



Inleiding Groepentheorie

lieven le bruyn

Overzicht

- [Inhoudsopgave](#)
- [Begin Artikel](#)

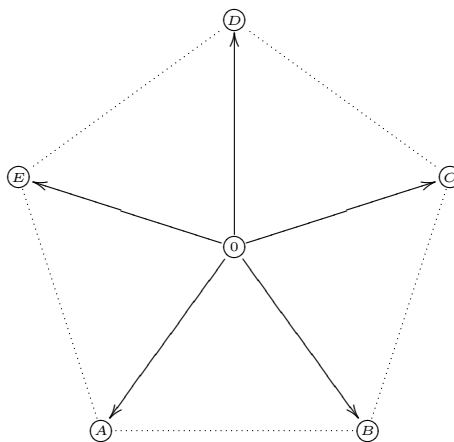
Inhoudsopgave

- 1.. Groepen en symmetrie**
- 2.. De stelling van Cayley (1854)**
- 3.. Normaaldivisoren en quotiënten**
- 4.. De stelling van Lagrange (1770)**
- 5.. De kleinste groepen**
- 6.. De 14-15 puzzel**
- 7.. De stelling van Cauchy (1846)**
- 8.. Microsudoku**
- 9.. De stelling van Jordan-Hölder (1889)**
- 10.. Galois groepen**
- 11.. De stellingen van Sylow (1872)**
- 12.. De Rubik kubus**
- 13.. Alle groepen van orde ≤ 30**

Oplossingen van de Opgaven

1. GROEPEN EN SYMMETRIE

OPGAVE 1. Een oefening uit de 4de LWi : bekijk de vectoren in het vlak gegeven door de hoekpunten van een regelmatige 5-hoek



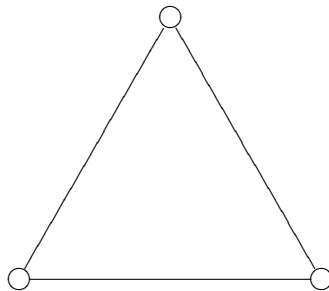
Toon aan dat de vectoriële som van deze vectoren

$$\vec{A} + \vec{B} + \vec{C} + \vec{D} + \vec{E} = \vec{0}$$

de nulvector is.

Natuurlijk is er niets speciaal aan de regelmatige *vijf*hoek en kunnen we het argument herhalen voor iedere regelmatige n -hoek. We willen alle symmetrieën van het vlak bepalen die een regelmatige n -hoek in zichzelf voeren. Merk op dat als je twee zulke symmetrieën f en g hebt dat dan ook hun *samenstelling* $g \circ f$ (lees : g na f) een symmetrie van de regelmatige n -hoek is.

OPGAVE 2. Bepaal alle vlakke symmetrieën van een regelmatige 3-hoek



en ga na hoe de samenstelling op koppels van symmetrieën werkt.

OPGAVE 3. Welke symmetrie is de samenstelling van twee vlakke rotaties met hetzelfde centrum?

Welke symmetrie is de samenstelling van twee spiegelingen van het vlak?

Als r een vlakke rotatie is waarvan het centrum ligt op de spiegelas van een spiegeling s , welke symmetrie is dan de samenstelling $r \circ s$ en welke symmetrie is de samenstelling $s \circ r$?

De samenstelling van vlakke symmetrieën is opnieuw een symmetrie en is *associatief*. Hiermee bedoelen we dat voor alle vlakke symmetrieën f, g en h geldt dat

$$(f \circ g) \circ h = f \circ (g \circ h)$$

Dus, de symmetrie verkregen door eerst h te doen en daarop $f \circ g$ te doen is dezelfde als die verkregen door eerst $g \circ h$ te doen en daarop nog eens f los te laten.

Verder is het duidelijk dat samenstellen met de *identiteits* symmetrie i niets verandert aan een vlakke symmetrie f , met andere woorden

$$i \circ f = f = f \circ i$$

Tenslotte heeft ook iedere vlakke symmetrie f een *inverse* symmetrie f^{-1} zodat de samenstelling de identiteits-symmetrie geeft

$$f \circ f^{-1} = i = f^{-1} \circ f$$

Bvb. de inverse van een rotatie r is de rotatie r^{-1} met zelfde centrum en rotatie-hoek maar met tegengestelde orientatie. De inverse van een spiegeling s is de spiegeling zelf, dwz. $s^{-1} = s$ want tweemaal spiegelen doet niets.

We gaan nu deze eigenschappen waaraan symmetrie-operaties steeds voldoen formaliseren in een definitie.

Definitie 1 Een **groep** is een verzameling G waarop een bewerking gedefinieerd is

$$G \times G \longrightarrow G \quad (a, b) \mapsto a.b$$

die voldoet aan de volgende voorwaarden :

1. **intern** : voor alle elementen $a, b \in G$ geldt ook dat $a.b \in G$
2. **associatief** : voor alle elementen $a, b, c \in G$ geldt $(a.b).c = a.(b.c)$
3. **eenheidselement** : er bestaat in G een element e zodat voor alle $a \in G$ geldt $e.a = a.e = a$
4. **inverse** : voor alle elementen $a \in G$ bestaat er een invers element $a^{-1} \in G$ zodat $a.a^{-1} = e = a^{-1}.a$.

OPGAVE 4. Toon aan dat een groep G een uniek eenheidselement heeft en dat ieder element $g \in G$ een unieke inverse heeft.

In het geval van de symmetrie-groep van een gelijkzijdige driehoek, onze verzameling is

$$G = \{i, r_1, r_2, s_1, s_2, s_3\}$$

onze groepsbewerking is de samenstelling, dus $\cdot = \circ$ en het eenheidselement is de identiteits-symmetrie, dus $e = i$.

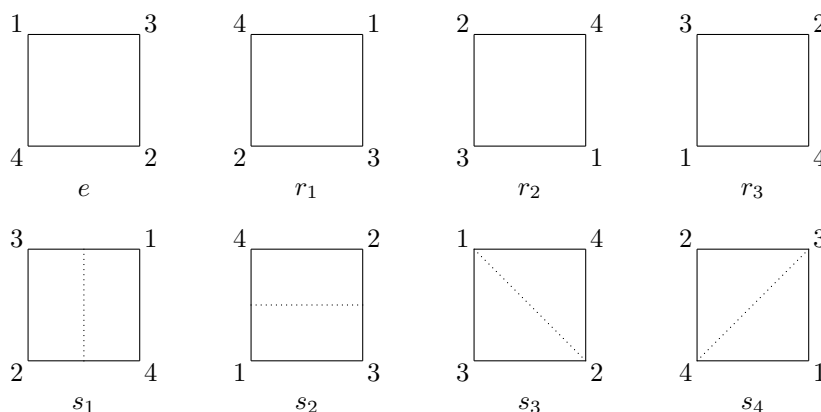
Definitie 2 Een groep G noemen we **eindig** als het aantal elementen van G , genoteerd $\#G$ en genoemd de **orde van** G , eindig is. Een groeps-element $a \in G$ is **van eindige orde** als er een natuurlijk getal $n \in \mathbb{N}$ bestaat zodat

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_n = e$$

waar e het eenheidselement is van G . De minimale waarde n die dit doet noemen we de **orde van** a .

OPGAVE 5. Wat is de orde van de symmetriegroep van een gelijkzijdige driehoek en wat is de orde van elk van zijn elementen?

OPGAVE 6. Een vierkant heeft devolgende 8 symmetrieën. 4 rotaties (inclusief de identiteits-rotatie) met centrum het middelpunt van het vierkant en rotatiehoek een veelvoud van 90° en 4 spiegelingen waarvan de assen ofwel een diagonaal zijn ofwel overstaande zijden in twee delen. We zullen deze symmetrieën als volgt noteren



Bepaal de groep-tabel van deze symmetrie-groep. Dit wil zeggen, maak een tabel zoals voorheen die alle samenstellingen van twee van deze symmetrieën aangeeft. Geef ook de orde van elk van de elementen aan.

OPGAVE 7. Bepaal de orde van de symmetrie-groep van een regelmatige 5-hoek. Veralgemeen dit daarna tot een regelmatige n -hoek.

