e_2 * x)$ ?  **$x$ .**
- Vervang in bovenstaande vergelijkingen  $x$  eens door  $e_1$  en door  $e_2$ . Bewijs dat  $e_1 = e_2$ , dus dat er maar één identiteitselement bestaat.

**$e_1 * e_2 = e_1$ , want  $e_2$  is een identiteitselement, maar  $e_1 * e_2 = e_2$ , want  $e_1$  is een identiteitselement. Dit betekent dat  $e_1 = e_2$ .**

**11** Kan een element  $x$  in een groep  $(G, *)$  twee inverse elementen hebben?

Wat is het invers element van 5 in  $(\mathbb{Z}, +)$ ? **-5.**

Bewijs de uniciteit van het invers element voor alle groepen.

- Stel dat een element  $x$  in de groep  $(G, *)$  twee inverse elementen heeft  $\alpha_1$  en  $\alpha_2$ .
- Per definitie is dan  $x * \alpha_1 = e$  en  $x * \alpha_2 = e$ .
- Bewijs dat  $\alpha_1 = \alpha_2$ , dus dat er maar één invers element van  $x$  bestaat.  
Tip: Bereken  $\alpha_1 * x * \alpha_2$  op twee manieren.

**$\alpha_1 = \alpha_1 * e = \alpha_1 * (x * \alpha_2) = (\alpha_1 * x) * \alpha_2 = e * \alpha_2 = \alpha_2$ . Dit betekent dat  $\alpha_1 = \alpha_2$ .**

— 11

**\*12** In een groep  $(G, *)$  met  $a, b \in G$ , heeft de vergelijking  $x * a = b$  altijd een unieke oplossing voor  $x$

In  $(\mathbb{Z}, +)$ , wat is  $x$  in  $x + a = b$ ?  **$x = b + (-a)$ .**

Bekijk de Cayley tabel uit oefening 6, herken je de uitspraak in deze groep?

Bewijs de eigenschap voor alle groepen.

- Neem  $a$  en  $b$  in groep  $(G, *)$ , we bewijzen dat  $x$  in  $x * a = b$  uniek is.
- **$x$  bestaat:**  $x = b * a^{-1}$ , want  $x * a * a^{-1} = (b * a^{-1}) \implies x * e = b * a^{-1} \implies x = b * a^{-1}$ .  
Tip: Rechts vermenigvuldig  $(*)$  in  $x * a = b$  aan beide kanten met  $a^{-1}$ .
- **$x$  is uniek:** Tip: Stel dat  $x_1$  en  $x_2$  oplossingen zijn voor de vergelijking  $x * a = b$ . Dan is  $x_1 * a = b$ , maar ook  $x_2 * a = b$ .

**Met de tip zien we dat  $x_1 * a = b = x_2 * a$ . Als we beide leden rechts vermenigvuldigen met  $a^{-1}$ , dan krijgen we  $x_1 * a * a^{-1} = x_2 * a * a^{-1}$  of  $x_1 = x_2$ .**

— 12

## 1.4 Oefeningen

### 1.1

13 Zijn onderstaande verzamelingen onder de vermenigvuldigingsbewerking groepen?

- $(\mathbb{Z}_0, \cdot)$ , de verzameling van gehele getallen zonder 0.
- $(\mathbb{Q}, \cdot)$ , de verzameling van rationale getallen.
- $(\mathbb{Q}_0, \cdot)$ , de verzameling van rationale getallen zonder nul.

— 13

Merk op dat het identiteitselement gelijk moet zijn aan 1.

a) Nee, want onder de vermenigvuldiging is het invers element van een geheel getal  $a$  gelijk aan  $\frac{1}{a}$  en deze breuk is geen element van de verzameling  $\mathbb{Z}$ .

b) Nee, want 0 heeft geen invers element. Er is geen enkel getal dat we kunnen vermenigvuldigen met 0 zodat we het identiteitselement 1 uitkomen.

c) Ja, dit is een groep.

*Geslotenheid:* Twee rationale getallen vermenigvuldigen geeft opnieuw een rationaal getal.

*Associativiteit:* De vermenigvuldiging is associatief.

*Identiteitselement:* 1 is het identiteitselement, want  $\forall a \in \mathbb{Q}, a \cdot 1 = a = 1 \cdot a$ .

*Invers element:* Het invers element van  $a \in \mathbb{Q}$  is gelijk aan  $\frac{1}{a}$ , want  $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$ .

14 Zijn onderstaande verzamelingen met bijhorende bewerking groepen?

- $(\mathbb{N}, *)$ , met  $a * b = \min(a, b)$ .
- $(\mathbb{N}, *)$ , met  $a * b = \max(a, b)$ .
- $(\mathbb{N}, *)$ , met  $a * b = a^b$ .

— 14

a) Nee, want de verzameling heeft geen identiteitselement. als  $e$  bestaat, dan zou  $a * e = \min(a, e) = a$ . Dit betekent dat  $e$  groter moet zijn dan alle natuurlijke getallen en dit kan natuurlijk niet.

b) Nee, want een willekeurig element  $a$  heeft geen invers element. Merk op dat 0 het identiteitselement is, want  $a * 0 = \max(a, 0) = a = \max(0, a) = 0 * a$ . We kunnen nooit een invers element  $a^{-1}$  vinden van een natuurlijk getal  $a$  groter dan 0, want  $a * a^{-1} = \max(a, a^{-1})$ . Dit maximum kan nooit gelijk zijn aan 0.

c) Nee, er bestaat geen identiteitselement. Je zou misschien denken dat 1 het identiteitselement is, want  $a * 1 = a^1 = a$ , maar dan moet  $1 * a = 1^a = a$  en dat is natuurlijk niet waar.

15 Hieronder staat een cayley tabel van een verzameling die bestaat uit **2 elementen** namelijk de elementen EVEN (alle even getallen) en ONEVEN (alle oneven getallen). Is deze verzameling samen met de optelling een groep?

+	EVEN	ONEVEN
EVEN		
ONEVEN		

+	EVEN	ONEVEN
EVEN	EVEN	ONEVEN
ONEVEN	ONEVEN	EVEN

Ja, dit is een groep met 2 elementen.

*Geslotenheid:* De optelling van twee even of oneven getallen is altijd een geheel getal en dus even of oneven.

*Associativiteit:* De optelling is altijd associatief.

*Identiteitselement:* EVEN is het identiteitselement, want  $EVEN + EVEN = EVEN$  en  $ONEVEN + EVEN = ONEVEN = EVEN + ONEVEN$ .

*Invers element:* Beide elementen hebben een invers element. Het invers element van EVEN is EVEN en het invers element van ONEVEN is ONEVEN.

**16** Beschouw de verzameling  $Q = \{1, -1, i, -i, j, -j, k, -k\}$  en de bewerking  $\cdot$  met de volgende rekenregels:

- $(-1) \cdot (-1) = 1$
- Voor alle elementen  $a \in Q$  geldt dat  $(-1) \cdot a = -a = a \cdot (-1)$
- $i \cdot i = j \cdot j = k \cdot k = i \cdot j \cdot k = -1$
- $i \cdot j = -j \cdot i$ ,  $i \cdot k = -k \cdot i$  en  $j \cdot k = -k \cdot j$

- a) Wat is het identiteitselement?
  - b) Wat is het invers element van  $i$  en van  $-k$ ?
  - c) Bereken  $j \cdot k$  en  $k \cdot j$ , is de groepsbewerking van  $Q$  commutatief?
  - d) Maak een cayleytabel van groep  $Q$
  - e) Toon aan dat  $Q$  een groep is. Associativiteit hoef je niet aan te tonen.
- $Q$  is een bekende groep die we de **quaternionengroep** noemen.

a) Het identiteitselement is 1, want  $1 \cdot a = (-1) \cdot (-1) \cdot a = (-1) \cdot (-a) = a$ .

b) Het invers element van  $i$  is  $-i$ , want  $i \cdot (-i) = i \cdot (-1) \cdot i = i \cdot i \cdot (-1) = (-1) \cdot (-1) = 1$  en andersom is ook  $(-i) \cdot i = 1$ .

Het invers element van  $-k$  is  $k$ , want  $(-k) \cdot k = (-1) \cdot k \cdot k = (-1) \cdot (-1) = 1$  en andersom is ook  $k \cdot (-k) = 1$ .

c)  $i \cdot j \cdot k = -1$ , beide leden links vermenigvuldigen met  $i$  geeft ons  $\underbrace{i \cdot i}_{=-1} \cdot j \cdot k = i \cdot (-1)$  en

$-j \cdot k = -i$  en dus is  $j \cdot k = i$ .

$k \cdot j = -j \cdot k$ , dus  $k \cdot j = -i$ . De groep is niet commutatief.

d)

·	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	j	-j
-i	-i	i	1	-1	-k	k	-j	j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

e) *Geslotenheid*: Dit zie je in de Cayleytabel, twee elementen vermenigvuldigen geeft opnieuw een element in  $Q$ .

*Identiteitselement*: 1 is het identiteitselement (zie a).

*Invers element*: We kunnen voor elk element het invers element aflezen in de tabel.  $i$  en  $-i$ ,  $j$  en  $-j$ ,  $k$  en  $-k$  zijn inverse van elkaar, terwijl 1 en  $-1$  hun eigen invers element zijn.

**\*17**

Vul onderstaande tabel in **zodat** de tabel een cayleytabel van een groep is. Verklaar waarom deze tabel maar op één unieke manier ingevuld kan worden.

*	a	b	c
a			
b			
c			a

$c$  kan niet het identiteitselement zijn, want dan zou  $c * c = e$ . We kunnen verder rekenen in de eerste kolom.  $c * a$  moet gelijk zijn aan  $b$  of  $c$ . Merk op dat als  $c * a = c$  dan moet  $c * b = b$ , maar dit kan niet, want dan zou  $c$  het identiteitselement zijn. De enige optie is dus dat  $c * a = b$ . Dit betekent dat  $c * b = c$  en dus is  $b$  het identiteitselement. Je kan de tabel nu verder aanvullen.

*	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

## 1.2

**18** In de groep  $G$  die alle symmetrieën bevat van de gelijkzijdige driehoek ( $G = \{e, R, R^2, S, RS, SR\}$  uit 1.1.1).

- a) Wat is de orde van deze groep?  
b) Bepaal de orde van alle elementen.

— 18

a) De orde is 6, want  $G$  heeft 6 elementen.  
b)  $\text{ord}(e) = 1$ ,  $\text{ord}(R) = \text{ord}(R^2) = 3$  en  $\text{ord}(S) = \text{ord}(RS) = \text{ord}(R^2S) = 2$ . Zie voorbeeld in 1.3 voor de berekening. Je kan ook redeneren met symmetrieën. De orde van een spiegeling is altijd 2, want twee keer achter elkaar spiegelen over dezelfde as geeft je de oorspronkelijke figuur.

**19** Vul volgende zinnen aan voor een willekeurige groep  $(G, *)$  en willekeurige  $a \in G$ . Verklaar je antwoord.

- a) Als  $\text{ord}(a) = 1$ , dan is  $a \dots$ .  
b) Als  $\text{ord}(a) = 2$ , dan is het inverse van  $a$  gelijk aan  $\dots$ .  
c) Als  $\text{ord}(a) = 4$ , dan is  $\text{ord}(a * a)$  gelijk aan  $\dots$ .

— 19

a)  $a = e$ , want het enige element met orde 1 is het identiteitselement.  
b)  $a^{-1} = a$ , want als  $\text{ord}(a) = 2$  dan is  $\text{ord}(a * a) = e$ .  
c) als  $\text{ord}(a) = 4$ , dan is  $a * a * a * a = e$ , dus  $(a * a) * (a * a) = e$  en  $\text{ord}(a * a) = 2$ .

**20** Beschouw opnieuw de quaternionengroep uit oefening 16.

Dit is de verzameling  $Q = \{1, -1, i, -i, j, -j, k, -k\}$

met de bewerking  $\cdot$  die de volgende rekenregels volgt:

- $(-1) \cdot (-1) = 1$
- Voor alle elementen  $a \in Q$  geldt dat  $(-1) \cdot a = -a = a \cdot (-1)$
- $i \cdot i = j \cdot j = k \cdot k = i \cdot j \cdot k = -1$
- $i \cdot j = -j \cdot i$ ,  $i \cdot k = -k \cdot i$  en  $j \cdot k = -k \cdot j$

In oefening 15 bewezen we dat  $Q$  een groep is. Beantwoord de volgende vragen:

- a) Wat is  $\#Q$ ?  
b) Wat is  $\text{ord}(k)$ ?  
c) Wat is  $\text{ord}(-k)$ ?  
d) Hoeveel elementen hebben orde 2?

— 20

a)  $\#G = 8$ , want  $Q$  bevat 8 elementen.  
b)  $\text{ord}(k) = 4$ , want  $\underbrace{k \cdot k}_{=-1} \cdot \underbrace{k \cdot k}_{=-1} = (-1) \cdot (-1) = 1$ .  
c)  $\text{ord}(-k) = 4$ , want  $-k \cdot (-k) = (-1) \cdot k \cdot (-1) \cdot k = (-1) \cdot (-1) \cdot k \cdot k = 1 \cdot (-1) = -1$   
en dus  $(-k) \cdot (-k) \cdot (-k) \cdot (-k) = (-1) \cdot (-1) = 1$ .  
d) Enkel het element  $-1$ , want  $(-1) \cdot (-1) = 1$ . De orde van  $i, -i, j$  en  $-j$  kunnen we op dezelfde manier berekenen als de orde van  $k$  en  $-k$ .

## 1.3

\*21

Stel dat  $(G, *)$  een willekeurige groep is. Laat zien dat

- a) Als  $a * a = a$ , dan is  $a$  het identiteitselement.  
 b)  $a * x = b$  heeft altijd een unieke oplossing.  
 c) Als  $(a * b)^{-1} = a^{-1} * b^{-1}$  voor alle  $a, b \in G$ , dan is  $G$  een commutatieve groep.

— 21

a) Vermenigvuldig beide leden rechts met  $a^{-1}$ , we krijgen dan

$$a * a * a^{-1} = a * a^{-1} \implies a = e.$$

Inderdaad  $a$  is het eenheidselement.

b)  $x$  bestaat, want als we beide leden van de vergelijking links vermenigvuldigen met  $a^{-1}$ , krijgen we  $a^{-1} * (a * x) = (a^{-1} * a) * x = e * x$  in het linkerlid en  $a^{-1} * b$  in het rechterlid. We zien dus dat  $x = a^{-1} * b$ .