Definitie 3 Een **deelgroep** H van een groep G met eenheidselement e is een deelverzameling $H \subset G$ zodanig dat H

1. het eenheidselement bevat $e \in H$
2. intern is voor de groepsbewerking, dat is, voor alle $h, h' \in H$ geldt ook $h \cdot h' \in H$
3. gesloten is onder inversen, dus als $h \in H$ dan ook $h^{-1} \in H$

OPGAVE 8. Toon aan dat de deelverzameling R van alle rotatie-symmetrieën van een regelmatige n -hoek (inclusief de identiteit) een deelgroep is van de groep van alle symmetrieën van de n -hoek. Toon ook aan dat de deelverzameling S van alle spiegelingen

(samen met de identiteit) geen deelgroep is van de symmetrie-groep van een regelmatige n -hoek. Vind minstens nog een andere deelgroep van de symmetrie-groep.

Laat ons nogmaals de groep-tabellen bekijken van de symmetrie-groepen van een regelmatige driehoek

$\circ$	i	r_1	r_2	s_1	s_2	s_3
i	i	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	i	s_3	s_1	s_2
r_2	r_2	i	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	i	r_1	r_2
s_2	s_2	s_3	s_1	r_2	i	r_1
s_3	s_3	s_1	s_2	r_1	r_2	i

en van het vierkant

$\circ$	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
e	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	e	s_4	s_3	s_1	s_2
r_2	r_2	r_3	e	r_1	s_2	s_1	s_4	s_3
r_3	r_3	e	r_1	r_2	s_3	s_4	s_2	s_1
s_1	s_1	s_3	s_2	s_4	e	r_2	r_1	r_3
s_2	s_2	s_4	s_1	s_3	r_2	e	r_3	r_1
s_3	s_3	s_2	s_4	s_1	r_3	r_2	e	r_2
s_4	s_4	s_1	s_3	s_2	r_1	r_3	r_2	e

Merk op dat beiden voldoen aan de *Sudoku-eigenschap* : ieder element komt juist eenmaal voor in iedere rij en in elke kolom van de tabel.

Stelling 1 *De groep-tabel van een willekeurige groep voldoet aan de Sudoku-eigenschap.*

Bewijs. Stel dat dit niet het geval is, dan zouden er bvb. in dezelfde rij tweemaal hetzelfde element x moeten voorkomen. Dus, er is zijn elementen f, g en h met $g \neq h$ zodat de groep-tabel er parti el als volgt uitziet

$\cdot$	e	$\dots$	g	$\dots$	$\dots$	h	$\dots$	$\dots$
e	e	$\dots$	g	$\dots$	$\dots$	h	$\dots$	$\dots$
$\vdots$	$\vdots$		$\vdots$			$\vdots$		
$\vdots$	$\vdots$		$\vdots$			$\vdots$		
f	f	$\dots$	x	$\dots$	$\dots$	x	$\dots$	$\dots$
$\vdots$	$\vdots$		$\vdots$			$\vdots$		

Dit wil zeggen, we hebben

$$x = f.g = f.h$$

Nu kunnen we alle termen met f^{-1} links-vermenigvuldigen en krijgen dan

$$f^{-1}.x = f^{-1}.(f.g) = f^{-1}.(f.h)$$

wegens associativiteit zijn de laatste twee termen gelijk aan

$$f^{-1}.x = (f^{-1}.f).g = (f^{-1}.f).h$$

en wegens de eigenschap van het invers element wordt dat

$$f^{-1}.x = e.g = e.h$$

en tenslotte wegens de eigenschap van het eenheids element e

$$f^{-1}.x = g = h$$

En dit is in tegenspraak met de onderstelling dat $g \neq h$. Dus kan er op dezelfde rij nooit tweemaal eenzelfde element voorkomen.

Analoog ook voor kolommen. Stelt dat er in de f -kolom tweemaal eenzelfde y zou voorkomen, dan zouden er verschillende elementen $g \neq h$ in G zijn met

$$y = g.f = h.f$$

Maar dan rechts vermenigvuldigen met f^{-1} en argumenten als boven levert

$$(g.f).f^{-1} = (h.f).f^{-1} \quad \text{en dus} \quad g.(f.f^{-1}) = h.(f.f^{-1}) \quad \text{en dus ook} \quad g.e = h.e$$

waaruit wederom de tegenspraak $g = h$ volgt. $\square$

OPGAVE 9. Als je weet dat een groep G bestaat uit het eenheidselement e , rotaties met zelfde centrum r en r' en vlak-spiegelingen s, s' en s'' . Gebruik wat je weet over rotaties, spiegelingen, de groep-eigenschappen en de Sudoku-eigenschap om volgende groep-Sudoku volledig op te lossen met slechts 1 gegeven

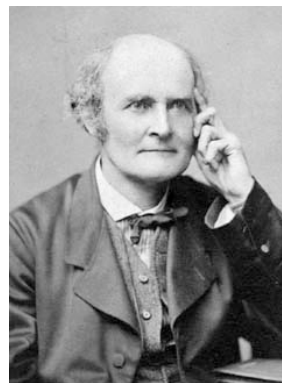
$\circ$	e	r	r'	s	s'	s''
e						
r				s'		
r'						
s						
s'						
s''						

Definitie 4 De groep van orde n bestaande uit alle rotatie-symmetrieën van een regelmatige n -hoek noemen we de **cyclische groep van orde n** en noteren we met C_n .

De groep van orde $2n$ bestaande uit alle symmetrieën van een regelmatige n -hoek noemen we de **diheder groep van orde $2n$** en noteren we met D_n .

2. DE STELLING VAN CAYLEY (1854)

Arthur Cayley werd geboren op 16 augustus 1821 in Richmond (Engeland) en stierf op 75 jarige leeftijd op 26 januari 1895 in Cambridge (Engeland).



De **stelling van Cayley**, die hij bewees op 33-jarige leeftijd, stelt dat elke eindige groep een deelgroep is van een symmetrische groep en dat we dus iedere eindige groep kunnen opvatten als een permutatie groep.

De voorbeelden van groepen die we tot nu toe gezien hebben zijn allen symmetriegroepen van meetkundige objecten (regelmatige n -hoeken). Een ander belangrijk voorbeeld van een eindige groep is de *symmetrische groep* S_n .

Definitie 5 Een **permutatie** van n elementen is een *bijectie* σ

$$\{1, 2, \dots, n\} \xrightarrow{\sigma} \{1, 2, \dots, n\}$$

en wordt voorgesteld als een $2 \times n$ *matrix*

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

De samenstelling van twee permutaties (bijecties) is opnieuw een permutatie (bijectie)

$$\begin{aligned} \sigma \circ \tau &= \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \dots & \sigma(\tau(n)) \end{pmatrix} \end{aligned}$$

Definitie 6 De **symmetrische groep** op n elementen is de groep met als elementen alle permutaties op n elementen en als groepsbewerking de samenstelling.

OPGAVE 10. Toon aan dat S_n inderdaad een groep is van orde $n!$

Omdat we vaak berekeningen zullen maken in S_n verkiezen we een meer efficiënte schrijfwijze voor permutaties.

Definitie 7 De **Cayley-notatie** van een permutatie $\sigma \in S_n$ (ook wel **cycle-notatie** of **cycle-decompositie** van σ genoemd) is de schrijfwijze

$$\sigma = (a_1, a_2, \dots, a_{i_1})(b_1, b_2, \dots, b_{i_2}) \dots (x_1, x_2, \dots, x_{i_x})$$

waarbij we bedoelen dat

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{i_1}) = a_1$$

$$\sigma(b_1) = b_2, \sigma(b_2) = b_3, \dots, \sigma(b_{i_2}) = b_1$$

$$\vdots$$

$$\sigma(x_1) = x_2, \sigma(x_2) = x_3, \dots, \sigma(x_{i_x}) = x_1$$

Dus, als bvb.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 6 & 7 & 3 & 5 & 4 & 2 \end{pmatrix}$$

dan is de Cayley-notatie van σ gelijk aan

$$\sigma = (1, 8, 2)(3, 6, 5)(4, 7)$$

In de Cayley-notatie mogen we cycles van lengte één weglaten, dwz. als $\sigma(i) = i$ dan hoeven we in de notatie van σ niet de 1-cycle (i) op te nemen. Dus, als bvb.

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 4 & 3 & 5 & 7 & 1 \end{pmatrix}$$

dan is de (verkorte) Cayley-notatie van τ gelijk aan

$$(1, 8)(3, 6, 5)$$

OPGAVE 11. Schrijf alle zes permutaties op 3 elementen $\{1, 2, 3\}$ in verkorte Cayley-notatie.

Merk op dat de Cayley-notatie van een permutatie *niet uniek bepaald is*. Bijvoorbeeld

$$(1, 8, 2)(3, 6, 5)(4, 7) \quad \text{en} \quad (7, 4)(3, 6, 5)(2, 1, 8)$$

bepalen dezelfde permutatie σ . We zien dus dat twee Cayley-notaties dezelfde permutaties bepalen op

- volgorde van de verschillende cycles na en op
- cyclische volgorde van de termen in de cycles na.

Het volstaat om voor een permutatie één van de mogelijke notaties te nemen.

Rekenregels voor permutaties: Gegeven twee permutaties $\sigma, \tau \in S_n$, hoe bepalen we het product $\sigma \circ \tau$ en het invers element σ^{-1} gegeven Cayley-notaties voor σ en τ ?

(product) : Schrijf de notatie voor σ links van de notatie voor τ . Om het beeld van een getal i te bepalen onder $\sigma \circ \tau$ zoek je naar de meest rechtse cycle waarin i voorkomt (indien i nergens voorkomt wordt natuurlijk i naar zichzelf gestuurd). Stel dat deze cycle i naar j stuurt dan zoek je vervolgens naar een cycle striks links waarin j nogmaals voorkomt (is er zo geen dan wordt i naar j gestuurd onder $\sigma \circ \tau$). Als deze cycle j naar k stuurt dan wordt onder $\sigma \circ \tau$ het element i naar k gestuurd. Herhaal nu de operatie voor k enzovoort. Op deze manier vind je de Cayley-notatie voor $\sigma \circ \tau$.

Bvb. als $\sigma = (1, 8, 2)(3, 6, 5)(4, 7)$ en $\tau = (1, 8)(3, 6, 5)$ dan bekijk je

$$(1, 8, 2)(3, 6, 5)(4, 7)(1, 8)(3, 6, 5)$$

Begin met 1 : de meest rechtse cycle waarin 1 voorkomt is $(1, 8)$ en die stuurt 1 naar 8. Dan moeten we zoeken naar een meer linkse cycle waarin 8 voorkomt en die is $(1, 8, 2)$ en stuurt 8 naar 2. Dus wordt 1 naar 2 gestuurd onder $\sigma \circ \tau$ en begint onze Cayley-notatie met

$$\sigma \circ \tau = (1, 2,$$

Neem nu 2 : de meest rechtse cycle waarin een 2 voorkomt is $(1, 8, 2)$ en die stuurt 2 naar 1. Er is geen meer linkse cycle meer waarin 1 voorkomt dus wordt 2 naar 1 gestuurd onder $\sigma \circ \tau$. Dus sluit onze eerste cycle en weten we al

$$\sigma \circ \tau = (1, 2)(3,$$

Bekijk 3 : meeste rechtse cycle is $(3, 6, 5)$ die 3 naar 6 stuurt en 6 komt in een meer linkse cycle voor nl. $(3, 6, 5)$ die 6 naar 5 stuurt. Dus wordt 3 naar 5 gestuurd en hebben we

$$\sigma \circ \tau = (1, 2)(3, 5,$$

Bekijk nu 5 en ga na dat uiteindelijk 5 naar 6 gestuurd wordt (via een 3). Dat 6 naar 3 gestuurd wordt (via een 5). En dan hebben we al

$$\sigma \circ \tau = (1, 2)(3, 5, 6)(4,$$

want het eerste getal dat we nog niet hebben is 4. Dus bekijk 4 en stel vast dat dit naar 7 gestuurd wordt. Vervolgens ga je na dat 7 onder $\sigma \circ \tau$ naar 4 wordt gestuurd. Dus

$$\sigma \circ \tau = (1, 2)(3, 5, 6)(4, 7)(8,$$

maar 8 wordt naar zichzelf gestuurd (via een 1) en dus mogen we deze 1-cycle weglaten. Omdat we nu de beeldwaarden kennen van alle acht de elementen, hebben we

$$\sigma \circ \tau = (1, 2)(3, 5, 6)(4, 7)$$

OPGAVE 12. Bereken de producten $\sigma \circ \tau$ en $\tau \circ \sigma$ in de symmetrische groep op 12 elementen S_{12} met

$$\begin{cases} \sigma = (1, 2)(3, 4)(5, 6)(7, 8)(9, 10)(11, 12) \\ \tau = (1, 3, 2)(4, 7, 5)(8, 9, 11) \end{cases}$$

(Ter informatie voor veel later : σ en τ zijn voortbrengers van de sporadische simpele Mathieu group M_{12} van orde 95040)

(invers element) : Het voordeel van de Cayley-notatie is dat je ook makkelijk het inverse element σ^{-1} kan bepalen door gewoon de orde van elke cycle om te keren. In het voorbeeld dat $\sigma = (1, 8, 2)(3, 6, 5)(4, 7)$ is $\sigma^{-1} = (2, 8, 1)(5, 6, 3)(7, 4)$. Immers,

$$\sigma^{-1} \circ \sigma = (2, 8, 1)(5, 6, 3)(7, 4)(1, 8, 2)(3, 6, 5)(4, 7) = ()$$

OPGAVE 13. Pas deze rekenregels toe om de groep-tabel van de symmetrische groep op 3 elementen te bepalen. Gebruik hiervoor de volgorde van elementen

$$S_3 = \{(), (1, 2), (1, 3, 2), (2, 3), (1, 3), (1, 2)\}$$

Deze specifieke ordening zal ons toelaten een verband te zien met de symmetrie-groep van een regelmatige 3-hoek.

In wiskunde zijn niet enkel de objecten van een bepaalde soort (in ons geval, groepen) belangrijk maar ook de afbeeldingen, zeg maar de verbanden, tussen deze objecten. We weten dat een afbeelding tussen twee *verzamelingen*

$$f : V \longrightarrow W$$

aan ieder element $v \in V$ een beeldwaarde $f(v) \in W$ toekent. Als de verzamelingen extra structuur hebben (zoals in ons geval een groep-structuur) dan willen we natuurlijk enkel die afbeeldingen bekijken die deze extra structuur bewaren.

Definitie 8 Als G een groep is met groepsbewerking $\cdot$ en eenheidselement e_G en H een groep met groepsbewerking $*$ en eenheidselement e_H , dan noemen we een afbeelding

$$f : G \longrightarrow H$$

een **groepsmorphisme** indien f eenheidselementen naar elkaar stuurt, dus

$$f(e_G) = e_H$$

en verder producten naar producten stuurt, dat is

$$f(g \cdot g') = f(g) * f(g')$$

voor alle elementen g en g' van G . Een groepsmorphisme f noemen we een **monomorfisme** indien f injectief is, een **epimorfisme** indien f surjectief is en een **isomorfisme** indien f een bijectie is.

Definitie 9 Voor een groepsmorphisme $f : G \longrightarrow H$ is de **kern** van f de deelverzameling

$$\ker(f) = \{g \in G : f(g) = 1_H\}$$

van elementen van G die naar het eenheidselement van H gestuurd worden en is het **beeld** van f de deelverzameling

$$\text{im}(f) = \{f(g) \mid g \in G\}$$

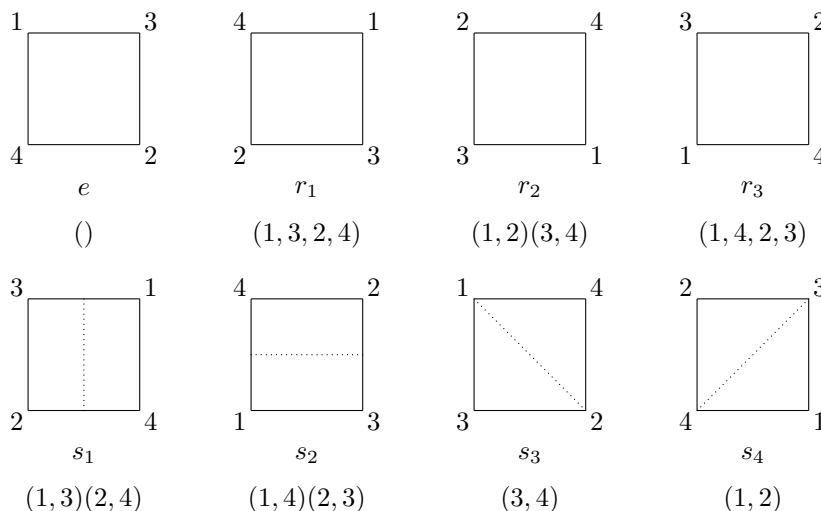
van H bestaande uit alle beelden van elementen van G .