$x$  is uniek, stel dat  $x_1$  en  $x_2$  beide oplossingen zijn, dan  $a * x_1 = b = a * x_2$ . Als we nu beide leden links vermenigvuldigen met  $a^{-1}$  krijgen we  $a^{-1} * a * x_1 = a^{-1} * a * x_2 \implies x_1 = x_2$ .

c) We weten dat  $(a * b) * (a * b)^{-1} = e$ , dan  $(a * b) * a^{-1} * b^{-1} = e$ , vermenigvuldig nu beide leden rechts met  $b$  en daarna met  $a$ . We hebben nu

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

Vanwege de associativiteit van de bewerking kunnen we dit verder uitrekenen als volgt:

$$a * b * a^{-1} * \underbrace{b^{-1} * b}_{=e} * a = e * b * a \implies a * b * \underbrace{a^{-1} * a}_{=e} = b * a \implies (a * b) = b * a.$$

Inderdaad  $G$  is commutatief.

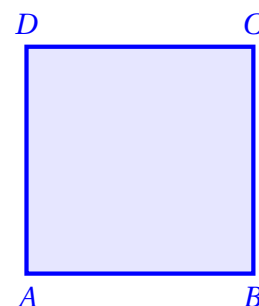
## 2 | Voorbeelden van groepen

Er bestaan erg veel verschillende groepen. Veel groepen krijgen binnen de wiskunde een specifieke naam zodat iedereen weet over welke groep we spreken, zonder altijd opnieuw de volledige groep en zijn rekenregels te moeten beschrijven. In dit hoofdstuk komen enkele interessante voorbeelden van groepen aan bod.

### 2.1 Symmetriegroepen

Symmetriegroepen hebben we in paragraaf 1.1 al heel veel gebruikt. Deze groepen kunnen we met symmetrieën van meetkundige figuren voorstellen. Voordat we een definitie geven, ontdekken we met onderstaande oefening de rekenregels van een speciale soort symmetriegroep, de diëdergroep.

- 22** In deze oefening bekijken we de groep  $(K, \circ)$ , waarbij  $K$  de verzameling is die alle symmetrieën van een vierkant  $(ABCD)$  bevat met de bewerking om symmetrieën te combineren.



Net zoals bij een gelijkzijdige driehoek zijn al deze symmetrieën combinaties van rotaties en spiegelingen.

Hoeveel elementen heeft de verzameling  $K$ ? **8**

Kies één rotatie (R) en één spiegeling (S).

- 1) Rotatie over  $90^\circ$  (in wijzerzin) (R)    2) Spiegeling over diagonaal AC (S)

Vul onderstaande rekenregels verder aan:

- $R \circ R \circ R \circ R = R^4 = \dots$      $e$
- $S \circ S = S^2 = \dots$      $e$
- $R \circ S = RS = S \circ \dots$      $RS = S \circ R^3 = SR^3$
- $S \circ R = SR = \dots \circ S$      $SR = R^3 \circ S = R^3 S$

Maak een Cayleytabel van groep  $(K, \circ)$ . Tip: Kijk nog eens terug naar oefening 4.

$\circ$	$e$	$R$	$R^2$	$R^3$	$S$	$RS$	$R^2S$	$R^3S$
$e$	$e$	$R$	$R^2$	$R^3$	$S$	$RS$	$R^2S$	$R^3S$
$R$	$R$	$R^2$	$R^3$	$e$	$RS$	$R^2S$	$R^3S$	$S$
$R^2$	$R^2$	$R^3$	$e$	$R$	$R^2S$	$R^3S$	$S$	$RS$
$R^3$	$R^3$	$e$	$R$	$R^2$	$R^3S$	$S$	$RS$	$R^2S$
$S$	$S$	$R^3S$	$R^2S$	$RS$	$e$	$R^3$	$R^2$	$R$
$RS$	$RS$	$S$	$R^3S$	$R^2S$	$R$	$e$	$R^3$	$R^2$
$R^2S$	$R^2S$	$RS$	$S$	$R^3S$	$R^2$	$R$	$e$	$R^3$
$R^3S$	$R^3S$	$R^2S$	$RS$	$S$	$R^3$	$R^2$	$R$	$e$

## Symmetriegroepen

De **symmetriegroep** van een meetkundige figuur is de verzameling van alle symmetriën van een bepaalde meetkundige figuur samen met de groepsbewerking het samenstellen van symmetrieën voorstelt.

Een groep die enkel bestaat uit rotaties van een meetkundige figuur noemen we een **rotatiegroep**.

△ Lijnspiegelingen zijn ook rotaties (van  $180^\circ$ ), maar dit kunnen we enkel zien door de figuur 3-dimensionaal te bekijken. Een rotatiegroep van een 2-dimensionale figuur bevat dus geen spiegelingen.

### Diëdergroep

Een symmetriegroep van een regelmatige veelhoek noemen we een **diëdergroep**. We gebruiken hiervoor de notatie  $D_n$ , waarbij  $n$  het aantal hoekpunten van de veelhoek is.

- $D_3$  is dus de groep die alle symmetrieën van de gelijkzijdige driehoek bevat, zoals in paragraaf 1.1.1.
- De symmetriegroep van de rechthoek, zoals in paragraaf 1.1.4, is geen diëdergroep, want een rechthoek is geen regelmatige veelhoek.

De verzameling  $D_n$  bevat  $2n$  elementen ( $n$  rotaties en  $n$  spiegelingen), dus  $\#(D_n) = 2n$ . Als  $R$  een rotatiesymmetrie voorstelt en  $S$  een spiegelsymmetrie, dan volgt de groepsbewerking  $\circ$  de volgende regels:

- $\underbrace{R \circ R \circ R \dots}_{n \text{ keer}} = R^n = e$ .
- $S \circ S = S^2 = e$ .
- $S \circ R = SR = R^{n-1}S$  of analoog  $R \circ S = RS = SR^{n-1}$ .

We kunnen de  $2n$  elementen dus schrijven als:

$$\{e, R, R^2, \dots, R^{n-1}, S, RS, R^2S, \dots, R^{n-1}S\}.$$

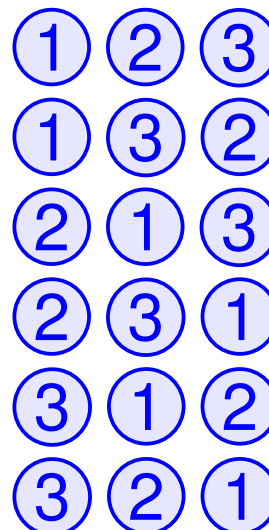
## 2.2 Permutatiegroepen

### 2.2.1 Permutaties

Permutaties ken je misschien al van de lessen kansrekenen en combinatoriek. In deze lessen definiëren we een **permutatie** als een ordening van een verzameling van elementen.

Bijvoorbeeld: Hiernaast zie je alle permutaties van een verzameling bestaande uit drie objecten.

Kan je zelf nog een voorbeeld bedenken van een permutatie?



**Voorbeeld**

In dit voorbeeld beschrijven we een permutatie als een **herordening** en introduceren we de **cykelnotatie**.

In een verzameling met 4 elementen, kunnen we ieder element een rangnummer 1, 2, 3 of 4 geven.

De permutatie 2314 kunnen we dan zien als een herordening van de 'standaardordening' 1234. Door de permutatie te vergelijken met deze standaardordening, kan je zien welk element op welke positie staat.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

We zien dat  $1 \mapsto 2$ ,  $2 \mapsto 3$ ,  $3 \mapsto 1$  en  $4 \mapsto 4$ .

Dit kunnen we ook schrijven als  $1 \mapsto 2 \mapsto 3 \mapsto 1$  en  $4 \mapsto 4$ .

We gebruiken de **cykelnotatie** om permutaties te beschrijven. We noteren de permutatie waarbij  $1 \mapsto 2 \mapsto 3 \mapsto 1$  en  $4 \mapsto 4$  als  $(123)(4)$  of kortweg  $(123)$ .

We noteren de permutatie 2314 vanaf nu dus als  $(123)$ .

**Cykelnotatie**

Een permutatie schrijven we meestal in cyclische vorm, **cykels** genoemd. In een cykel staat een herordening van de standaardordening beschreven.

De cykel  $(a_1, a_2, a_3)$  betekent dat  $a_1 \mapsto a_2 \mapsto a_3 \mapsto a_1$ .

Merk op dat  $(a_1, a_2, a_3) = (a_2, a_3, a_1) = (a_3, a_1, a_2)$ . Het maakt dus niet uit welk element vooraan in de cykel staat zolang de opeenvolging hetzelfde blijft.

$()$  is de cykelnotatie voor de **identieke permutatie**. In deze permutatie wordt er geen enkel element verplaatst.

Twee of meer cykels waarbij ieder rangnummer maximaal één keer voorkomt, noemen we **disjuncte cykels**.

Voorbeelden:  $(123)(45)$ ,  $(13)(24)$ ,  $(45)(13)(26)$ .

**Voorbeeld**

Via deze notatie kunnen we ook makkelijk permutaties samenstellen. We doen dit via de  $\circ$ -bewerking. Herinner je dat we met de  $\circ$ -bewerking altijd van **rechts naar links** rekenen. Zo is bijvoorbeeld  $(134) \circ (12)$  gelijk aan de cykel  $(1234)$ .

We berekenen eerst de herordening die overeenkomt met cykel  $(12)$ . Dit is het rijtje 2134 zoals je hieronder kan zien.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Daarna passen we cykel  $(134)$  toe op deze nieuw herordening en vinden het rijtje 2341.

$$\begin{pmatrix} 2 & 1 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

We zien het volgende:

- (a)  $(1 \mapsto 2)$  in de rechtse cykel en  $(2 \mapsto 2)$  in de linkse cykel.  
De combinatie geeft dus  $(1 \mapsto 2)$ .
- (b)  $(2 \mapsto 1)$  in de rechtse cykel en  $(1 \mapsto 3)$  in de linkse cykel.  
De combinatie geeft dus  $(2 \mapsto 3)$ .
- (c)  $(3 \mapsto 3)$  in de rechtse cykel en  $(3 \mapsto 4)$  in de linkse cykel.  
De combinatie geeft dus  $(3 \mapsto 4)$ .
- (d)  $(4 \mapsto 4)$  in de rechtse cykel en  $(4 \mapsto 1)$  in de linkse cykel.  
De combinatie geeft dus  $(4 \mapsto 1)$ .

We kunnen de afbeeldingen samenvoegen als  $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$ . Dit komt overeen met cykel  $(1234)$ .

Inderdaad als we vertrekken van de standaardordening en herordening  $(1234)$  berekenen vinden we rijtje 2341.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

We kunnen een combinatie van cyclen ook snel berekenen via volgend trucje.

We berekenen de combinatie  $(234) \circ (123) = (13)(24)$  in 4 stappen.

1. We starten bij het eerste getal in de rechtse cykel (1):  
 $(1 \mapsto 2)$  in de rechtse cykel en  $(2 \mapsto 3)$  in de linkse cykel.  
De combinatie geeft dus  $(1 \mapsto 3)$ . We noteren **(13)**.
2. We gaan verder met het getal waarmee we eindigden in stap 1 (3):  
 $(3 \mapsto 1)$  in de rechtse cykel en  $(1 \mapsto 1)$  in de linkse cykel.  
De combinatie geeft dus  $(3 \mapsto 1)$ . We noteren **(13)**.  
We sluiten de cykel, maar zijn nog niet klaar.
3. We gaan verder met het volgende niet gebruikte getal in de rechtse cykel (2).  
 $(2 \mapsto 3)$  in de rechtse cykel en  $(3 \mapsto 4)$  in de linkse cykel.  
De combinatie geeft dus  $(2 \mapsto 4)$ . We noteren **(13)(24)**.
4. Tenslotte gaan we verder met het getal waarmee we eindigden in stap 3 (4).  
 $(4 \mapsto 4)$  in de rechtse cykel en  $(4 \mapsto 2)$  in de linkse cykel.  
De combinatie geeft dus  $(4 \mapsto 2)$ . We noteren **(13)(24)**.

Wanneer we alle getallen hebben gehad en de cykel terug gesloten is, zijn we klaar met het berekenen van de combinatie.

- 23** Bereken de volgende combinaties van permutaties van 5 elementen.  
Schrijf je antwoord als een disjuncte cykel.  
-  $(51) \circ (53)$

Dit is de permutatie  $(531)$ .

- $(34) \circ (1435)$

Dit is de permutatie  $(135)$ .

- $( ) \circ (1234) \circ (13)$

$(1234) \circ (13) = (14)(23)$ .

- $(15) \circ (14) \circ (13) \circ (12)$

$(15) \circ (14) \circ (13) \circ (12) = (145) \circ (13) \circ (12) = (1345) \circ (12) = (12345)$ .

- $(123) \circ (145) \circ (134)$

$(123) \circ (145) \circ (134) = (14523) \circ (134) = (235)$ .

Wat merk je op als je de eerste twee permutaties vergelijkt?  
Kan je dit verklaren?

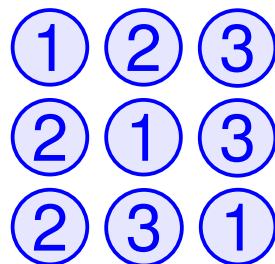
De permutaties zijn aan elkaar gelijk.

Ja, de volgorde van de cijfers in de cykelnotatie is hetzelfde, dus stellen zij dezelfde permutatie voor.

— 23

Alle permutaties van een bepaalde verzameling vormen samen een groep.  
Een voorbeeld van een verzameling met drie elementen kennen we al:  
De permutaties van de verzameling bestaande uit drie smileys.

- 24** De standaardordening van de drie objecten is  $(1)(2)(3)$   
Welke permutatie van de standaardordening (in cykelnotatie) komt overeen met onderstaande rijtjes?



Het eerste rijtje is 123, de cykelnotatie is  $( )$ .

Het tweede rijtje is 213, de cykelnotatie is  $(12)$ .

Het derde rijtje is 231, de cykelnotatie is  $(123)$ .

Hoeveel permutaties van drie elementen bestaan er? Noteer ze allemaal in cykelnotatie. Tip: We hebben ze allemaal opgesomd als rijtjes op het begin van deze paragraaf.

Er zijn 6 permutaties,  $()$ ,  $(12)$ ,  $(23)$ ,  $(13)$ ,  $(123)$  en  $(132)$ .

Toon aan dat alle permutaties van deze verzameling een groep vormen. Je moet hiervoor alle vier de groepsaxioma's controleren. Sommige zijn wat makkelijker te controleren dan andere!

**Geslotenheid:** De combinatie van twee permutaties van 3 elementen is opnieuw een permutatie van 3 elementen.

Bijvoorbeeld:  $(23) \circ (312) = (13)$ .

**Associativiteit:** Inderdaad, het combineren van permutaties is een associatieve operatie. We kunnen permutaties ook voorstellen als functies en we weten dat de compositie van functies associatief is. Als  $f, g$  en  $h$  functies zijn van een verzameling met 3 elementen naar dezelfde verzameling, dan is  $(h \circ (f \circ g))(x) = h((g \circ f)(x)) = h(g(f(x)))$  and  $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$ .

**Identiteitselement:** De identieke permutatie  $()$  is het identiteitselement.

De combinatie van een permutatie  $P$  met de permutatie die niets verandert blijft de permutatie  $P$ .