OPGAVE 14. Toon aan dat voor een groepsmorphisme $f : G \longrightarrow H$ de kern $\ker(f)$ een deelgroep is van G en dat het beeld $\text{im}(f)$ een deelgroep is van H .

OPGAVE 15. Toon aan dat een groepsmorphisme $f : G \longrightarrow H$ een monomorfisme is als en alleen als de kern minimaal is, $\ker(f) = \{e_G\}$.

Een voorbeeld van een groepsmorphisme is de afbeelding $D_n \longrightarrow S_n$ die aan elke symmetrie van een regelmatige n -hoek de permutatie associeert geïnduceerd op de n

hoekpunten. Bvb. aan elk van de acht symmetrieën van een vierkant kunnen we devolgende permutaties toekennen



En omdat in beide gevallen de groepsbewerking gegeven wordt door samenstelling, is deze afbeelding een groepsmorphisme. Een voorbeeld

$$f(r_1) \circ f(s_1) = (1, 3, 2, 4)(1, 3)(2, 4) = (1, 2) = f(s_4) = f(r_1 \circ s_1)$$

OPGAVE 16. Toon aan dat het groepsmorphisme $f : D_n \longrightarrow S_n$ een monomorfisme is. Bijgevolg is D_n isomorf met zijn beeld onder f en kunnen we dus de diheder-groep D_n opvatten als een deelgroep van S_n .

OPGAVE 17. In het speciale geval $n = 3$ toon aan dat D_3 isomorf is met S_3 , we noteren dit met $D_3 \simeq S_3$.

Omdat we goed kunnen werken met permutaties zou het leuk zijn indien we iedere eindige groep G zouden kunnen opvatten als een deelgroep van een symmetrische groep S_n voor zekere n . Arthur Cayley bewees in 1854 dat dit inderdaad het geval is. De truuk bestaat erin de kolommen van de groep-tabel van G op te vatten als permutaties op de groep-elementen (die we kunnen nummeren als de getallen $\{1, \dots, n\}$ (wegens de Sudoku-eigenschap zijn dit inderdaad permutaties). We zullen eerst een voorbeeld uitwerken.

De groep-tabel van de symmetrie-groep D_3 van een regelmatige driehoek is

$\circ$	i	r_1	r_2	s_1	s_2	s_3
i	i	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	i	s_3	s_1	s_2
r_2	r_2	i	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	i	r_1	r_2
s_2	s_2	s_3	s_1	r_2	i	r_1
s_3	s_3	s_1	s_2	r_1	r_2	i

Vergeet nu de namen van de symmetrieën en identificeer ze met getallen via

i	r_1	r_2	s_1	s_2	s_3
1	2	3	4	5	6

dan krijgt de groep-tabel devolgende vorm

$\circ$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	1	2	3
5	5	6	4	3	1	2
6	6	4	5	2	3	1

We sturen nu elke symmetrie (via de identificatie) naar de permutatie in S_6 gegeven door de rij in de groep-tabel. Bijvoorbeeld

$$r_1(=2) \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix} = (1, 2, 3)(4, 6, 5)$$

$$s_1(=4) \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (1, 4)(2, 5)(3, 6)$$

Deze operatie geeft een afbeelding $D_3 \xrightarrow{f} S_6$ dat een groepsmorfisme is, bvb.

$$f(r_1) \circ f(s_1) = (1, 2, 3)(4, 5, 6)(1, 4)(2, 5)(3, 6) = (1, 6)(2, 4)(3, 4) = f(s_3) = f(r_1 \circ s_1)$$

want de permutatie die hoort bij s_3 is inderdaad

$$s_3(=6) \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix} = (1, 6)(2, 4)(3, 5)$$

Merk verder op dat het beeld van een rotatie (een orde drie element) bestaat uit twee cycles van lengte drie en het beeld van een spiegeling (een orde twee element) bestaat uit drie cycles van lengte twee. Het bewijs van de stelling van Cayley formalizeert de voorgaande berekening.

Stelling 2 (Cayley (1854)) Zij G een eindige groep van orde n en beschouw voor elk element $a \in G$ de permutatie op G bepaald door links-vermenigvuldiging met a

$$\lambda_a : G \longrightarrow G \quad x \mapsto a.x$$

De afbeelding $\lambda : G \longrightarrow S_n$ is een groepsmorfisme en is injectief (een monomorfisme). Bijgevolg is G isomorf met een deelgroep van S_n .

Verder, als $a \in G$ een element is van orde r , dan bestaat de cycle-decompositie van de permutatie $\lambda_a \in S_n$ uit n/r cycles, elk van lengte r .

Bewijs. Om te beginnen is λ_a inderdaad een permutatie van G want als $a.x = a.y$ dan is $x = y$ (de Sudoku-eigenschap). Verder is λ een groepsmorfisme want

$$\lambda_{ab}(x) = (a.b).x = a.(b.x) = a.\lambda_b(x) = \lambda_a \circ \lambda_b(x)$$

en natuurlijk is λ_e de identiteits-permutatie. λ is ook een monomorfisme want stel dat $a \in \ker(\lambda)$ dan is λ_a de identiteits-permutatie en dus is voor elke $x \in G$ dat $a.x = x$ maar dan is $a = e$, bijgevolg is $\ker(\lambda) = \{e\}$.

Stel nu dat de orde van $a \in G$ gelijk is aan r , dwz. $a^r = e$. Als $x \in G$ dan zijn de elementen

$$\{x, a.x, a^2.x, \dots, a^{n-1}.x\}$$

allen verschillend en omdat ze uit elkaar verkregen worden door links-vermenigvuldiging met a , zien we dat λ_a de cycle van lengte r

$$(x, a.x, a^2.x, \dots, a^{n-1}.x)$$

Herhaal dit procedé voor $y \in G$ niet bevat in deze cycle. $\square$

Definitie 10 Het groepmorfisme $\lambda : G \longrightarrow S_n$ wordt de **links reguliere representatie** van G genoemd.

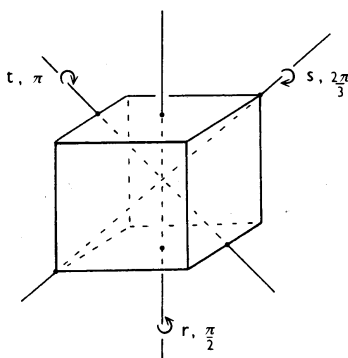
Een direct gevolg van de stelling van Cayley is :

Stelling 3 Als G een eindige groep is van orde n , dan is de orde van elk element $g \in G$ een deler van n .

Bewijs. De stelling van Cayley stelt dat de permutatie $\lambda_g \in S_n$ bestaat uit $\frac{n}{r}$ cycles van lengte r als r de orde is van g . In het bijzonder moet $\frac{n}{r}$ een geheel getal zijn en is dus $r = \text{orde}(g)$ een deler van $n = \#G$. $\square$

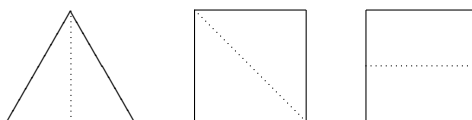
OPGAVE 18. Als p een priemgetal is, toon aan dat iedere groep G van orde p isomorf is met de cyclische groep C_p .

OPGAVE 19. Toon aan dat de kubus juist 24 rotatie-symmetrieën heeft en dat deze symmetrie-groep van de cubus isomorf is met S_4 , de symmetrische groep op 4 letters.



3. NORMAALDELERS EN QUOTIENTEN

We hebben gezien dat een regelmatige n -hoek juist $2n$ symmetrieën heeft, namelijk n rotaties met als centrum het middelpunt van de n -hoek en een rotatiehoek die een veelvoud van $360^\circ/n$ is en n spiegelingen om één van de n symmetrie-assen van de n -hoek (als n oneven is gaan die assen door een hoekpunt en het midden van de overstaande zijde, als n even is gaan ze door overstaande hoekpunten of door de middens van overstaande zijden)



We hebben ook gezien dat deze symmetrieën een groep vormen onder samenstelling, nl. de diheder-groep D_n . Neem nu C_2 de cyclische groep van orde twee, dwz. $C_2 = \{e, g\}$ met groep-tabel

$\cdot$	e	g
e	e	g
g	g	e

dan kunnen we een groeps-epimorfisme definiëren

$$\pi : D_n \longrightarrow C_2$$

door rotaties te sturen naar e en spiegelingen naar g . Dit is duidelijk een surjectieve afbeelding en is ook een groeps-morfisme omdat we weten hoe rotaties en spiegelingen samenstellen

$\circ$	rotatie	spiegeling
rotatie	rotatie	spiegeling
spiegeling	spiegeling	rotatie

De kern van π bestaat uit alle elementen van D_n die naar e gestuurd worden en dit zijn per constructie juist alle rotaties. Bijgevolg hebben we dat

$$\ker(\pi) = C_n$$

de deelgroep C_n van alle rotaties van de n -hoek. Deze deelgroep voldoet aan de extra voorwaarde dat voor elke symmetrie $g \in D_n$ en elke rotatie $r \in C_n$ we hebben dat

$$g \circ r \circ g^{-1} \in C_n$$

Immers, ofwel is g een rotatie en dan is ook g^{-1} een rotatie en dan staat er een samenstelling van drie rotaties die opnieuw een rotatie is, ofwel is g een spiegeling maar dan is $g^{-1} = g$ en staat er $g \circ (r \circ g)$ een samenstelling van twee spiegelingen, dus een

rotatie. We zeggen dat de deelgroep C_n van alle rotaties een *normaaldeler* is van de symmetrie-groep D_n .

Definitie 11 Een deelgroep H van een groep G is een **normaaldeler** als voor alle $g \in G$ geldt dat

$$g.H.g^{-1} = \{g.h.g^{-1} \mid h \in H\} \subset H$$

Als dit geldt, is natuurlijk $g.H.g^{-1} = H$ want elke $h \in H$ kunnen we ook schrijven als

$$h = g.g^{-1}.h.g.g^{-1} = g.(g^{-1}.h.g).g^{-1} = g.(g^{-1}.h^{-1}.g)^{-1}.g^{-1} = g.h'.g^{-1}$$

vermits $h^{-1} \in H$ en $g^{-1} \in G$. Als H een normaaldeler is van G noteren we dit met $N \triangleleft G$.

OPGAVE 20. Toon aan dat voor ieder epimorfisme π

$$\pi : G \longrightarrow G'$$

de kern $\ker(\pi)$ een normaaldeler is van G .

De naam *normaaldeler* suggereert dat we zulke deelgroep kunnen 'uitdelen' uit G en een *quotientgroep* $\bar{G} = G/H$ bekomen. Laat ons een voorbeeld geven.

In de symmetrie groep D_n laat ons met $\bar{D}_n = D_n/C_n$ de verzameling bestaande uit twee elementen noteren

$$\bar{D}_n = \{R, S\}$$

waarbij R staat voor de deelverzameling van D_n van alle rotaties en S staat voor de deelverzameling van alle spiegelingen in D_n . Merk dus op dat de *elementen* van $\bar{D}_n$ ook *deelverzamelingen* zijn van D_n . Dus, voor $n = 3$ hebben we bvb.

$$\bar{D}_3 = \{R = \{e, r_1, r_2\}, S = \{s_1, s_2, s_3\}\}$$

en we hebben een natuurlijke surjectieve afbeelding

$$D_n \longrightarrow \bar{D}_n \quad g \mapsto \bar{g} = g \circ C_n = \{g \circ r \mid r \in C_n\}$$

die aan iedere symmetrie g de deelverzameling $g \circ C_n$ associeert. Merk op dat $\bar{g}$ bestaat uit ofwel alle rotaties ofwel alle spiegelingen in D_n . Bvb. voor $n = 3$ is

$$\bar{s}_1 = s_1 \circ C_3 = \{s_1 \circ i, s_1 \circ r_1, s_1 \circ r_2\} = \{s_1, s_2, s_3\}$$

Bijgevolg kunnen we op $\bar{D}_n$ een groepsstructuur zetten met groep-tabel

.	R	S
R	R	S
S	S	R

met als eenheidselement R zodanig dat de afbeelding $D_n \longrightarrow \bar{D}_n$ een groeps-epimorfisme is (gebruik de eigenschappen van samenstellingen van rotaties en spiegelingen). We noemen $\bar{D}_n = D_n/C_n$ de *quotientgroep* van D_n bepaald door de normaaldeler C_n en noemen het epimorfisme $D_n \longrightarrow \bar{D}_n$ de *quotientafbeelding*.

Definitie 12 Laat H een normaaldeler zijn van een groep G . De **quotientgroep** van G bepaald door H is de verzameling van deelverzamelingen van G

$$\bar{g} = \{g.h \mid h \in H\}$$

met als groepsbewerking

$$\bar{g} \cdot \bar{g}' = \overline{g \cdot g'}$$

en wordt genoteerd als $\bar{G} = G/H$. De bijhorende **quotientafbeelding**

$$G \longrightarrow \bar{G} = G/H \quad g \mapsto \bar{g}$$

is een epimorfisme van groepen.

Stelling 4 Als $H \triangleleft G$ dan is $\bar{G} = G/H$ inderdaad een groep. Als G eindig is, dan is de orde van de quotientgroep gelijk aan

$$\#\bar{G} = \frac{\#G}{\#H}$$

In het bijzonder is de orde van H een deler van de orde van G .

Bewijs. deel 1 : Merk op dat wegens de Sudoku-eigenschap van de groep-tabel van G elk van de deelverzamelingen

$$\bar{g} = \{g \cdot h \mid h \in H\}$$

bestaat uit juist $\#H$ elementen. We beweren dat voor alle $g, g' \in G$ geldt dat

$$\text{ofwel } \bar{g} \cap \bar{g}' = \emptyset \quad \text{ofwel } \bar{g} = \bar{g}'$$

Stel dat $x \in \bar{g} \cap \bar{g}'$ dan bestaan er $h, h' \in H$ zodat

$$g \cdot h = x = g' \cdot h'$$

maar dan is

$$g = g' \cdot h' \cdot h^{-1} \quad \text{en} \quad g' = g \cdot h \cdot (h')^{-1}$$

Voor elke $h'' \in H$ hebben we dus dat

$$\begin{cases} g \cdot h'' = g' \cdot h' \cdot h^{-1} \cdot h'' = g' \cdot (h' \cdot h^{-1} \cdot h'') \in \bar{g}' \\ g' \cdot h'' = g \cdot h \cdot (h')^{-1} \cdot h'' = g \cdot (h \cdot (h')^{-1} \cdot h'') \in \bar{g} \end{cases}$$

en dus

$$\bar{g} \subset \bar{g}' \quad \text{en} \quad \bar{g}' \subset \bar{g}$$

We hebben dus aangetoond dat ofwel $\bar{g}$ en $\bar{g}'$ disjunct zijn ofwel dezelfde deelverzameling van G zijn. Bijgevolg kunnen we in elk van de deelverzamelingen juist één element g_i kiezen en dan hebben we een disjuncte unie

$$G = \bar{g}_1 \sqcup \bar{g}_2 \sqcup \dots \sqcup \bar{g}_k$$

waarbij $k = \#G/H$. Omdat we al weten dat elk van de deelverzamelingen $\bar{g}_i$ bestaat uit juist $\#H$ elementen hebben we dus voor het aantal elementen van G (de orde van G) dat

$$\#G = \#\bar{g}_1 + \#\bar{g}_2 + \dots + \#\bar{g}_k = k \cdot \#H$$

waaruit dus volgt dat het aantal elementen van $\bar{G} = G/H$ gelijk is aan

$$\#G/H = \frac{\#G}{\#H}$$

en dus dat in het bijzonder de orde van H een deler is van de orde van G .