**Invers element:** Je kan voor ieder element het inverse berekenen.

De permutaties  $()$ ,  $(12)$ ,  $(13)$ ,  $(23)$  hebben zichzelf als invers element. De permutaties  $(123)$  en  $(132)$  zijn elkaars invers, want  $(123) \circ (132) = () = (132) \circ (123)$ .

### Permutatiegroepen

Een **permutatiegroep** is een verzameling van permutaties van een verzameling elementen en de groepsbewerking  $\circ$  die het combineren van permutaties voorstelt. Meestal stellen we de verzameling voor als een verzameling getallen  $\{1, 2, 3, \dots\}$  of letters  $\{A, B, C, \dots\}$  die de rangnummers van de verschillende elementen voorstellen.

We noteren met  $S_n$  de groep die **alle** permutaties bevat van  $n$  elementen.  $\#S_n = n!$ , want er zijn natuurlijk  $n!$  permutaties van  $n$  symbolen.

De groep die alle permutaties van ①, ② en ③ bevat is dus  $S_3$ .

Een groep behoort niet altijd tot één specifieke soort van groepen!

Sommige permutatiegroepen kunnen we bijvoorbeeld voorstellen als symmetriegroepen van bepaalde meetkundige figuren.

We zullen dit tegenkomen in hoofdstuk 3.



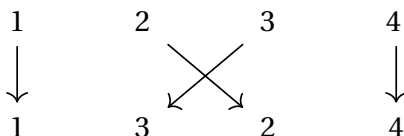
### 2.2.2 De alternerende permutatiegroep

In deze paragraaf zullen we de even permutaties onder de loep nemen. Hiervoor moeten we eerst nog enkele nieuwe begrippen introduceren.

⚠ Een permutatie die precies twee elementen omwisselt noemen we een **transpositie**.

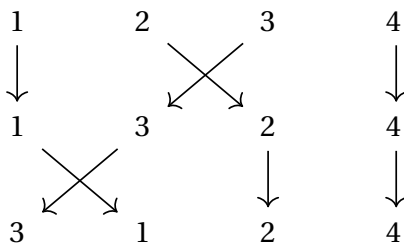
#### Voorbeeld

In dit voorbeeld bekijken we even en oneven permutaties in groep  $S_4$ . De permutatie  $(23)$  is een transpositie, we wisselen object 2 en 3 om.



De permutatie  $(23)$  is een **oneven permutatie**, want dit is een samenstelling van een oneven aantal transposities.

De permutatie  $(132)$  kunnen we ook schrijven als samenstelling van transposities.  $(132) = (13) \circ (23)$  (Reken dit zelf na).



De permutatie  $(132)$  is een **even permutatie**, want dit is een samenstelling van een even aantal transposities.

We kunnen  $(132)$  (=  $(213)$ ) ook schrijven als  $(21) \circ (31)$ . Over het algemeen kunnen we een even (respectievelijk oneven) permutatie op verschillende manieren schrijven als een samenstelling van transposities, maar het aantal transposities zal altijd even of (respectievelijk oneven) zijn. Dit tonen we niet aan in deze lessenreeks.

#### Soorten permutaties

Een samenstelling van een even aantal transposities noemen we een **even permutatie**.

Een samenstelling van een oneven aantal transposities noemen we een **oneven permutatie**.

*Voorbeeld in  $S_4$ :*

$(\ )$ ,  $(123)$ ,  $(13)(24)$  zijn even permutaties.

$(23)$ ,  $(1243)$  zijn oneven permutaties.

**25** Schrijf volgende permutaties als samenstellingen van transposities en geef ook aan of de permutaties even of oneven zijn.

- (124)

$(124) = (24) \circ (14)$ , even.

- (1523)

$(1523) = (23) \circ (53) \circ (13)$ , oneven.

- (52314)

$(52314) = (14) \circ (34) \circ (24) \circ (54)$ , even.

-  $(123) \circ (241)$  Tip: Schrijf eerst als één permutatie

$(123) \circ (241) = (24)(13) = (24) \circ (13)$ , even.

Wanneer is een permutatie even en wanneer oneven?  
Kun je een algemene regel bedenken?

Als de cykel(s) een even aantal elementen bevat(ten) is de permutatie oneven (en andersom).

— 25

**26** Je kan misschien zelf wel raden dat alle even permutaties van  $S_n$  samen een groep vormen. Toch is het heel moeilijk om dit aan te tonen voor willekeurige  $n$ . Daarom bekijken we in deze oefening enkel de permutatiegroep  $S_3$ .

Wat zijn de even permutaties van 3 elementen in  $S_3$ ?  $(\ )$ ,  $(132)$ ,  $(123)$ .

Bewijs dat alle even permutaties van 3 elementen een groep vormen.

*Geslotenheid:* De combinatie van twee even permutaties is opnieuw even. Een even permutatie gecombineerd met  $(\ )$  is sowieso even en  $(132) \circ (123) = (\ ) = (123) \circ (132)$ . Dus alle combinaties zijn opnieuw even.

*Associativiteit:* De associativiteit geldt in  $S_3$  en dus ook in een deelverzameling van  $S_3$ .

*Identiteitselement:* We weten al uit vorige oefeningen dat  $(\ )$  het identiteitselement is.

*Invers element:* Alle elementen hebben een inverse, want  $(123) \circ (132) = (\ ) = (132) \circ (123)$  en  $(\ )$  is zijn eigen inverse.

### Alternerende groep

De verzameling die alle even permutaties van  $n$  elementen bevat, is een deelverzameling van  $S_n$  met orde  $\frac{n!}{2}$ .

We noemen deze groep de **Alternerende groep** en noteren deze met  $A_n$ .

— 26

## 2.3 Oefeningen

**27** Welke bekende groepen worden hieronder beschreven?  
Geef ook de orde van deze groepen.

- a) Alle mogelijke manieren om 10 leerlingen te verdelen over 10 stoelen.  
b) Alle symmetrieën van een regelmatige achthoek.

— 27

- a) Dit zijn alle permutaties van 10 leerlingen, dus groep  $S_{10}$  met  $\#S_{10} = 10!$ .  
b) Dit is een symmetriegroep van een regelmatige veelhoek, dus groep  $D_8$  met  $\#D_8 = 8 \cdot 2 = 16$ .

**28** Beschouw de diëdergroepen  $D_4$  en  $D_5$ .

- a) Hoe kunnen we meetkundig  $D_4$  en  $D_5$  voorstellen en wat is hun orde?  
b) Bereken  $R^2(S)^{-1}RS(R^3)^{-1}$  in  $D_4$ .  
c) Bereken  $R^2(S)^{-1}RS(R^3)^{-1}$  in  $D_5$ .  
d) Is  $D_n$ , voor  $n > 1$ , een commutatieve groep? Verklaar.

— 28

a)  $\#D_4 = 8$  en dit is de symmetriegroep van een vierkant,  $\#D_5 = 10$  en dit is de symmetriegroep van een regelmatige vijfhoek.

$$b) R^2 \underbrace{S^{-1}}_{=S} RS \underbrace{(R^3)^{-1}}_{=R} = R^2 \underbrace{SR}_{=R^3S} = R^2(R^3S)SR = R^5R = R^6 = R^4R^2 = eR^2 = R^2.$$

$$c) R^2 \underbrace{S^{-1}}_{=S} RS \underbrace{(R^3)^{-1}}_{=R^2} = R^2 \underbrace{SR}_{=R^4S} SR^2 = R^2(R^4S)SR^2 = R^6R^2 = R^8 = R^5R^3 = eR^3 = R^3.$$

d) Nee,  $D_n$  is nooit een commutatieve groep, want  $SR = R^{n-1}S \neq RS$ .

**29** Maak een cayleytabel van de rotatiegroep van een regelmatige vijfhoek.

— 29

$\circ$	$e$	$R$	$R^2$	$R^3$	$R^4$	$S$	$RS$	$R^2S$	$R^3S$	$R^4S$
$e$	$e$	$R$	$R^2$	$R^3$	$R^4$	$S$	$RS$	$R^2S$	$R^3S$	$R^4S$
$R$	$R$	$R^2$	$R^3$	$R^4$	$e$	$RS$	$R^2S$	$R^3S$	$R^4S$	$S$
$R^2$	$R^2$	$R^3$	$R^4$	$e$	$R$	$R^2S$	$R^3S$	$R^4S$	$S$	$RS$
$R^3$	$R^3$	$R^4$	$e$	$R$	$R^2$	$R^3S$	$R^4S$	$S$	$RS$	$R^2S$
$R^4$	$R^4$	$e$	$R$	$R^2$	$R^3$	$R^4S$	$S$	$RS$	$R^2S$	$R^3S$
$S$	$S$	$R^4S$	$R^3S$	$R^2S$	$RS$	$e$	$R$	$R^2$	$R^3$	$R^4$
$RS$	$RS$	$S$	$R^4S$	$R^3S$	$R^2S$	$R$	$e$	$R^4$	$R^3$	$R^2$
$R^2S$	$R^2S$	$RS$	$S$	$R^4S$	$R^3S$	$R^2$	$R$	$e$	$R^4$	$R^3$
$R^3S$	$R^3S$	$R^2S$	$RS$	$S$	$R^4S$	$R^3$	$R^2$	$R$	$e$	$R^4$
$R^4S$	$R^4S$	$R^3S$	$R^2S$	$RS$	$S$	$R^4$	$R^3$	$R^2$	$R$	$e$

**30** Beschouw de groep  $S_5$ .

- Wat is  $\#S_5$ ?
- Wat is de orde van de alternerende groep  $A_5$ ?
- Wat is de orde van het element  $(123)$ .
- Is  $S_n$ , voor  $n > 2$ , een commutatieve groep?

— 30

a)  $\#S_5 = 5! = 120$ .

b) We weten dat  $\#A_5 = \frac{\#S_5}{2} = \frac{5!}{2} = \frac{120}{2} = 60$ .

c)  $\text{ord}((123)) = 3$ , want  $(123) \circ (123) = (132)$  en  $(123) \circ \underbrace{(123) \circ (123)}_{=(132)} = (123) \circ (132) = e$ .

d) Nee, want bijvoorbeeld  $(13) \circ (12) = (123)$  en  $(12) \circ (13) = (132)$ .

**31** Bepaal de orde van de volgende elementen uit groep  $S_4$ .

- $(AB)$
- $(ABC)$
- $(AB)(CD)$
- $(ABCD)$

— 31

$\text{ord}((AB)) = 2$ , want  $(AB) \circ (AB) = e$ .

$\text{ord}((ABC)) = 3$ , want  $(ABC) \circ (ABC) = (ACB)$  en  $(ABC) \circ (ABC) \circ (ABC) = (ABC) \circ (ACB) = e$ .

$\text{ord}((AB)(CD)) = 2$ , want  $(AB)(CD) \circ (AB)(CD) = e$ .

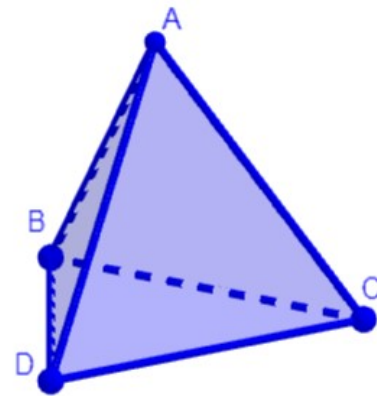
$\text{ord}((ABCD)) = 4$ , want  $(ABCD) \circ (ABCD) = (AC)(BD)$  en  $(ABCD) \circ (ABCD) \circ (ABCD) \circ (ABCD) = (AC)(BD) \circ (AC)(BD) = e$ .

## 3 | Deelgroepen en de stelling van Lagrange

### 3.1 De regelmatige tetraëder

We zullen zelf ontdekken wat een deelgroep precies is. De stelling van Lagrange is nauw verbonden met dit begrip. We maken hiervoor gebruik van een belangrijke symmetriegroep, namelijk de groep gevormd door alle symmetrieën van een regelmatige tetraëder.

Een tetraëder (of viervlak) is een meetkundige figuur die bestaat uit 4 vlakken in de vorm van driehoeken. De figuur heeft vier hoekpunten en zes ribben. Een tetraëder met gelijkzijdige driehoeken als vlakken noemen we een **regelmatige tetraëder** (of regelmatig viervlak).



In deze paragraaf onderzoeken we de symmetrieën van de regelmatige tetraëder. Herinner je dat een symmetrie van een figuur altijd een hoekpunt van de figuur afbeeldt op een ander hoekpunt. We zullen de symmetrieën dus ook beschrijven door te kijken wat er met de hoekpunten gebeurt.

#### 3.1.1 GEOGEBRA: De symmetrieën van een regelmatige tetraëder

De symmetrieën van een 3d-figuur bepalen is niet makkelijk. Daarom maken we gebruik van een GeoGebra applet. Surf naar <https://www.geogebra.org/m/jcdephhn>.

Op de applet staat links een lijst met verschillende objecten die tevoorschijn komen door de tabbladen uit te klappen. Je kan verschillende objecten in de lijst aan en uit zetten door op het de bolletjes voor de objecten te klikken. **Zorg dat objecten 'Tetra' en 'TetraR' geselecteerd staan.**

Rechts kan je de geselecteerde objecten bestuderen. Je kan in- en uitzoomen door te scrollen en als je je muis ingedrukt houdt, kan je de objecten roteren. Gebruik dit om de objecten goed te kunnen bestuderen. **Als je een actie ongedaan wil maken, kan je het commando CTRL + Z gebruiken.**

We gaan op zoek naar alle symmetrieën van de regelmatige tetraëder. Beantwoord de volgende vragen door te experimenteren met de GeoGebra applet.

### Rotatiesymmetrieën

We gaan eerst op zoek naar rotatiesymmetrieën van de tetraëder. Selecteer de rotatieas **a** onder het tabblad 'Line'.

De getekende rechte  $a$  gaat door hoekpunt  $A$  en loodrecht op driehoek  $\triangle BCD$ . Merk op dat de rechte  $a$  door het zwaartepunt van de driehoek gaat. We roteren de tetraëder rond deze rechte. Selecteer hiervoor slider **Hoek** onder het tabblad 'Angle' en druk op play, voer zelf enkele hoekgroottes in of gebruik de pijltjestoetsen. Over hoeveel graden moet je draaien om een symmetrie van de tetraëder te krijgen?  $0^\circ$ ,  $120^\circ$  of  $240^\circ$ .

Beschrijf de verschillende symmetrieën (transformaties) van de figuur die je verkrijgt door te roteren over deze rotatieas  $a$ .

Vermeld ook waar ieder hoekpunt naar getransformeerd wordt via de cykelnotatie.

De rotatie rond rechte  $a$  over  $120^\circ$  met cykelnotatie  $(BCD)$ , want hoekpunt  $A$  wordt op zichzelf afgebeeld en de hoekpunten  $B, C$  en  $D$  verplaatsen onderling.

De rotatie rond  $a$  over  $240^\circ$  met cykelnotatie  $(BDC)$ .

⚠ Vergeet ook niet de rotatie rond  $a$  over  $360^\circ$  (of  $0^\circ$ ) met cykelnotatie  $()$ .

Zijn er nog andere rechten door hoekpunten die als rotatieas van een symmetrie fungeren? Beschrijf deze nauwkeurig.

De rechte door hoekpunt  $B$  en loodrecht op  $\triangle ACD$ .

De rechte door hoekpunt  $C$  en loodrecht op  $\triangle ABD$ .

De rechte door hoekpunt  $D$  en loodrecht op  $\triangle ABC$ .

Hoeveel symmetrieën van de figuur heb je op deze manier gevonden?

We hebben 4 rotatieassen gevonden en er zijn 3 rotaties rond elke as die ook symmetrieën zijn, maar de identieke rotatie van  $0^\circ$  mogen we slechts één keer meetellen!

Er zijn dus 9 symmetrieën van de figuur die we verkrijgen door de figuur te roteren over een rechte door een hoekpunt.

We hebben nog niet alle rotatiesymmetrieën gevonden. We kunnen namelijk ook roteren over rechte die niet door een hoekpunt gaan.

Deselecteer **TetraR** en **a** en zet de slider terug op  $0^\circ$ .

Selecteer rotatieas **b**.

De getekende rechte  $b$  gaat door het midden van zijde  $AB$  en het midden van zijde  $CD$ .

Selecteer **TetraS**. Onder het tabblad 'Number' kan je bij het object **Perspectief** zelf een waarde intypen. Typ het volgende commando: **SetViewDirection(vector(E,F))** en druk op 'enter'. We bekijken de figuur nu vanuit een ander perspectief. We kijken volgens rechte  $b$ , want  $E$  is het midden van  $AB$  en  $F$  is het midden van  $CD$ . Op ons scherm is de rechte  $b$  nu één punt. Gebruik opnieuw slider **Hoek** en druk op play of voer zelf enkele hoekgroottes in om te roteren over rechte  $b$ .

Vanuit dit perspectief lijkt het alsof er 4 rotatiesymmetrieën bestaan rond deze rotatieas. Namelijk de rotaties over 0, 90, 180 en 270 graden.

Typ onder **Perspectief** het commando: **SetViewDirection()** en druk op 'enter'. We bekijken de figuur nu vanuit het origineel perspectief. Nu zien we dat enkel de rotaties over 0 en 180 graden symmetrieën zijn.

Beschrijf wat de rotatie over  $180^\circ$  met de hoekpunten doet in cykelnotatie.

De cykelnotatie is  $(AB)(CD)$ .

De andere twee rotaties zijn geen symmetrieën van de figuur. Je hebt vast en zeker opgemerkt dat bij deze transformaties de beeldfiguur precies een tetraëder is die ondersteboven staat. We zullen deze dan ook later nog nodig hebben.

Deselecteer **TetraS**. Het commando 'reflect' in GeoGebra spiegelt een object. Als je **TetraS2** selecteert, zie je het beeld na de spiegeling van de tetraëder over  $b$ . Na de spiegeling uit te voeren, stellen we vast dat de spiegeling een symmetrie van de figuur is. Beschrijf naar waar je de hoekpunten hebt gespiegeld in cykelnotatie.

De cykelnotatie is  $(AB)(CD)$ . Dit is dus hetzelfde als roteren over  $180^\circ$  rond de spiegellijn.

⚠ Eigenlijk zijn spiegelingen over een rechte dus rotaties over  $180^\circ$  rond deze rechte.

Zijn er nog andere rechten waarrond roteren over  $180^\circ$  een symmetrie van de figuur oplevert? Beschrijf deze nauwkeurig.

Ja, de rechte door het midden van  $BC$  en  $AD$ .

De rechte door het midden van  $AC$  en  $BD$ .

Hoeveel (nieuwe) symmetrieën van de figuur heb je gevonden?  
Hoeveel rotatiesymmetrieën zijn er dus in totaal?

Er zijn 3 nieuwe rotatiesymmetrieën gevonden. Aangezien dit eigenlijk ook rotaties zijn, zijn er in totaal 12 rotatiesymmetrieën.

### Spiegelsymmetrieën

Spiegelsymmetrieën zijn symmetrieën die we verkrijgen door te spiegelen om een vlak. We gaan op zoek naar de spiegelsymmetrieën van de tetraëder. Deselecteer de objecten **Spiegelijn**, **TetraS** en **TetraS2** en selecteer het vlak **Alpha** ( $\alpha$ ) onder tabblad **Plane**. In dit vlak liggen de volledige zijde  $AB$  en het midden van zijde  $CD$ .

Als je **TetraV** selecteert, zie je het beeld na de spiegeling van de tetraëder over  $\alpha$ . Na de spiegeling uit te voeren, stellen we vast dat de spiegeling een symmetrie van de figuur is. Beschrijf wat de transformatie met de hoekpunten doet in cykelnotatie.

De cykelnotatie is  $(CD)$ .

Zijn er nog andere vlakken waarover we kunnen spiegelen zo dat de spiegeling een symmetrie van de figuur is? Beschrijf deze nauwkeurig en leg uit hoe je aan het aantal komt.

Hoeveel (nieuwe) symmetrieën van de figuur heb je gevonden?  
Er zijn 6 vlakspiegelingen die symmetrieën van de figuur voorstellen.

De tetraëder heeft 6 ribben. We kunnen dus 6 vlakken construeren die allemaal door een ribbe en het midden van de overstaande ribbe gaan. Voorbeelden van vlakken die je op deze manier kan construeren zijn het vlak door zijde  $AC$  en het midden van zijde  $BD$  en het vlak door zijde  $CD$  en het midden van zijde  $AB$ .

### Rotatiespiegelsymmetrieën

We hebben eerder al gesproken over rotaties waarvan de beeldfiguur precies een ondersteboven tetraëder was. Je hebt vast wel opgemerkt dat we met een goed gekozen spiegeling deze ondersteboven tetraëder opnieuw op de oorspronkelijke tetraëder kunnen afbeelden.

Selecteer terug rechte  $b$ , over hoeveel graden moeten we roteren zodat de beeldfiguur een ondersteboven tetraëder is?  $90^\circ$  of  $270^\circ$ .

Selecteer het vlak **Beta** ( $\beta$ ) onder tabblad **Plane**. Dit vlak gaat door de middens van alle ribben van de oorspronkelijke tetraëder waar de rechte  $b$  juist niet door gaat. Namelijk het midden van ribbe  $AC$ , ribbe  $AD$ , ribbe  $BC$  en ribbe  $BD$ .

Het commando 'reflect' in GeoGebra spiegelt een object. Als je **TetraV2** selecteert, zie je het beeld nadat we eerst roteren rond rechte  $b$  en daarna spiegelen over vlak  $\beta$ . Als we bij slider **Hoek**  $90^\circ$  of  $270^\circ$  invullen zien we dat deze combinatie van transformaties een symmetrie is.

\* We gaan beschrijven wat de combinatie van de rotatie rond rechte  $b$  over  $90^\circ$  met de spiegeling over vlak  $\beta$  met hoekpunt  $A$  doet.

We bekijken eerst de rotatie rond rechte  $b$  over  $90^\circ$  (**TetraS**). De beeldfiguur van deze transformatie is een ondersteboven tetraëder en de hoekpunten worden dus **niet** op andere hoekpunten afgebeeld. Via **SetViewDirection(vector(E,F))** lijken de hoekpunten wel op andere hoekpunten afgebeeld. Op welk hoekpunt lijkt, onder dit perspectief hoekpunt  $A$  te worden afgebeeld?  $D$ .

Spiegeling  $\beta$  (**Beta**) zorgt ervoor dat de ondersteboven tetraëder terug recht wordt gespiegeld. Controleer dit in GeoGebra. Dit wil zeggen dat hoekpunt  $A$  nu echt wordt afgebeeld op hoekpunt  $D$ .

Doe hetzelfde voor alle andere hoekpunten. Beschrijf wat de combinatie van transformaties doet met de hoekpunten in cykelnotatie.

De cykelnotatie is  $(ADBC)$ .



Door bepaalde rotaties en spiegelingen te combineren die eigenlijk geen symmetrieën zijn, kunnen we ook nieuwe symmetrieën vinden. Binnen de wiskunde noemen we transformaties die combinaties van een rotatie en een spiegeling zijn, waarbij de rotatieas loodrecht staat op het spiegelvlak, **rotatiespiegelingen**.

Zijn er nog andere rechten waarrond roteren een ondersteboven tetraëder oplevert?

Ja, De rechte door het midden van  $BC$  en  $AD$ .  
De rechte door het midden van  $AC$  en  $BD$ .

We kunnen de ondersteboven tetraëder altijd afbeelden op de oorspronkelijke tetraëder via een spiegeling. Hoeveel (nieuwe) symmetrieën van de figuur heb je gevonden?

Er zijn 3 rechten waarrond we kunnen roteren over  $90^\circ$  en  $270^\circ$  om een ondersteboven tetraëder te krijgen. Deze rechten gaan door het midden van twee verschillende ribben. We vinden dus op 6 manieren een ondersteboven tetraëder. We kunnen vervolgens de ondersteboven tetraëder spiegelen over een het vlak dat door de middens van de vier andere ribben gaat om zo 6 nieuwe symmetrieën van de figuur te vinden.

### Besluit

We vatten eerst alles even samen, hoeveel symmetrieën heeft de regelmatige tetraëder in totaal? Er zijn in totaal 12 rotatiesymmetrieën, 6 spiegelsymmetrieën en 6 rotatiespiegelsymmetrieën. In totaal heeft de regelmatige tetraëder dus 24 symmetrieën.

We hebben ook ontdekt dat we iedere symmetrie kunnen beschrijven door te kijken naar wat er gebeurt met de vier hoekpunten. Met andere woorden, iedere symmetrie van de regelmatige tetraëder bepaalt een permutatie van de vier hoekpunten. Er bestaan in totaal 24 permutaties van vier elementen. Dit wil zeggen dat er maximaal 24 symmetrieën bestaan. We hebben dus alle symmetrieën gevonden.

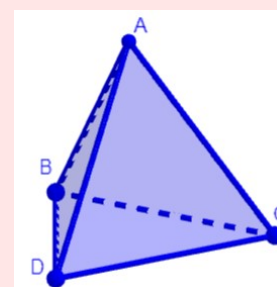
In paragraaf 2.2.2 zagen we al een verzameling die exact alle permutaties van vier elementen bevat. Sterker nog, herinner je dat deze verzamelingen samen met de  $\circ$ -bewerking waarmee we permutaties kunnen combineren zelfs groepen zijn. De permutatiegroep met 24 elementen, noemden we  $(S_4, \circ)$ .

Vul onderstaande samenvatting in samen met de leerkracht.

De symmetriegroep van de regelmatige tetraëder is  $S_4$ , waarbij ieder element een **permutatie** van de hoekpunten voorstelt.

Deze symmetriegroep bevat:

1. 12 Rotatiesymmetrieën.
2. 6 Spiegelsymmetrieën.
3. 6 Rotatiespiegelsymmetrieën.



### 3.1.2 De symmetriegroep van de regelmatige tetraëder

We kunnen de symmetrieën algemeen via permutaties van hoekpunten beschrijven. Hiermee kunnen we namelijk veel makkelijker rekenen.

- 32** Beschrijf nauwkeurig de symmetrieën die horen bij de volgende cycli.

-  $(ABC)$

Dit is een rotatie over  $120^\circ$  rond de rotatieas door  $D$ .

-  $(AC)$

Dit is een spiegeling over het vlak door zijde  $BD$  en het midden van zijde  $AC$ .

-  $(AC)(BD)$

Dit is een rotatie over  $180^\circ$  rond de rechte door het midden van  $BD$  en het midden van zijde  $AC$ .

-  $(ABCD)$

Dit is een rotatiespiegeling met rotatieas de rechte door het midden van ribbe  $AC$  en ribbe  $BD$ , het spiegelvlak is automatisch het vlak door het midden van de vier andere ribben.

— 32

- 33** Schrijf in onderstaande tabel alle permutaties van  $S_4$  (in cykelnotatie) bij de juiste soort symmetrie.

Rotaties (van $120^\circ$ en $240^\circ$ )	$(ABC), (ACB), (BCD), (BDC), (ACD), (ADC), (ABD), (ADB)$
Lijnspiegelingen	$(AB)(CD), (AC)(BD), (AD)(BC)$
Vlakspiegelingen	$(AB), (AC), (AD), (BC), (BD), (CD)$
Rotatiespiegelingen	$(ABCD), (ACBD), (ACDB), (BADC), (BCAD), (BDCA)$

Hoe kan je, zonder te rekenen, zien tot welke soort symmetrie een permutatie behoort?

Alle cycli met hetzelfde aantal letters behoren tot dezelfde soort symmetrie.

— 33

### 3.1.3 Deelgroepen van de symmetriegroep van de regelmatige tetraëder

Zoals de naam al voorspelt is een deelgroep een **groep** die een **deel is van** een andere groep. Een deelverzameling  $H$  van  $G$  die aan de vier groepsaxioma's voldoet onder de bewerking op groep  $G$  is dus een **deelgroep** van  $G$ .

Meetkundig kunnen we deelgroepen vinden door delen van een figuur 'vast te houden' zodat bepaalde symmetrieën niet uitgevoerd kunnen worden.

In de volgende oefening zullen we de top (hoekpunt  $A$ ) vasthouden. Dit heeft als gevolg dat het grondvlak van de regelmatige tetraëder altijd op zijn plaats blijft. We kunnen wel de hoekpunten van het grondvlak onderling verplaatsen, maar niet naar de top van de tetraëder.

- 34** a) Welke symmetrieën kunnen we uitvoeren als we de top (hoekpunt  $A$ ) vast houden? Geef de symmetrieën zowel in woorden als via cykelnotatie van de permutaties.

Alle symmetrieën waarin  $A$  niet voorkomt in de cykelnotatie.

De identieke transformatie, met cykelnotatie  $()$ . Rotaties over  $120^\circ$  en  $240^\circ$  rond de rotatieas door hoekpunt  $A$ , met cykelnotatie  $(BCD)$  en  $(BDC)$ .

Spiegeling over het vlak door zijde  $AB$  en het midden van  $CD$ , met cykelnotatie  $(CD)$ .

Spiegeling over het vlak door zijde  $AC$  en het midden van  $BD$ , met cykelnotatie  $(BD)$ .

Spiegeling over het vlak door zijde  $AD$  en het midden van  $BC$ , met cykelnotatie  $(BC)$ .

Vormen deze symmetrieën samen een groep?

We moeten de vier groepsaxioma's nagaan:

**Associativiteit** geldt want de groepsbewerking  $\circ$  op  $S_4$  is associatief.

Het **identiteitselement** is de identieke transformatie  $()$ , zoals in  $S_4$ . **Geslotenheid** geldt want twee symmetrieën combineren die  $A$  niet verplaatsen, zal opnieuw een symmetrie zijn die  $A$  niet verplaatst. Ieder element heeft een **Invers element**:  $(CD)$ ,  $(BD)$ ,  $(BC)$  en  $()$  zijn hun eigen inverse en  $(BCD)$  en  $(BDC)$  zijn elkaars inverse.