deel 2 : Om the beginnen moeten we aantonen dat de definitie van de product-regel

$$\bar{g} \cdot \bar{g}' = \overline{g \cdot g'}$$

goedgedefinieerd is. Hiermee bedoelen we dat deze definitie niet afhangt van de gekozen elementen g in $\bar{g}$ en g' in $\bar{g}'$. Dus neem andere elementen $z \in \bar{g}$ en $z' \in \bar{g}'$. Dan weten we al dat $z = g.h$ en $z' = g'.h'$. Verder hebben we elementen $h.h' \in H$ zodat

$$z = g.h \quad \text{en} \quad z' = g'.h'$$

maar dan hebben we dat

$$z.z' = (g.h).(g'.h') = g.h.g'.h' \stackrel{!}{=} g.g'.h''.h \in \overline{g.g'} \quad \text{en dus} \quad \overline{z.z'} = \overline{g.g'}$$

De cruciale gelijkheid $\stackrel{!}{=}$ gebruikt het feit dat H een normaaldivisor is. Immers omdat

$$g.H.g^{-1} = H \quad \text{volgt} \quad g.H = H.g = \{h.g \mid h \in H\} \quad \text{voor alle } g \in G$$

en daarom dat we elke $h.g'$ kunnen schrijven als een $g'.h''$ eventueel voor h'' verschillend van h maar nog altijd in de normaaldivisor H . Alle groeps-eigenschappen voor $\bar{G}$ volgen nu uit deze van G .

Het eenheidselement van $\bar{G}$ is het element (de deelverzameling) $\bar{e}$ want

$$\bar{e}.\bar{g} = \overline{e.g} = \bar{g} = \overline{g.e} = \bar{g}.\bar{e}$$

Het invers element van $\bar{g}$ is het element (deelverzameling) $\bar{g}^{-1}$ want

$$\bar{g}.\bar{g}^{-1} = \overline{g.g^{-1}} = \bar{e}$$

en associativiteit van de bewerking volgt ook uit deze voor G want

$$\bar{g}.\overline{(g'.g'')} = \overline{g.g'.g''} = \overline{g.(g'.g'')} = \overline{(g.g').g''} = \overline{g.g'.\overline{g''}} = \overline{(g.g').g''} = \overline{(g.g').g''}$$

en dus is de verzameling van deelverzamelingen $\bar{G}$ met deze bewerking inderdaad een groep. $\square$

Lees het bewijs nog eens na en ga na dat we de normaaldivisor-eigenschap enkel in deel 2 gebruikt hebben. Dwz. in het eerste deel van het bewijs hebben we enkel gebruikt dat H een deelgroep is van G .

4. DE STELLING VAN LAGRANGE (1770)

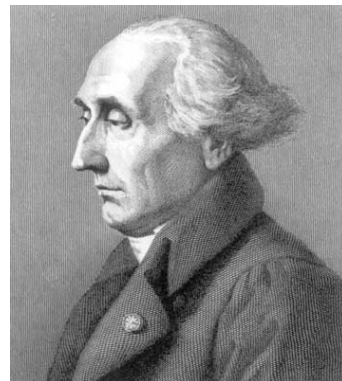
Definitie 13 Als H een deelgroep is van een groep G dan zijn de *rechter-nevenklassen* van H in G de verzameling G/H van deelverzamelingen

$$\bar{g} = g.H = \{g.h \mid h \in H\}$$

van G . Analoog kunnen we de **linker-nevenklassen** van H in G als de verzameling van deelverzamelingen $H.g$ definiëren.

We kunnen nu het gevolg van de stelling van Cayley dat stelt dat de orde van elk groeps-element een deler is van de orde van de groep uitbreiden tot deelgroepen. Dit is de *stelling van Lagrange (1770)*.

Joseph-Louis Lagrange werd geboren als Giuseppe Lodovico Lagrangia op 25 januari 1736 in Turijn (toen Sardinië-Piemonte, nu Italië) en stierf op 77 jarige leeftijd op 10 april 1813 in Parijs (Frankrijk).



De **stelling van Lagrange**, die hij op 34 jarige leeftijd bewees, stelt dat de orde van een deelgroep steeds een deler is van de orde van de hele groep en in het bijzonder dat de orde van een groeps-element steeds een deler moet zijn van de orde van de groep.

Stelling 5 (Lagrange (1770)) Als G een eindige groep is van orde $\#G = n$ en H een deelgroep van orde $\#H = m$, dan is m een deler van n .

Bewijs. Uit deel 1 van het vorige bewijs, dat enkel gebruikt dat H een deelgroep is en *niet* de strengere eis van normaaldeur volgt dat het aantal rechter-nevenklassen gelijk is aan

$$\#G/H = \frac{\#G}{\#H}$$

en dus in het bijzonder dat het aantal elementen van de deelgroep H een deler is van het aantal elementen van G . $\square$

Definitie 14 Als $H \triangleleft G$ dan noemen we de orde van de quotientgroep $\overline{G} = G/H$ de **index** van de normaaldeeler H in G en noteren dit met $[G : H]$.

Als H een deelgroep is van G dan noemen we het aantal rechter-nevenklassen van H in G de **index** van de deelgroep H in G en noteren dit met $[G : H]$.

OPGAVE 21. Toon aan dat voor een deelgroep H van G het aantal linker-nevenklassen gelijk is aan het aantal rechter-nevenklassen.

Voorgaande argumenten gebruiken impliciet een belangrijke wiskundige notie, namelijk die van een **equivalentie-relatie**. Omdat je later nog andere quotient-structuren zal definiëren aan de hand van deze notie nemen we even de tijd voor enkele definities.

Definitie 15 Een **relatie** $\mathcal{R}$ op een verzameling V is een deelverzameling

$$\mathcal{R} \subset V \times V = \{(v, w) \mid v, w \in V\}$$

van de productverzameling bestaande uit alle koppeltjes van elementen van V . Als $(v, w) \in \mathcal{R}$ dan zeggen we dat v en w in relatie tot elkaar staan en noteren dit door $v \sim w$ (merk op dat de orde van de componenten van een koppel een rol speelt en dus ook de plaatsing van de termen rond een $\sim$ teken).

Definitie 16 Een **equivalentie relatie** $\mathcal{R}$ op een verzameling V is een relatie $\mathcal{R}$ die voldoet aan devolgende eisen

- **reflexief** : Voor iedere $v \in V$ geldt $x \sim x$.
- **symmetrisch** : Als $x \sim y$ dan ook $y \sim x$.
- **transitief** : Als $x \sim y$ en $y \sim z$ dan ook $x \sim z$.

Definitie 17 Als $\mathcal{R}$ een equivalentie relatie is op een verzameling V en als v een element is van V dan is de **equivalentie klasse** van v de deelverzameling

$$[v] = \{w \in V \mid v \sim w\}$$

Merk op dat twee equivalentie klassen ofwel disjunct zijn ofwel gelijk. Immers, als $u \in [v] \cap [w]$ dan is $v \sim u$ en $w \sim u$ maar wegens symmetrie en transitiviteit dan ook $v \sim w$ en dus $[v] = [w]$.

OPGAVE 22. Als G een groep is en H een deelgroep, toon aan dat de relatie

$$\mathcal{R} = \{(g, g') \mid g^{-1} \cdot g' \in H\} \subset G \times G$$

een equivalentie relatie is en dat de bijhorende equivalentie klasse

$$[g] = \overline{g}$$

gelijk is aan de linker-nevenklasse van g ten opzichte van H .

Definitie 18 Een **partitie** van een verzameling V is een disjuncte unie van deelverzamelingen van V . Dit wil zeggen, er zijn niet-lege deelverzamelingen V_i van V met

$$V = \bigcup_i V_i$$

en zodat voor $i \neq j$ we hebben dat $V_i \cap V_j = \emptyset$.

OPGAVE 23. Toon aan dat er een natuurlijke bijjectie bestaat tussen de equivalentie relaties op een verzameling V en de verschillende partities van V . Deze correspondentie wordt gegeven door naar de equivalentie klassen te kijken.