- b) Welke symmetrieën kunnen we uitvoeren als we ribbe  $AB$  vasthouden. Let op,  $A$  en  $B$  onderling mogen, maar moeten niet wisselen met elkaar.

Alle symmetrieën met cykelnotatie waarin  $A$  en  $B$  gewisseld worden of niet voorkomen.

De identieke transformatie met cykelnotatie  $()$ . De spiegeling over de rechte door het midden van zijde  $AB$  en het midden van zijde  $CD$  met cykelnotatie  $(AB)(CD)$ . De spiegeling over het vlak door zijde  $AB$  en het midden van zijde  $CD$ , met cykelnotatie  $(CD)$ . De spiegeling over het vlak door zijde  $CD$  en het midden van zijde  $AB$ , met cykelnotatie  $(AB)$ .

Toon aan dat deze symmetrieën een groep vormen.

We moeten de vier groepsaxioma's nagaan:

**Associativiteit** en het **identiteitselement** gelden om dezelfde reden als in vraag a. **Geslotenheid** geldt want twee symmetrieën combineren die  $A$  en  $B$  onderling wisselen of niet verplaatsen, zal opnieuw een symmetrie zijn die  $A$  en  $B$  niet verplaatst of onderling wisselt. Ieder element is zijn eigen **invers element**, want twee keer spiegelen over dezelfde spiegelas (of vlak) is de identieke transformatie.

## 3.2 Het deelgroepcriterium

We kunnen controleren of  $H$  een groep is door de vier groepsaxioma's na te gaan zoals in de vorige paragraaf. We kunnen ook de vier groepsaxioma's in één eenvoudig criterium samenvoegen. Dit wordt ook wel het **deelgroepcriterium** genoemd.

### Deelgroep

#### Deelgroep

Stel dat  $(G, *)$  een groep is. Als  $H$  een deelverzameling is van de verzameling  $G$  en  $(H, *)$  is een groep, dan noemen we  $(H, *)$  een **deelgroep** van  $(G, *)$ .<sup>a</sup>

#### Het deelgroepcriterium

Een niet-lege deelverzameling  $H$  van de groep  $G$  is een deelgroep als en slechts als

$$\text{voor alle } a, b \in H \text{ geldt dat } a * b^{-1} \in H.$$

<sup>a</sup>Het identiteitselement van  $(G, *)$  en respectievelijk het invers element van  $x \in G$  zijn ook het identiteitselement van  $(H, *)$  en het invers element van  $x \in H$ . Dit bewijzen we niet in deze lessenreeks.

**35** In deze oefening bewijzen we het deelgroepcriterium.

Stel dat  $H$  een deelgroep is van  $G$  onder groepsbewerking  $*$ .

Dan is  $H$  ook een groep en voldoet  $H$  aan de vier groepsaxioma's.

Welke groepsaxioma's op  $H$  hebben we nodig om te zien dat de uitspraak:

voor alle  $a, b \in H$  geldt dat  $a * b^{-1} \in H$ , waar is?

We nemen twee willekeurige elementen  $a$  en  $b$  uit  $H$ . We moeten aantonen dat  $a * b^{-1} \in H$ . Ieder element heeft een invers element dus  $b^{-1}$  bestaat. De geslotenheid van  $H$  wil zeggen dat voor alle  $x_1, x_2 \in H$ :  $x_1 * x_2 \in H$ . Neem  $x_1 = a$  en  $x_2 = b^{-1}$  kiezen, dan voor alle  $a, b \in H$ :  $a * b^{-1} \in H$ .

Het deelgroepcriterium is natuurlijk veel interessanter in de andere richting.

We zullen bewijzen dat, als het deelgroepcriterium geldt, dan  $H$  ook een deelgroep is van  $G$ . Stel dat  $H$  een niet-lege deelverzameling is van groep  $G$  (**dus nog geen groep**) en we weten dat: voor alle  $a, b \in H$  geldt dat  $a * b^{-1} \in H$ . Kan je nu bewijzen dat  $H$  ook een groep is? Tip: Maak gebruik van de eigenschappen van groep  $G$ .

#### Associativiteit

Neem drie willekeurige elementen  $a, b, c \in H$ . We moeten aantonen dat  $(a * b) * c = a * (b * c)$ . Tip: Natuurlijk zijn  $a, b, c$  ook elementen in  $G$ , waar bewerking  $*$  ook op geldt.

Als  $a, b, c \in H$  willekeurig, dan geldt ook  $a, b, c \in G$ . De associativiteit geldt dus voor  $a, b$  en  $c$  of dus  $(a * b) * c = a * b * c = a * (b * c)$ .

#### Identiteitselement

**Stap 1**: Het identiteitselement  $e$  van groep  $G$ , is ook een element in verzameling  $H$ .

Leg uit waarom. Op welke  $a$  en  $b$  uit  $H$  pas je het deelgroepcriterium toe om dit te zien?

Als  $a \in H$ , dan vinden we volgens het deelgroepcriterium dat  $a * a^{-1} = e \in H$ . Merk op dat we zelfs niet nodig hebben dat  $a^{-1} \in H$ .

**Stap 2:** Het identiteitselement van  $G$  is ook het identiteitselement van  $H$ .  
Leg uit waarom. Tip: Opnieuw zijn  $a$  en  $e$  ook elementen van  $G$ .

Als  $a \in H$  en  $e$  het identiteitselement van  $G$  is, dan geldt ook  $a \in G$ . We vinden dan dat  $a * e = a = e * a$ .

### Invers element

We moeten aantonen dat ieder element  $a$  van  $H$  zeker een invers element  $a^{-1}$  heeft binnen groep  $G$ . Leg uit, hoe je het criterium kunt gebruiken om te laten zien dat het element  $a^{-1}$  ook deel van  $H$  is.

Als  $e, a \in H$ , dan  $e * a^{-1} = a^{-1} \in H$ .

### Geslotenheid

Toon de geslotenheid aan. Tip: Maak gebruik van het vorige axioma.

Als  $a, b \in H$ , dan  $a^{-1}, b^{-1} \in H$ , en dus ook volgens het deelgroepcriterium  $a * (b^{-1})^{-1} = a * b \in H$  en  $b * (a^{-1})^{-1} = b * a \in H$ .

$H$  is dus een groep, want  $H$  voldoet aan de vier groepsaxioma's.

Sterker nog  $H$  is een deelgroep van  $G$ , want  $H$  is ook een deelverzameling van  $G$ .

35

Als we in het vervolg moeten controleren of een bepaalde verzameling een deelgroep is van een andere groep, dan doen we dit door het deelgroepcriterium na te gaan.



Iedere groep  $G$  heeft al zeker 2 deelgroepen, namelijk  $\{e\}$  van orde 1 en  $G$  zelf van orde  $\#G$ . We noemen deze de **triviale deelgroepen**.

- 36** Bepaal alle deelgroepen van groep  $D_3$ .  
*De symmetriegroep van de regelmatige driehoek.*

Hieronder zie je de Cayleytabel van  $D_3$ .

$\circ$	$e$	$R$	$R^2$	$S$	$RS$	$R^2S$
$e$	$e$	$R$	$R^2$	$S$	$RS$	$R^2S$
$R$	$R$	$R^2$	$e$	$RS$	$R^2S$	$S$
$R^2$	$R^2$	$e$	$R$	$R^2S$	$S$	$RS$
$S$	$S$	$R^2S$	$RS$	$e$	$R^2$	$R$
$RS$	$RS$	$S$	$R^2S$	$R$	$e$	$R^2$
$R^2S$	$R^2S$	$RS$	$S$	$R^2$	$R$	$e$

Als we zoeken naar **alle** deelgroepen van  $D_3$ , kunnen de triviale deelgroepen natuurlijk niet ontbreken.  $D_3$  heeft dus al zeker twee deelgroepen, namelijk  $\{e\}$  en  $D_3$ .

*Deelgroepen van orde 2.*

Het identiteitselement  $e$  moet altijd deel zijn van de deelgroep. Een deelgroep van orde 2 bevat dus nog precies één ander element  $x$ . De deelgroep is dus  $\{e, x\}$ . We gaan op zoek naar welke elementen we in  $x$  kunnen invullen.

Een groep bevat ook altijd alle inverse elementen, de deelgroep moet dus naast  $x$  ook  $x^{-1}$  bevatten. Waaraan is  $x^{-1}$  dan gelijk?  $x$ . We kunnen nu  $x$  bepalen, kijk bijvoorbeeld in de Cayleytabel.

Hoeveel (en welke) deelgroepen van orde 2 bestaan er?

Controleer het deelgroepcriterium voor één van de deelgroepen die je hebt gevonden.

$D_3$  heeft 3 deelgroepen van orde 2,  $\{e, S\}, \{e, RS\}, \{e, R^2S\}$

Voor verzameling  $\{e, S\}$  geldt het deelgroepcriterium, want  $eS^{-1} = eS = S \in \{e, S\}$ ,  $ee^{-1} = e \in \{e, S\}$ ,  $SS^{-1} = e \in \{e, S\}$  en  $Se^{-1} = S \in \{e, S\}$ .

We kunnen deze deelgroepen ook meetkundig interpreteren. Welk object van de gelijkzijdige driehoek moeten we vasthouden opdat de symmetrieën van de driehoek die we nog kunnen uitvoeren precies een deelgroep van orde 2 vormen?

Iedere deelgroep van orde 2 komt overeen met het vasthouden van één hoekpunt.

*Deelgroepen van orde 3*

Deelgroepen van hogere orde zijn vaak moeilijker te vinden. Hiervoor kunnen we gebruik maken van de Cayleytabel. Verwijder enkele elementen uit groep  $D_3$  (dus rijen en kolommen) van de Cayleytabel en maak zo een gereduceerde tabel.

Kan je een gereduceerde tabel vinden die opnieuw een groep weergeeft?

Tip: er bestaat exact één deelgroep van orde 3.

Duid de gereduceerde tabel aan in bovenstaande tabel.

Alle elementen in de deelgroep van orde 3 zijn rotaties.

Toon aan dat deze groep inderdaad voldoet aan het deelgroepcriterium.

als  $a$  en  $b$  rotaties zijn, dan is  $b^{-1}$  ook een rotatie en  $RS^{-1}$  ook een rotatie. We zien dus dat  $RS^{-1}$  deel is van de deelgroep.

Welke bekende groep (uit hoofdstuk 2) is deze deelgroep van orde 3?

De rotatiegroep van de gelijkzijdige driehoek.

Bestaan er, naast  $D_3$  zelf, nog andere deelgroepen van  $D_3$  met een orde hoger dan 3? Nee, 1 (of 2) rij(en) en kolom(men) uit de Cayleytabel verwijderen geeft ons in dat geval geen deelgroep.

Uit de stelling van Lagrange, die we in de volgende paragraaf ontdekken, zullen we kunnen afleiden dat er geen deelgroepen met een orde hoger dan 3 bestaan.

### 3.3 De stelling van Lagrange

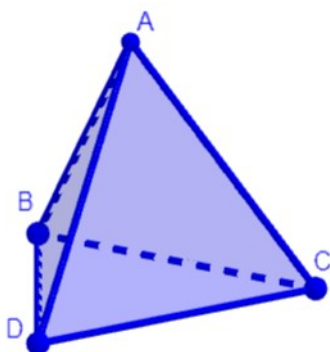
In deze paragraaf bekijken we telstrategieën waarmee we makkelijk alle symmetrieën van een meetkundige figuur kunnen tellen. Daarna sluiten we deze paragraaf af met de stelling van Lagrange, één van de belangrijkste stellingen uit de groepentheorie.

De stelling van Lagrange is een interessante stelling die een verband tussen de ordes van een groep en zijn deelgroepen weergeeft. We kunnen dit verband ontdekken via het tellen van symmetrieën.

#### 3.3.1 Tellen van symmetrieën

We weten al dat er 24 symmetrieën van de regelmatige tetraëder bestaan en dat de groep die alle symmetrieën van de regelmatige tetraëder bevat overeenkomt met  $S_4$ . We hebben dit getal gevonden door alle symmetrieën van de figuur te beschrijven en classificeren. Dit lukt natuurlijk niet meer voor meetkundige figuren met nog meer symmetrieën. We kunnen via slimme telstrategieën het aantal symmetrieën van een meetkundige figuur makkelijk bepalen. We oefenen dit in a.h.v. de regelmatige tetraëder.

- 37** In deze oefening zullen we symmetrieën van de regelmatige tetraëder tellen via telstrategieën.



We hebben al bewezen dat alle symmetrieën die we kunnen uitvoeren door de top  $A$  vast te houden een deelgroep vormen. Deze deelgroep is precies  $S_3$ , alle symmetrieën van het grondvlak.

Wat is  $\text{ord}(S_3)$ ? **6**.

Hoeveel verschillende hoekpunten kunnen we op deze manier vasthouden? **4**.

Wat valt je op als je beide getallen met elkaar vermenigvuldigt?

**$6 \cdot 4 = 24$ , dit is de orde van  $S_4$ , de symmetriegroep van de tetraëder.**

We gaan deze observatie in detail bekijken.

We geven de naam  $H$  aan de symmetriegroep van het grondvlak.  $H$  bevat dus alle permutaties van de drie hoekpunten van het grondvlak ( $B, C$  en  $D$ ) of dus de deelgroep die overeenkomt met de top ( $A$ ) vast te houden zoals in oefening 34a.

Combineer de permutatie die  $A$  op  $B$  transformeert (in cykelnotatie  $(AB)$ ) met **alle** elementen van  $H$  (Bijvoorbeeld:  $(AB) \circ () = (AB)$ ). Zijn deze permutaties samen ook een deelgroep van de symmetriegroep van de regelmatige tetraëder?

**$(AB) \circ () = (AB), (AB) \circ (BC) = (ABC), (AB) \circ (CD) = (AB)(CD),$**

**$(AB) \circ (BD) = (ABD), (AB) \circ (BCD) = (ABCD), (AB) \circ (BDC) = (ABDC).$**

**Dit is geen deelgroep, want het identiteitselement  $()$  is geen deel van de verzameling.**

Dit zijn precies alle symmetrieën die  $B$  op  $A$  afbeelden. De nieuwe verzameling en  $H$  hebben dus geen enkel element gemeenschappelijk.

Combineer nu de transformatie die  $A$  op  $C$  afbeeldt en andersom (in cykelnotatie  $(AC)$ ) opnieuw met alle elementen van  $H$ . Hoeveel elementen hebben  $H$ , de verzameling uit de vorige vraag en deze verzameling gemeenschappelijk?

$(AC) \circ () = (AC)$ ,  $(AC) \circ (BC) = (ACB)$ ,  $(AC) \circ (CD) = (ACD)$ ,  
 $(AC) \circ (BD) = (AC)(BD)$ ,  $(AC) \circ (BCD) = (ACDB)$ ,  $(AC) \circ (BDC) = (ACBD)$ .  
 Deze verzameling heeft niets gemeenschappelijk met de vorige twee.

Een verzameling die bestaat uit de combinatie van een bepaald element (uit de symmetriegroep van de tetraëder) met alle elementen van  $H$  noemen we een **nevenklasse** van  $H$ . De orde van een nevenklasse van  $H$  is altijd gelijk aan de orde van  $H$ . Daarnaast hebben twee nevenklassen geen elementen gemeenschappelijk of, als ze dezelfde verzameling zijn, alle elementen gemeenschappelijk.

Zijn er nog nevenklasse van  $H$  die we hierboven nog niet hebben beschreven?

Ja, de verzameling van alle symmetrieën die  $A$  op  $D$  afbeelden en de verzameling van alle symmetrieën die  $A$  op  $A$  afbeelden.

We kunnen nu de observatie op de vorige pagina verklaren:

We kunnen hoekpunt  $A$  op 3 andere hoekpunten of zichzelf afbeelden. Dit wil zeggen dat  $H$  in totaal 4 nevenklasse heeft. De orde van iedere nevenklasse is gelijk aan 6 en de nevenklasse hebben geen enkel element gemeenschappelijk. De orde van alle nevenklassen samen is dus 24. Alle nevenklassen samen vormen dus precies de symmetriegroep van de regelmatige tetraëder.

— 37

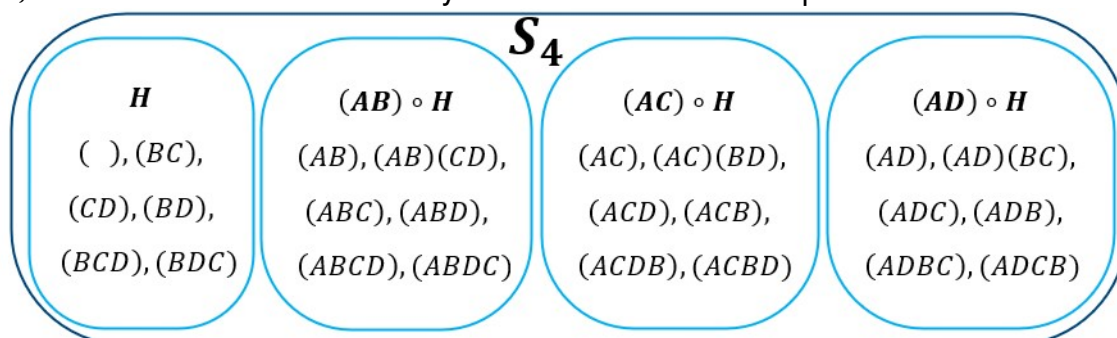
Stel dat  $H$  een deelgroep is van een groep  $G$ . Voor een willekeurig element  $g \in G$ , noemen we de verzameling



$g * H = \{g * h | h \in H\}$  een **linkernevenklasse** van  $H$ .

### Voorbeeld

Als  $H$  de deelgroep is van  $S_4$  uit de vorige oefening, dan is  $(AB) \circ H$  de nevenklasse die alle symmetrieën bevat die  $B$  op  $A$  afbeelden.



- 38** We blijven werken met de symmetriegroep van de regelmatige tetraëder ( $S_4$ ). Wat is de orde van de deelgroep die ontstaat door de ribbe  $AB$  vast te houden (en we  $AB$  onderling wel mogen wisselen) zoals in oefening 34b? **4**.  
We noemen deze deelgroep  $K$ .

Hoeveel ribben kunnen we op deze manier vasthouden? **6**.

Hoeveel nevenklassen heeft verzameling  $K$ ? **6**.

Bereken  $(BC) \circ K$ .

$(BC) \circ K$  heeft 4 elementen, namelijk  $(BC) \circ () = (BC)$ ,  $(BC) \circ (AB) = (BAC)$ ,  $(BC) \circ (CD) = (BCD)$ ,  $(BC) \circ (AB)(CD) = (BACD)$ .

Bereken  $(BAC) \circ K$ .

$(BAC) \circ K$  heeft 4 elementen, namelijk  $(BAC) \circ () = (BAC)$ ,  $(BAC) \circ (AB) = (BC)$ ,  $(BAC) \circ (CD) = (BACD)$ ,  $(BAC) \circ (AB)(CD) = (BCD)$ .

Wat valt je op als je deze twee vergelijkt, kan je dit verklaren?

Beide verzamelingen zijn dezelfde nevenklasse. Als twee nevenklasse één gemeenschappelijk element hebben, moeten ze meteen volledig dezelfde verzameling zijn.

Wat kunnen we besluiten over de orde van alle nevenklassen samen?

$K$  heeft 4 elementen en 6 nevenklasse. Dit wil zeggen dat iedere nevenklasse 4 elementen bevat en dus is de orde van alle nevenklassen samen gelijk aan  $6 \cdot 4 = 24$ . Dit is precies de orde van de volledige groep  $S_4$ .

**Conclusie:** Wat is het verband tussen de orde van de symmetriegroep van de regelmatige tetraëder en de orde van een deelgroep van deze groep?

De orde van een deelgroep (van  $S_4$ ) is een deler van de orde van  $S_4$ .

— 38

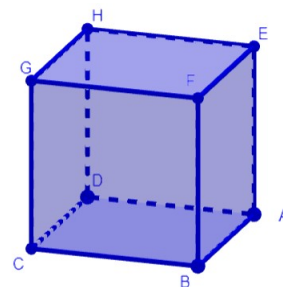
- 39** Wat is de orde van de symmetriegroep van een kubus? Met andere woorden, hoeveel symmetrieën heeft een kubus?

Hoeveel symmetrieën kunnen we uitvoeren wanneer we het grondvlak vasthouden? **8**.

Uit hoeveel vierkanten bestaat deze figuur? **6**.

Hoeveel symmetrieën heeft deze figuur?  **$8 \cdot 6 = 48$** .

Wat is de orde van de symmetriegroep van de kubus? **48**.



— 39

We kunnen nu ook de symmetrieën tellen van heel ingewikkelde figuren.

Probeer zelf eens de symmetrieën te tellen van enkele figuren uit de inleiding van deze lessenreeks (zie oef. 49).

In de volgende paragraaf bespreken we de stelling van Lagrange. Een veralgemening van bovenstaand rekentrucje om symmetrieën te tellen.

## 3.3.2 De stelling van Lagrange

**De stelling van Lagrange**

Zij  $G$  een eindige groep en  $H \subset G$  een deelgroep van  $G$ .

Dan zegt **de stelling van Lagrange** dat de orde van  $H$  een deler is van de orde van  $G$ .

*In symbolen:*

Er bestaat een natuurlijk getal  $n$  zo dat  $\#G = n \cdot \#H$ .

We hebben gezien dat het natuurlijk getal  $n$  precies het aantal nevenklassen van  $H$  voorstelt. Dit getal ( $n$ ) wordt ook wel de **index** van  $H$  in  $G$  genoemd en noteren we als  $[G : H]$  en is dus gelijk aan  $\frac{\#G}{\#H}$ .

Als we de oefeningen over nevenklassen op de vorige pagina veralgemenen hebben we de stelling eigenlijk al bewezen.

**Voorbeeld**

We kunnen deze stelling goed gebruiken als extra controle bij het vinden van deelgroepen. Kijk eens terug naar oefening 36. In  $D_3$  bestaat er sowieso geen (niet-triviale) deelgroep met orde 4 of 5, want 4 en 5 zijn geen delers van  $\#D_4 = 6$ .

- 40** Beschouw de groepen  $S_4$  en  $A_4$ .  
Bestaat er een deelgroep van  $S_4$  met orde 10?  
Zo ja, geef een expliciet voorbeeld, wat is de index van die groep in  $S_4$ ?

**Neen, 10 is geen deler van  $\#S_4 = 24$ .**


Bestaat er een deelgroep van  $S_4$  met orde 6?  
Zo ja, geef een expliciet voorbeeld, wat is de index van die groep in  $S_4$ ?

**Ja, bijvoorbeeld  $S_3$  is een deelgroep van  $S_4$  met orde 6. De index is  $[S_4 : S_3] = \frac{\#S_4}{\#S_3} = \frac{24}{6} = 4$ .**

Bestaat er een deelgroep van  $A_4$  met orde 6?  
Zo ja, geef een expliciet voorbeeld, wat is de index van die groep in  $A_4$ .

**Nee, 6 is wel een deler van  $\#A_4 = 12$ , maar toch bestaat er geen deelgroep. Dit is een voorbeeld van het volgende rode kadertje.**

**Let op!**

-  De stelling van Lagrange zegt **niet** dat als een natuurlijk getal  $m$  een deler van de orde van een groep is, er altijd een deelgroep  $H$  met  $\#H = m$  bestaat.

## 3.4 Oefeningen

### 3.1 & 3.2

41 Beschouw opnieuw de regelmatige tetraëder. Welke symmetrieën kunnen we uitvoeren als we de ribbe  $AB$  vasthouden (en  $A$  en  $B$  onderling **niet** mogen wisselen)?

- a) Beschrijf zowel de symmetrieën in woorden als via cykelnotatie van de permutaties.  
b) Toon aan dat deze symmetrieën een deelgroep vormen van  $S_4$ . — 41

a) De identieke transformatie  $()$  en de spiegeling over het vlak door zijde  $AB$  en het midden van zijde  $CD$ , met cykelnotatie  $(CD)$ .

b) Merk op dat  $(CD) \circ (CD) = ()$ , dus  $(CD)^{-1} = (CD)$ . We zien dat het deelgroepcriterium geldt, want  $()^{-1} \circ (CD) = (CD)$ ,  $(CD)^{-1} \circ () = (CD)$ ,  $(CD)^{-1} \circ (CD) = ()$  en  $()^{-1} \circ () = ()$ .

42 Gebruik het deelgroepcriterium om de volgende vragen te beantwoorden.

a) Is de verzameling van alle even getallen (samen met 0) een deelgroep van  $(\mathbb{Z}, +)$ ?

b) Is de verzameling van alle oneven getallen (samen met 0) een deelgroep van  $(\mathbb{Z}, +)$ ? — 42

a) Ja, we moeten bewijzen dat als  $a$  en  $b$  even getallen, zijn dan is  $a + b^{-1}$  ook even. Merk op dat als  $a$  en  $b$  even zijn, dat  $b^{-1} = -b$  ook even is en  $a + (-b)$  ook (de som van twee even getallen is even).

Bijvoorbeeld  $a = 4, b = 8$ , dan is  $a + b^{-1} = 4 + (-8) = -4$ .

b) Nee, want als  $a$  en  $b$  oneven getallen zijn, dan is  $a + b^{-1} = a + (-b)$  altijd een even getal (tenzij  $a$  of  $b$  gelijk is aan 0). Bijvoorbeeld als  $a = 1$  en  $b = 5$ , dan is  $a + b^{-1} = 1 + (-5) = -4$ .

43 Beschouw opnieuw de quaternionengroep. Dit is de verzameling  $Q = \{1, -1, i, -i, j, -j, k, -k\}$  met de bewerking  $\cdot$  die de volgende rekenregels volgt:

- $(-1) \cdot (-1) = 1$
- Voor alle elementen  $a \in Q$  geldt dat  $(-1) \cdot a = -a = a \cdot (-1)$
- $i \cdot i = j \cdot j = k \cdot k = i \cdot j \cdot k = -1$
- $i \cdot j = -j \cdot i, i \cdot k = -k \cdot i$  en  $j \cdot k = -k \cdot j$

Tip: Kijk nog eens terug naar de Cayleytabel uit oefening 16.

a) Laat zien dat  $A = \{1, -1\}$  een deelgroep is van  $Q$ .

b) Wat is de kleinste deelgroep van  $Q$  die de verzameling  $\{1, i\}$  bevat.

c) Wat is de kleinste deelgroep van  $Q$  die de verzameling  $\{1, i, j\}$  bevat. — 43

a) Dit kunnen we narekenen met het deelgroepcriterium, want het invers element van  $-1$  is  $-1$ . Via het deelgroep criterium zien we dat  $1 \cdot (-1)^{-1} = 1 \cdot (-1) = -1 \in A$ ,  $1 \cdot (1)^{-1} = 1 \in A$ ,  $(-1) \cdot (-1)^{-1} = 1 \in A$  en  $(-1) \cdot (1)^{-1} = -1 \in A$ . Het deelgroepcriterium geldt.

b) We kunnen het deelgroepcriterium gebruiken om de verzameling aan te vullen. Als  $i$  en  $1$  in de deelgroep liggen, dan moet  $1 \cdot i^{-1} = 1 \cdot (-i) = -i$  ook in de deelgroep liggen en dus ook  $i \cdot (-i)^{-1} = i \cdot i = -1$ . Je kan nu nagaan dat de verzameling  $\{1, -1, i, -i\}$  een deelgroep is.

c) We kunnen het deelgroepcriterium gebruiken om de verzameling aan te vullen. Als  $i$  en  $j$  in de deelgroep liggen, dan moet  $j \cdot (i)^{-1} = j \cdot (-i) = -j \cdot i = i \cdot j$  ook in de deelgroep liggen. In hoofdstuk 1 hebben we al uitgerekend dat  $i \cdot j = k$ . Aangezien  $i, j$  en  $k$  in de deelgroep liggen, zien we uit b) dat  $-1, -k, -i$  en  $-j$  ook in de deelgroep moeten liggen. De deelgroep is dus de volledige verzameling  $Q$ .

44 Geef alle deelgroepen van  $S_4$  met orde 2.

— 44

Een deelgroep van orde 2 heeft 2 elementen. We hebben gezien dat dit betekent dat de deelgroep naast het identiteitselement een element bevat dat zichzelf als invers element heeft. De deelgroepen zijn dus:

$\{(), (12)\}$ ,  $\{(), (13)\}$ ,  $\{(), (14)\}$ ,  $\{(), (23)\}$ ,  $\{(), (24)\}$ ,  $\{(), (34)\}$ ,  $\{(), (12)(34)\}$ ,  $\{(), (13)(24)\}$  en  $\{(), (14)(23)\}$ .

45 Stel dat  $m$  en  $n$  willekeurige natuurlijke getallen zijn met  $m < n$ .

a) Bewijs dat  $S_m$  een deelgroep is van  $S_n$ .

\*b) Laat zien dat  $A_n$ , de alternerende groep van  $n$  objecten, een deelgroep is van  $S_n$ .

Tip: gebruik de algemene definitie van een even permutatie.

— 45

a) Een deelgroep is een groep die een deelverzameling is van een andere groep.  $S_m$  is een groep en ook een deelverzameling van  $S_n$ , want alle permutaties van  $m$  elementen zijn ook permutaties van  $n$  elementen. In deze permutaties verplaatsen we de achterste elementen niet.  $S_m$  is dus zeker een deelgroep van  $S_n$ .

b) We moeten laten zien dat het deelgroepcriterium geldt. Als  $a$  en  $b$  even permutaties zijn van  $S_n$ , dan is  $b^{-1} \circ a$  ook een even permutatie.