Na deze uitstap in algemene quotient structuren, laat ons terugkeren tot groepen. We geven enkele voorbeelden van normaaldelers.

Definitie 19 Een groep G noemen we **Abels** indien alle elementen van G met elkaar commuteren. Dus,

$$g \cdot g' = g' \cdot g$$

voor alle $g, g' \in G$.

Eenvoudige voorbeelden van Abelse groepen zijn cyclische groepen C_n . Soms gebruikt men voor Abelse groepen het somteken (+) om de groepsbewerking aan te geven ipv. het produktteken (.). Wij zullen echter steeds het product gebruiken om (nog meer) verwarring te vermijden.

Definitie 20 De **commutator deelgroep** van een groep G is de deelgroep voortgebracht door alle **commutatoren**, dwz. alle elementen van de vorm

$$[g, h] = g \cdot h \cdot g^{-1} \cdot h^{-1}$$

voor elementen $g, h \in G$. Een algemeen element van de commutator deelgroep is dus een product van commutatoren

$$[g_1, h_1] \cdot [g_2, h_2] \cdot \dots \cdot [g_k, h_k]$$

(in het algemeen is het niet waar dat het product van twee commutatoren opnieuw een commutator is). Soms noteert men de commutator deelgroep (soms ook de **afgeleide groep** genoemd) met G' of met $[G, G]$.

OPGAVE 24. Toon aan dat de commutator deelgroep een normaaldeeler is van G en dat de quotientgroep

$$G/G'$$

een Abelse groep is.

Definitie 21 Het **centrum** Z van een groep G is de deelverzameling

$$Z = \{z \in G \mid z \cdot g = g \cdot z \text{ voor alle } g \in G\}$$

van elementen die met alle elementen van G commuteren.

OPGAVE 25. Toon aan dat het centrum Z een normaaldeeler is van G .

In het algemeen kunnen we weinig zeggen over de quotientgroep G/Z . Wanneer we echter voorwaarden opleggen aan dit quotient kunnen we soms eigenschappen van G afleiden.

OPGAVE 26. Als G een eindige groep is met centrum Z en als de quotient groep G/Z cyclisch is. Toon aan dat G een Abelse groep moet zijn.

Voor het epimorfisme $\pi : D_n \longrightarrow C_2$ hebben we $\ker(\pi) = C_n$ en we hebben aangetoond dat de quotientgroep $D_n/C_n = \{R, S\}$ isomorf is met $C_2 = \text{im}(\pi)$. Dit is geen toeval.

Stelling 6 (Eerste isomorfie stelling) *Voor ieder groepsmorfisme*

$$G \xrightarrow{f} H$$

met beeld $\text{im}(f)$ en kern $\ker(f)$ geldt dat de quotientgroep

$$G/\ker(f) \simeq \text{im}(f)$$

isomorf is met het beeld.

Bewijs. We hebben devolgende situatie

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \searrow F & \\ G/\ker(f) & & \end{array}$$

waarbij π de quotient-afbeelding is $G \twoheadrightarrow \bar{G} = G/\ker(f)$. We definiëren een afbeelding

$$\bar{G} \xrightarrow{F} H \quad \text{door} \quad \bar{g} \mapsto f(g)$$

We moeten aantonen dat dit onafhankelijk is van het gekozen element g in de nevenklasse $\bar{g}$. Stel dat $g' \in \bar{g}$ (en dus dat $\bar{g} = \bar{g'}$) dan is er een $k \in \ker(f)$ zodat $g' = g.k$ maar dan geldt omdat f een groepsmorfisme is dat

$$f(g') = f(g.k) = f(g).f(k) = f(g).e_H = f(g)$$

en bijgevolg is F goed gedefinieerd. F is per constructie duidelijk een groepsmorfisme. We beweren dat F injectief is (een monomorfisme). Immers, als

$$F(\bar{g}) = e_H \quad \text{dan} \quad f(g) = e_H$$

en dus $g \in \ker(f)$ en dus $\bar{g} = \bar{e}$. F is ook surjectief (een epimorfisme) op het beeld $\text{im}(f)$ en dus is $F : \bar{G} \longrightarrow \text{im}(f)$ een isomorfisme. $\square$

We zien dus dat er een één-één verband is tussen normaaldelers van G en isomorfie-classes van epimorfismen $G \twoheadrightarrow H$. Anders gezegd, ieder epimorf beeld H van G is isomorf met een quotientgroep $\bar{G} = G/N$ voor een normaaldeeler $N \triangleleft G$, waarbij N de kern is van het epimorfisme.

Definitie 22 Laat $N \triangleleft G$ een normaaldeeler zijn van G en $H \subset G$ een deelgroep van G dan noteren we met $H.N$ de deelgroep van G

$$H.N = \{h.n \mid h \in H \text{ en } n \in N\}$$

Merk op dat $N \subset H.N$ en als $N \subset H$ dan is $H = H.N$.

OPGAVE 27. Toon aan dat $H.N$ inderdaad een deelgroep is van G . Toon aan dat als $H \triangleleft G$ dan ook $H.N \triangleleft G$.

OPGAVE 28. Toon aan dat er een natuurlijk één-één verband is tussen

- deelgroepen van de quotientgroep $\overline{G} = G/N$
- deelgroepen H van G zodat $N \subset H$

Onder deze correspondentie gaan normaaldelers naar normaaldelers.

Stelling 7 (Tweede isomorfie stelling) Als $N \subset H$ beiden normaaldelers zijn van G dan is $\pi(H) = H/N$ een normaaldeeler van de quotientgroep $\overline{G} = G/N$. We kunnen dus verder uitdelen en krijgen een isomorfisme

$$(G/N)/(H/N) \simeq \tilde{G} = G/H$$

met de quotientgroep verkregen door ineens H uit te delen.

Bewijs. Noteer de quotientafbeelding $\phi : G \rightarrow \tilde{G} = G/H$ die g naar $\tilde{g} = g.H$ stuurt. Definiëer nu de afbeelding

$$\overline{G} = G/N \xrightarrow{f} G/H = \tilde{G} \quad \text{door} \quad \overline{g} \mapsto \tilde{g}$$

Deze afbeelding hangt niet af van de keuze van elementen in de nevenklassen. Immers, als $g' \in \overline{g}$ (en dus $\overline{g} = \overline{g'}$) dan is er een $n \in N$ zodat $g' = g.n$ maar omdat $n \in N \subset H$ is dus ook $g' \in \tilde{g} = g.H$ en dus $\tilde{g'} = \tilde{g}$. We hebben nu de situatie

$$\begin{array}{ccc} & G & \\ \swarrow \kappa & & \searrow \varphi \\ \overline{G} = G/N & \xrightarrow{f} & \tilde{G} = G/H \end{array}$$

en omdat de quotient-afbeeldingen groepsmorphisme zijn is ook f een groepsmorphisme. Het eenheidselement in $\tilde{G}$ is $\tilde{e} = H$, dus de kern van f is

$$\ker(f) = \{\overline{g} \mid f(\overline{g}) = \tilde{e}\} = \{\overline{h} \mid h \in H\} = \pi(H) = H/N$$

maar dan volgt het gestelde uit de eerste isomorfie stelling. $\square$

OPGAVE 29. Als $H \subset G$ een deelgroep is en $N \triangleleft G$ een normaaldeeler dan is de doorsnede

$$H \cap N$$

een normaaldeeler van H .

Stelling 8 (Derde isomorfie stelling) Als $N \triangleleft G$ een normaaldeeler is en $H \subset G$ een deelgroep, dan geldt

$$H/(H \cap N) \simeq (H.N)/N$$

Bewijs. Bekijk het groepsmorphisme (samenstelling van de inclusie en de quotientafbeelding)

$$H \xrightarrow{f} \overline{G} = G/N \quad h \mapsto \overline{h} = h.N$$

dan is het beeld de deelgroep $\pi(H) = H.N/N$ van $\overline{G}$ en de kern is gelijk aan

$$\ker(f) = \{h \in H \mid \bar{h} = \bar{e}\} = \{h \in H \mid h \in N\} = H \cap N$$

en het resultaat volgt opnieuw uit de eerste isomorfie stelling.