We controleren eerst dat het inverse van een even permutatie ook een even permutatie is. Een even permutatie bestaat uit een combinatie van een even aantal transposities. De inverse permutatie van een permutatie is de permutatie die alle transposities in precies de omgekeerde volgorde uitvoert. Bijvoorbeeld: Het inverse van  $(12) \circ (23)$  is  $(23) \circ (12)$ . Dit wil zeggen dat het inverse ook uit een even aantal transposities bestaat en dus ook een even permutatie is.

We controleren ook dat de combinatie van twee even permutaties een even permutatie is. Als beide permutaties bestaan uit een even aantal transposities. Dan zal de combinatie ook bestaan uit een even aantal transposities, want een even aantal transposities uitvoeren en daarna nog eens een even aantal transposities uitvoeren is opnieuw een even aantal transposities. Bijvoorbeeld: de combinatie van  $(12) \circ (23)$  na  $(23) \circ (13)$  is  $(12) \circ \underbrace{(23) \circ (23)}_{=e} \circ (13) = (12) \circ (13)$ .

Als het inverse van een even permutatie even is en de combinatie van twee even permutaties ook en we kiezen  $a$  en  $b$  twee even permutaties, dan is  $b^{-1} \circ a$  ook een even permutatie en dus deel van  $A_n$ . Het deelgroepcriterium geldt.

## 3.3

46 Bepaal de index van onderstaande deelgroepen.

- De permutatiegroep  $S_4$  in permutatiegroep  $S_5$ .
- De permutatiegroep  $S_3$  in permutatiegroep  $S_5$ .
- De rotatiegroep van een vierkant, zeg  $R_4$ , in de symmetriegroep van een vierkant.
- De rotatiegroep van een regelmatige  $n$ -hoek, zeg  $R_n$ , in de symmetriegroep van deze  $n$ -hoek  $D_n$ . Is de index afhankelijk van  $n$ ?
- De alternerende permutatiegroep  $A_n$  in permutatiegroep  $S_n$ . Is de index afhankelijk van  $n$ ?

— 46

- a)  $[S_5 : S_4] = \frac{\#S_5}{\#S_4} = \frac{5!}{4!} = \frac{120}{24} = 5$ . b)  $[S_5 : S_3] = \frac{\#S_5}{\#S_3} = \frac{5!}{3!} = \frac{120}{6} = 20$ .  
 c)  $[D_4 : R_4] = \frac{\#D_4}{\#R_4} = \frac{2 \cdot 4}{4} = \frac{8}{4} = 2$ . d)  $[D_n : R_n] = \frac{\#D_n}{\#R_n} = \frac{2 \cdot n}{n} = \frac{2n}{n} = 2$ .  
 e)  $[S_n : A_n] = \frac{\#S_n}{\#A_n} = \frac{n!}{\frac{n!}{2}} = \frac{2n!}{n!} = 2$ .

47 Beschouw opnieuw de quaternionengroep. Dit is de verzameling  $Q = \{1, -1, i, -i, j, -j, k, -k\}$  met de bewerking  $\cdot$  die de volgende rekenregels volgt:

- $(-1) \cdot (-1) = 1$
- Voor alle elementen  $a \in Q$  geldt dat  $(-1) \cdot a = -a = a \cdot (-1)$
- $i \cdot i = j \cdot j = k \cdot k = i \cdot j \cdot k = -1$
- $i \cdot j = -j \cdot i$ ,  $i \cdot k = -k \cdot i$  en  $j \cdot k = -k \cdot j$

Tip: Kijk nog eens terug naar de Cayleytabel uit oefening 16.

- Bereken de nevenklassen van de deelgroep  $\{1, -1, i, -i\}$ .
- Bereken de nevenklassen van de deelgroep  $\{1, -1, j, -j\}$ .
- Bereken de nevenklassen van de deelgroep  $\{1, -1\}$ .

— 47

a) De stelling van Lagrange leert ons dat het aantal nevenklassen gelijk is aan  $\frac{\#Q}{\#\{1, -1, i, -i\}} = \frac{8}{4} = 2$ . De nevenklassen zijn dus  $\{1, -1, i, -i\}$  en  $\{j, -j, k, -k\}$ .

b) De nevenklassen zijn  $\{1, -1, j, -j\}$  en  $\{i, -i, k, -k\}$ . We vinden dus twee nevenklassen.

c) De nevenklassen zijn  $\{1, -1\}$ ,  $\{i, -i\}$ ,  $\{j, -j\}$  en  $\{k, -k\}$ . We vinden dus vier nevenklassen.

48 Een regelmatig achthoek of een octaëder is een meetkundige figuur met 8 zijvlakken in de vorm van gelijkzijdige driehoeken.

- Wat is de orde van de symmetriegroep van deze figuur?
- Alle symmetrieën van één zijvlak van de octaëder vormen een deelgroep van de symmetriegroep van een octaëder. Verklaar in woorden hoe je dit meetkundig kan zien. Hoeveel nevenklassen heeft deze deelgroep?

— 48

a) De deelgroep die bestaat uit alle symmetrieën die we kunnen uitvoeren als we één gelijkzijdige driehoek vasthouden (d.w.z. dat we de drie hoekpunten van deze driehoek enkel onderling mogen wisselen) is exact gelijk aan  $D_3$ , de symmetriegroep van de gelijkzijdige driehoek en heeft dus 6 symmetrieën. Aangezien er 8 andere driehoeken zijn die allemaal hetzelfde patroon volgen, kunnen we via de stelling van Lagrange opmerken dat het totaal aantal symmetrieën gelijk is aan  $6 \cdot 8 = 48$ .

b) We weten al uit a) dat de symmetriegroep van één zijvlak gelijk is aan  $D_3$  en dus 6 symmetrieën heeft. Via de stelling van Lagrange weten we dat deze symmetriegroep  $\frac{48}{6} = 8$  nevenklassen heeft. Een nevenklasse, die niet gelijk is aan  $D_3$ , bevat meetkundig de symmetrieën die ons gekozen zijvlak op een ander zijvlak afbeelden. De nevenklasse die wel gelijk is aan  $D_3$  bevat de symmetrieën die ons gekozen zijvlak op zichzelf afbeelden.

**\*49**

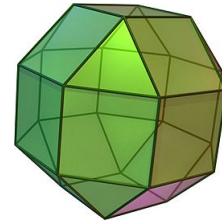
Bepaal de symmetriegroep van onderstaande figuren.

a) Een afgeknotte icosaeëder heeft 32 vlakken waarvan er 20 een zeshoek en 12 een vijfhoek zijn, 60 hoekpunten en 90 ribben. De vijfhoeken grenzen uitsluitend aan zeshoeken, de zeshoeken grenzen om en om aan een vijfhoek en een zeshoek. Dit is precies de meetkundige figuur waarop een klassieke voetbal is gebaseerd.



b) Een **romboëdrische kuboctaëder** is een meetkundige figuur met 26 vlakken waarvan acht gelijkzijdige driehoeken en 18 vierkanten. Ze heeft 24 hoekpunten en 48 ribben.

Opgelet: We kunnen niet alle vierkanten vasthouden op dezelfde manier als we het grondvlak vasthouden. Welke vierkanten wel? (Tip: Zoek naar verschillende patronen)



a) Wanneer we een vijfhoek vasthouden kunnen we tien symmetrieën uitvoeren. Deze symmetrieën vormen samen  $D_5$ , de symmetriegroep van een vijfhoek. Aangezien er 12 andere vijfhoeken zijn die allemaal hetzelfde patroon volgen, omringd door zeshoeken, kunnen we via de stelling van Lagrange opmerken dat het totaal aantal symmetrieën gelijk is aan  $12 * 10 = 120$ .

**Opmerking:** De deelgroep bestaande uit symmetrieën die we kunnen uitvoeren door een vlak vast te houden is niet altijd gelijk aan de symmetriegroep van dit vlak.

De symmetriegroep van een zeshoek is  $D_6$ , maar merk op dat niet alle symmetrieën van  $D_6$  ook symmetrieën zijn van de volledige figuur. Met andere woorden  $D_6$  is **geen** deelgroep van de figuur en kan dus niet gebruikt worden om symmetrieën te tellen. Wanneer we een zeshoek vasthouden, kunnen we nog 6 symmetrieën uitvoeren (3 rotaties en 3 spiegelingen uit  $D_6$ ). Aangezien de figuur bestaat uit 20 zeshoeken vinden we via de stelling van Lagrange  $6 * 20 = 120$  symmetrieën.

b) Wanneer het het grondvlak vasthouden, kunnen we nog 8 symmetrieën uitvoeren. Deze symmetrieën vormen samen  $D_4$ , de symmetriegroep van een vierkant.

De figuur bestaat uit 18 vierkanten, maar niet alle vierkanten volgen hetzelfde patroon als het grondvlak. Het grondvlak is volledig omringd door vierkanten, terwijl het paarse vierkant omringd is door zowel vierkanten als driehoeken. Hierdoor zal de deelgroep bestaande uit alle symmetrieën die we kunnen uitvoeren door het paarse vierkant vast te houden minder dan 8 symmetrieën bevatten en dus niet gelijk zijn aan de symmetriegroep van een vierkant ( $D_4$ ). (Zie ook opmerking bij vraag a).

*Bv: de rotaties over  $90^\circ$  of  $270^\circ$  rond de rotatieas door het zwaartepunt van het paarse vlak zijn geen symmetrieën omdat deze driehoeken op vierkanten afbeelden en omgekeerd!*

In totaal zien we dat 6 vierkanten hetzelfde patroon volgen als het grondvlak. Via de stelling van Lagrange vinden we dan dat de figuur  $8 * 6 = 48$  symmetrieën heeft.

**\*50**

Stel dat  $(G, *)$  een groep is met  $\#G = n$  en  $x \in G$  zodat  $\text{ord}(G) = k$ .

a) Toon aan dat  $H = \{e, x, x^2, \dots, x^{k-1}\}$  een deelgroep is van  $G$ .

b) Gebruik de stelling van Lagrange om een relatie te vinden tussen de orde van een element ( $k$ ) en de orde van een groep ( $n$ ).

a) Merk eerst op dat alle machten van  $x$  elementen zijn van  $H$ . We kunnen ieder geheel getal  $n$  schrijven als de som van een veelvoud van  $k$  en een restterm kleiner dan  $k$ , dus  $n = rk + m$  met  $m < k$ . Nu is  $x^n = x^{rk+m} = x^{rk} * x^m = \underbrace{x^{kr}}_{=e^r} * x^m = e * x^m = x^m$  omdat

$\text{ord}(x) = k$ , moet  $x^k = e$ . Een element  $x^n = x^{rk+m}$  is dus altijd gelijk aan een element  $x^m$  van  $H$ .

We bewijzen dat  $H$  een deelgroep is via het deelgroepcriterium. Dan moeten we bewijzen dat voor willekeurige  $a, b \in H$  geldt  $a * b^{-1} \in H$ . Nu is  $a = x^i$  en  $b = x^j$ , waarbij  $i, j$  natuurlijke getallen zijn kleiner dan  $k - 1$ . We kunnen dan ook  $b^{-1}$  berekenen.  $b^{-1} = x^{k-j}$ , want  $x^j * x^{k-j} = x^{j+k-j} = x^k = e$  en op dezelfde manier  $x^{k-j} * x^j = e$ . We kunnen nu  $a * b^{-1}$  berekenen.  $a * b^{-1} = x^i * x^{k-j} = x^{i+k-j}$ . Dit element ligt inderdaad in  $H$ .

b) De stelling van Lagrange zegt dat de orde van een deelgroep  $H$  van groep  $G$  een deler is van de orde van  $G$ . Nu is  $\#H = k$  een deler van  $\#G = n$ , maar  $k$  was ook de orde van een element van  $G$ . Dit wil zeggen dat de orde van een element in een groep **altijd** een deler is van de orde van de groep.

# Uitbreiding

## 2.3 Cyclische groepen

Een derde soort groepen zijn de cyclische groepen. In de volgende oefening is een cyclische groep beschreven.

- 1 Beschouw de verzameling  $G = \{g, g^2, g^3, \dots, g^6\}$ , met de volgende rekenregels:
- $g^{6+k} = g^k = g^{k+6}$ , voor willekeurige  $k \in \mathbb{Z}$ .
  - $g^k * g^m = g^{k+m}$ , voor willekeurige  $k, m \in \mathbb{Z}$ .

Bijvoorbeeld:  $g^9 = g^{6+3} = g^3$  en  $g^{-2} = g^{6+(-2)} = g^4$ .

Heeft  $G$  een identiteitselement voor deze bewerking?

Ja,  $g^6$ . Als  $g^k$  een willekeurige element van  $G$  is, dan  $g^6 * g^k = g^{6+k} = g^k$ . Je kan zo ook bewijzen dat  $g^k * g^6 = g^k$ .

Toon aan dat  $(G, *)$  een groep is.

Kies willekeurig  $k, l, m \in \mathbb{Z}$ .

Geslotenheid:  $g^k * g^m = g^{k+m}$  en dit is opnieuw een element van  $G$ .

Associativiteit:  $(g^k * g^m) * g^n = g^{k+m} * g^n = g^{k+m+n}$  en  $g^k * (g^m * g^n) = g^k * g^{m+n} = g^{k+m+n}$ .

Identiteitselement: Het identiteitselement is  $g^6$ .

Invers element:  $g^k * g^{6+(-k)} = g^{k+6+(-k)} = g^6 = g^{6+(-k)+k} = g^{6-k} * g^k$ .

— 1

### Cyclische groepen

Een **cyclische groep** is een groep die kan voortgebracht worden door één element. Een cyclische groep  $G$  ziet er als volgt uit:

$$G = \{e, g, g^2, \dots, g^{n-1}\},$$

waarbij  $g^n = e$ . De orde van de groep is  $n$ .

Het element  $g$  noemen we de **voortbrenger** van de groep, want we kunnen ieder element  $g^k$  uit  $G$  schrijven als  $g^k = \underbrace{g * g * g * \dots}_{k \text{ keer}}$ .

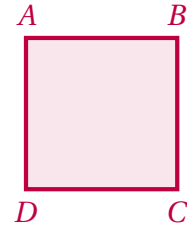
We noteren ook wel  $G = \langle g \rangle$ , waarbij  $g$  een voortbrenger is van groep  $G$  onder de groepsbewerking.

⚠ De voortbrenger is niet noodzakelijk uniek! Dit zullen we ontdekken in het volgende voorbeeld.

**Voorbeeld**

Rotatiegroepen van regelmatige veelhoeken zijn cyclische groepen. Deze groepen zijn van de vorm  $\{e, R, R^2, \dots, R^n\}$ , waarbij  $R$  een rotatie is over  $360/n$  graden. Je kan duidelijk zien dat  $R$  een voortbrenger is van de groep.

De rotatiegroep van een vierkant bestaat uit 4 elementen: de rotaties over  $90^\circ, 180^\circ, 270^\circ$  en  $360^\circ (= 0^\circ)$ . Dit is een cyclische groep, want de rotatie over  $90^\circ$  is een voortbrenger van de groep. De combinatie van twee keer roteren over  $90^\circ$ , is hetzelfde als roteren over  $180^\circ$  en de combinatie van drie keer roteren over  $90^\circ$ , is hetzelfde als roteren over  $270^\circ$ . Op deze manier kunnen we alle rotaties schrijven als combinaties van de rotatie over  $90^\circ$ . In symbolen is de rotatiegroep dus  $\{R, R^2, R^3, e\}$ , waarbij  $R$  de rotatie van  $90^\circ$  voorstelt.



De rotatie over  $90^\circ$  ( $R$ ) is niet de enige voortbrenger van de rotatiegroep. De rotatie over  $270^\circ$  ( $R^3$ ) is ook een voortbrenger van deze groep, want de combinatie van twee keer roteren over  $270^\circ$ , is hetzelfde als roteren over  $540^\circ$ . Een rotatie over  $540^\circ$  is natuurlijk een rotatie over  $180^\circ (= 540^\circ - 360^\circ)$ . Zo kan je verder rekenen en alle rotaties schrijven als combinaties van de rotatie over  $270^\circ$ . Bereken dit eens zelf!

Tenslotte kunnen we opmerken dat de rotatie over  $180^\circ$  ( $R^2$ ) **geen** voortbrenger is van deze rotatiegroep. Als we meerdere keren over  $180^\circ$  draaien, komen we altijd uit op  $180^\circ$  of  $360^\circ$ . We kunnen dus nooit een rotatie over  $90^\circ$  of  $270^\circ$  uitvoeren door meerdere keren over  $180^\circ$  te roteren.

- 2 Beschouw opnieuw groep  $G = \{g, g^2, \dots, g^6\}$ .  
Welke elementen zijn voortbrengers van deze groep?

De voortbrengers zijn  $g$  en  $g^5$ .

Wat is de grootste gemeenschappelijke deler van de exponenten van de voortbrengers met de orde van de groep?

De grootste gemeenschappelijke deler van deze exponenten met de orde van de groep (6) is gelijk aan 1.

## 2.4 Restklassegroepen

We starten met een voorbeeld en definitie voor het begrip restklasse.

### Voorbeeld

Op een analoge klok staan de uren aangegeven van 1 tot en met 12.

Stel dat het 7 uur is, dan kunnen we ons afvragen op welk cijfer de klok 8 uur later staat. Iedereen weet natuurlijk dat het antwoord op deze vraag 3 uur is, want  $7 + 8 = 15$  en op een analoge klok staat de kleine wijzer dus op 3 uur.

In dit voorbeeld hebben we modulair gerekend. Het resultaat van een berekening modulo 12 is de rest van het resultaat na geheeltallige deling door de modulus 12. Als we 15 staartdelen door 12, blijft er een rest 3 over of  $15 - 12 = 3$ .

### Modulair rekenen

**Modulair rekenen** is een vorm van rekenen met gehele getallen, waarbij we een bovengrens opleggen. Deze bovengrens noemen we de **modulus**.

Het resultaat van een berekening modulo  $m$  is de rest van het resultaat na geheeltallige deling door de modulus  $m$ .

Twee getallen die modulo  $m$  gelijk zijn noemen we **congruent** en we noteren dit met  $\equiv$ . Bijvoorbeeld:  $7 \equiv 2 \pmod{5}$ .

We rekenen dus eigenlijk met de getallen van 0 tot en met  $m - 1$ . We kunnen getallen modulo  $m$  zowel optellen (en aftrekken) als vermenigvuldigen (en delen). Dit betekent dat

$$(a \pmod{m}) + (b \pmod{m}) = (a + b) \pmod{m},$$

$$(a \pmod{m}) \cdot (b \pmod{m}) = (a \cdot b) \pmod{m}.$$

We noemen de verzameling die de getallen 0 tot en met  $m - 1$  bevat, de **restklasse** van  $m$  en noteren we met  $\mathbb{Z}/m\mathbb{Z}$ .

**3** Bereken de volgende wiskundige uitdrukkingen.

-  $(1 \pmod{2}) + (1 \pmod{2})$

$(1 \pmod{2}) + (1 \pmod{2}) = (1 + 1) \pmod{2} = 2 \pmod{2} \equiv 0 \pmod{2}.$

-  $(3 \pmod{7}) + (6 \pmod{7})$

$(3 \pmod{7}) + (6 \pmod{7}) = (3 + 6) \pmod{7} = 9 \pmod{7} \equiv 2 \pmod{7}.$

-  $(36 \pmod{13}) + (16 \pmod{13})$

$(36 \pmod{13}) + (16 \pmod{13}) = (36 + 16) \pmod{13} = 52 \pmod{13} \equiv 0 \pmod{13}.$

4 Bereken de volgende wiskundige uitdrukkingen.

$$- (1 \bmod 2) \cdot (1 \bmod 2)$$

$$(1 \bmod 2) \cdot (1 \bmod 2) = (1 \cdot 1) \bmod 2 = 1 \bmod 2.$$

$$- (3 \bmod 7) \cdot (6 \bmod 7)$$

$$(3 \bmod 7) \cdot (6 \bmod 7) = (3 \cdot 6) \bmod 7 = 18 \bmod 7 \equiv 4 \bmod 7.$$

$$- (36 \bmod 13) \cdot (16 \bmod 13)$$

$$(36 \bmod 13) \cdot (16 \bmod 13) = (36 \cdot 16) \bmod 13 = 576 \bmod 13 \equiv 4 \bmod 13.$$

— 4



Modulair rekenen is erg belangrijk binnen wiskunde en kent nog heel erg veel toepassingen en eigenschappen, maar in deze lessenreeks groepentheorie focussen we enkel op het rekenen zelf.

5 Toon aan dat voor een willekeurige  $m$ ,  $(\mathbb{Z}/m\mathbb{Z}, +)$  een groep is.

Voor willekeurige  $a, b, c \in \mathbb{Z}/m\mathbb{Z}$  gelden de volgende axioma's:

Associativiteit:  $[(a \bmod m) + (b \bmod m)] + (c \bmod m) = [(a + b) \bmod m] + (c \bmod m) = (a + b + c) \bmod m = (a \bmod m) + [(b + c) \bmod m] = (a \bmod m) + [(b \bmod m) + (c \bmod m)]$

Geslotenheid:  $(a \bmod m) + (b \bmod m) = (a + b) \bmod m \in \mathbb{Z}/m\mathbb{Z}$ .

Identiteitselement:  $0 \bmod m$  is het identiteitselement, want  $(0 \bmod m) + (a \bmod m) = a \bmod m = (a \bmod m) + (0 \bmod m)$ .

Invers element:  $-a \equiv m - a \bmod m$  is het invers element van  $a \bmod m$ , want  $(a \bmod m) + (m - a \bmod m) = m \equiv 0 \bmod m = (m - a \bmod m) + (a \bmod m)$ .

— 5

6 Is  $(\mathbb{Z}/m\mathbb{Z}, \cdot)$  een groep? De associativiteit en geslotenheid volgen uit de definitie van het modulair rekenen zoals in de vorige oefening. Toch is  $(\mathbb{Z}/m\mathbb{Z}, \cdot)$  nooit een groep. Waarom niet?

Tip: Bij het element  $0 \bmod m$  loopt het mis.

We zouden verwachten dat  $1 \bmod m$  het identiteitselement is, want voor alle  $a \neq 0$  geldt,  $(a \bmod m) \cdot (1 \bmod m) = a \bmod m = (1 \bmod m) \cdot (a \bmod m)$ . Nu heeft  $0 \bmod m$  geen inverse, want er bestaat geen enkel getal dat we kunnen vermenigvuldigen met 0 zodat we  $1 \bmod m$  uitkomen.

Laten we nu de restklasse van  $m$  zonder het element  $0 \bmod m$  beschouwen.

We noteren deze verzameling als  $(\mathbb{Z}/m\mathbb{Z})_0$ . Is  $((\mathbb{Z}/7\mathbb{Z})_0, \cdot)$  een groep?

Wat is het identiteitselement? Zoek voor ieder element het invers element.

Het invers element van 1 is 1. 2 en 4 zijn invers aan elkaar, want  $2 * 4 = 8 \equiv 1 \bmod 7$ . 3 en 5 zijn invers aan elkaar, want  $3 * 5 = 15 \equiv 1 \bmod 7$ . Het invers element van 6 is 6, want  $6 * 6 = 36 \equiv 1 \bmod 7$ .

Is  $((\mathbb{Z}/8\mathbb{Z})_0, \cdot)$  een groep?

Wat is het identiteitselement? Zoek voor ieder element een invers element.

Nee, de elementen 2, 4 en 6 hebben geen invers element.

Daarnaast is de verzameling ook niet gesloten, want  $2 * 4 = 8 \equiv 0 \pmod{8}$  en  $0 \pmod{8} \notin (\mathbb{Z}/8\mathbb{Z})_0$ .

\* Voor welke getallen  $m$  is  $((\mathbb{Z}/m\mathbb{Z})_0, \cdot)$  een groep?

Als  $m$  een priemgetal is, is  $((\mathbb{Z}/m\mathbb{Z})_0, \cdot)$  een groep.

— 6

### Restklassegroepen

De restklasse van een getal  $m$  is een groep onder de optelling. We noteren dit met  $(\mathbb{Z}/m\mathbb{Z}, +)$ . Merk op dat  $\#(\mathbb{Z}/m\mathbb{Z}) = m$ .

De restklasse van een getal  $m$  is nooit een groep onder de vermenigvuldiging, maar als  $m$  een priemgetal is, dan is de restklasse zonder het element  $0 \pmod{m}$  onder de vermenigvuldiging een groep van orde  $m - 1$ .

We noteren deze groep als  $((\mathbb{Z}/m\mathbb{Z})_0, \cdot)$  met  $\#(\mathbb{Z}/m\mathbb{Z})_0 = m - 1$ .

Inderdaad, als  $m$  een priemgetal is, dan zal de vermenigvuldiging van twee elementen uit de restklasse nooit een veelvoud van  $m$  zijn en dus nooit congruent aan  $0 \pmod{m}$ .

- 7 Is  $(\mathbb{Z}/m\mathbb{Z}, +)$  een cyclische groep? Geef een generator of een tegenvoorbeeld. Kijk eens terug naar hoofdstuk 2.3. Hoe kunnen we makkelijk alle generatoren vinden.

Ja, want het getal 1 is een generator van de groep.

De generatoren van deze groep zijn alle getallen waarvan de grootste gemeenschappelijke deler met  $m$  gelijk is aan 1.

— 7

- 8 Bepaal de orde van elk element in de groep  $((\mathbb{Z}/7\mathbb{Z})_0, \cdot)$ .

$\text{ord}(1) = 1, \text{ord}(2) = 3, \text{ord}(3) = 6, \text{ord}(4) = 3, \text{ord}(5) = 6, \text{ord}(6) = 2$ .

Is dit een cyclische groep? Geef alle generatoren indien dit een cyclische groep is.

De generatoren zijn 3 en 5.

— 8

### Oefeningen (HF2)

- 9 Geef alle generatoren van  $G = \langle g \rangle$ , waarbij  $G$  een cyclische groep is van orde 10.

— 9

De generatoren zijn  $g, g^3, g^7$ . Je kan dit zelf narekenen of inzien dat  $g^n$  een generator is als de kleinste gemene deler van  $n$  en 10 gelijk is aan 1.

- 10** Geef alle generatoren van de cyclische groep  $(\mathbb{Z}/15\mathbb{Z}, +)$ . — 10

De generatoren zijn 1, 2, 4, 6, 7, 8, 11, 13, 14. Je kan dit zelf narekenen (veel werk) of inzien dat een getal een generator is als de kleinste gemene deler van het getal en 15 gelijk is aan 1.

- 11** Is  $(\mathbb{Z}/143\mathbb{Z})_0, \cdot$  een groep? Waarom wel/niet? — 11

Deze verzameling is een groep onder de vermenigvuldiging als 143 een priemgetal is. Dit is niet zo want  $11 \cdot 13 = 143$ .

### Oefeningen (HF3)

- 12** Wat is de kleinste deelgroep van  $G = \langle g \rangle$ , waarbij  $G$  een cyclische groep is van orde 18 die:  
a) de verzameling  $X = \{e, g^3\}$  bevat.  
b) de verzameling  $Y = \{e, g^6\}$  bevat. — 12

a) We kunnen deze verzameling aanvullen met behulp van het deelgroepcriterium. Als de deelgroep  $e$  en  $g^3$  moet bevatten, dan ook  $e * (g^3)^{-1} = g^{18-3} = g^{15}$ . We kunnen nu makkelijk alle andere elementen vinden. Als  $g^3$  en  $g^{15}$  deel zijn van de deelgroep, dan is ook  $g^3 * (g^{15})^{-1} = g^3 * g^3 = g^{3+3} = g^6$ . Werk op dezelfde manier verder om alle andere elementen van de deelgroep te vinden.

De kleinste deelgroep die  $X$  bevat is  $\{e, g^3, g^6, g^9, g^{12}, g^{15}\}$ , dit zijn alle veelvouden van 3.

b) In a) hebben we ontdekt dat de deelgroep bestaat uit alle veelvouden van 6. De kleinste deelgroep die  $Y$  bevat is  $\{e, g^6, g^{12}\}$ . Je kan dit ook opnieuw narekenen via het deelgroepcriterium.

- \*13** Bepaal alle deelgroepen van  $(\mathbb{Z}/7\mathbb{Z}, +)$  en hun index. — 13

$(\mathbb{Z}/7\mathbb{Z}, +)$  heeft al zeker 2 triviale deelgroepen, de deelgroep met index 7 (de verzameling die enkel het identiteitselement bevat) en de deelgroep met index 1 (de volledige groep).

Je kan zelf narekenen dat  $(\mathbb{Z}/7\mathbb{Z}, +)$  geen enkele andere deelgroep heeft, want alle elementen zijn generatoren voor de groep.

Dit komt omdat 7 een priemgetal is en dus het kleinst gemeenschappelijke veelvoud van een getal kleiner dan 7 met 7 gelijk is aan 1.

- \*14** Bepaal alle deelgroepen van  $((\mathbb{Z}/7\mathbb{Z})_0, \cdot)$  en hun index. — 14

$((\mathbb{Z}/7\mathbb{Z})_0, \cdot)$  heeft al zeker 2 triviale deelgroepen, de deelgroep met index 6 (de verzameling die enkel het identiteitselement bevat) en de deelgroep met index 1 (de volledige groep).

Je kan zelf narekenen dat  $\{1 \pmod{7}, 6 \pmod{7}\}$  en  $\{1 \pmod{7}, 2 \pmod{7}, 4 \pmod{7}\}$  de enige andere deelgroepen van  $((\mathbb{Z}/7\mathbb{Z})_0, \cdot)$  zijn.