□

5. DE KLEINSTE GROEPEN

Het hoofdprobleem van de studie van eindige groepen is voor ieder natuurlijk getal $n \in \mathbb{N}$ te bepalen hoeveel groepen van orde n er zijn *op isomorfie na* en wat hun structuur is.

Definitie 23 De *directe product groep* $G \times H$ van twee groepen G en H bestaat uit alle koppels

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

met daarop de groepsbewerking

$$(g, h) \cdot (g', h') = (g \cdot_G g', h \cdot_H h')$$

Dit vorm een groep met als identiteits element $e = (e_G, e_H)$ en waarvan het inverse van een element gegeven wordt door $(g, h)^{-1} = (g^{-1}, h^{-1})$. De orde van de product groep is het product van de ordes van de groepen G en H .

Wanneer is een groep isomorf met het direct product van twee van zijn deelgroepen?

Stelling 9 (Direct Product stelling, versie 1) *Stel dat H en K deelgroepen zijn van een groep G die voldoen aan volgende eigenschappen*

1. *De deelgroepen H en K commuteren elementsgewijs dwz. $h.k = k.h$ voor alle $h \in H$ en alle $k \in K$.*
2. *Ieder element van G kan geschreven worden als $g = h.k$ voor een $h \in H$ en een $k \in K$, of maw. $G = H.K$.*
3. *Enkel het eenheidselement zit in de doorsnede van H en K , $H \cap K = \{e\}$*

Dan volgt dat G isomorf is met het directe product van H en K

$$G \simeq H \times K$$

Bewijs. We zullen aantonen dat ieder element $g \in G$ op **unieke wijze** geschreven kan worden als

$$g = h.k$$

met $h \in H$ en $k \in K$. Stel immers dat er twee zulke schrijfwijzen zijn

$$h.k = g = h_1.k_1$$

dan volgt dat

$$(h_1)^{-1}.h = k_1.k^{-1}$$

Het linkerlid zit in H en het rechterlid in K dus kunnen beide leden enkel gelijk zijn aan e en volgt bijgevolg dat $h = h_1$ en $k = k_1$. We kunnen bijgevolg een goed gedefinieerde afbeelding maken

$$G \xrightarrow{\phi} H \times K \quad g \mapsto (h, k) \quad \text{als } g = h.k$$

Dit is een groepsmorphisme want als $g = h.k$ en $g' = h'.k'$ dan volgt

$$\phi(g).\phi(g') = (h, k).(h', k') = (h.h', k.k') = \phi(h.h'.k.k') = \phi(h.k.h'.k') = \phi(g.g')$$

waar we voor de voorlaatste gelijkheid de commutatie eigenschap gebruikt hebben. Verder is het eenvoudig in te zien dat ϕ surjectief is (neem $g = h.k$) en ook injectief. Want als $\phi(g) = (e, e)$ dan is $g = e.e = e$. $\square$

We kunnen de moeilijkst te controleren commutatie-eigenschap vervangen door een normaaldeeler voorwaarde.

Stelling 10 (Direct Product stelling, versie 2) Een groep G is isomorf met het directe product van twee deelgroepen H en K als en slechts als

1. $H \triangleleft G$ en $K \triangleleft G$
2. $G = H.K$
3. $H \cap K = \{e\}$

Bewijs. Wegens voorgaande stelling moeten we enkel aantonen dat elementen $h \in H$ en $k \in K$ commuteren. Beschouw de *commutator*

$$[h, k] = h^{-1}.k^{-1}.h.k$$

We kunnen dit element op twee manieren schrijven

$$(h^{-1}.(k^{-1}).h).k = h^{-1}.(k^{-1}.(h).k)$$

Het linkerlid is een element van K (gebruik de normaaldeeler voorwaarde) en het rechterlid is wegens dezelfde eigenschap een element van H . Bijgevolg is dit het eenheidselement en geldt dus dat $h.k = k.h$.

Omgekeerd, als alle elementen van H en K elementsgewijs met elkaar commuteren, dan volgt dat H en K normaaldelers zijn van G . Immers, iedere $g \in G$ kan geschreven worden als $g = h.k$ maar dan geldt bvb. voor elke $k' \in K$ dat

$$(h.k)^{-1}.k'.(h.k) = k^{-1}.h^{-1}.k'.h.k = k^{-1}.k'.k.h^{-1}.h = k^{-1}.k'.k \in K$$

(en een zelfde argumentatie voor H). $\square$

OPGAVE 30. Bewijs dat de verzameling van alle gehele getallen modulo n , $\mathbb{Z}/n\mathbb{Z}$ met de geïnduceerde optelling

$$(a \bmod n) + (b \bmod n) = a + b \bmod n$$

isomorf is met de cyclische groep C_n van orde n .

We gaan alle groepen van orde ≤ 8 bepalen. Omdat 2, 3, 5 en 7 priemgetallen zijn, weten we dat er voor deze ordes enkel de cyclische groep C_p kan optreden, dus blijven de gevallen 4, 6 en 8 over.

OPGAVE 31. Als G een eindige groep is waarin elk element $g \neq e$ orde 2 heeft, dan is G een Abelse groep.

OPGAVE 32. Als G een groep is waarvan alle elementen orde twee hebben, dan heeft G orde 2^n en is G isomorf met

$$G \simeq C_2 \times C_2 \times \dots \times C_2$$

het product van n cyclische groepen van orde 2.

OPGAVE 33. Toon aan dat iedere groep van orde 4 isomorf is met ofwel

$$C_4 \quad \text{ofwel} \quad C_2 \times C_2$$

Definitie 24 De groep $C_2 \times C_2$ wordt ook de **groep van Klein** of de **Klein Vier-ergruppe** genoemd en wordt vaak met V_4 genoteerd.

OPGAVE 34. Toon aan dat een groep G van orde 6 ofwel Abels is en dan isomorf is met

$$G \simeq C_6$$

de cyclische groep van orde 6 ofwel niet-Abels is en dan isomorf is met

$$G \simeq S_3$$

de *symmetrische groep op 3 elementen*, d.i. alle bijecties van $\{1, 2, 3\}$ met samenstelling als groepsbewerking.

Laat ons nu enkele algemene opmerkingen maken over groepen van orde $8 = 2^3$. De orde van de niet-eenheidselementen zijn ofwel 2, ofwel 4 ofwel 8. Als er een element van orde 8 is kan het enkel de cyclische groep C_8 zijn. Als **alle** elementen orde 2 hebben dan weten we uit opgave 32 dat $G \simeq C_2 \times C_2 \times C_2$.

Bijgevolg mogen we onderstellen dat er tenminste één element $a \in G$ is van orde vier. Neem nu een niet-eenheidselement $b \in G$ dat niet bevat is in de deelgroep $\langle a \rangle \subset G$. We beweren dat de elementen

$$G = \{e, a, a^2, a^3, b, a.b, a.b^2, a.b^3\}$$

allen verschillend zijn en dus alle elementen van G geven. Immers,

$$b.a^i = b.a^j \quad \text{impliceert} \quad a^i = a^j \quad \text{en} \quad a^i = b.a^j \quad \text{impliceert} \quad b = a^{j-i} \in \langle a \rangle$$

en het laatste is onmogelijk. Bijgevolg moet b^2 één van deze elementen zijn. Nu is

$$b^2 \notin \{b, a.b, a^2.b, a^3.b\}$$

want anders zou $b = e$ of a een element van kleinere orde zijn. Dus blijven er maar vier mogelijkheden over

$$b^2 \in \{e, a^2, a, a^3\}$$

De gevallen $b^2 = a$ en $b^2 = a^3$ kunnen niet optreden want dan zou de orde van b gelijk zijn aan 8 en dat geval hebben we al uitgesloten. Blijven dus twee mogelijkheden over $b^2 = e$ of $b^2 = a^2$.

OPGAVE 35. Toon aan dat iedere Abelse groep G van orde 8 isomorf is met

$$C_8 \quad \text{ofwel} \quad C_2 \times C_4 \quad \text{ofwel} \quad C_2 \times C_2 \times C_2$$

OPGAVE 36. Stel de vermenigvuldigingstabel op voor deze groepen

- $C_8 = \langle a \mid a^8 = e \rangle$
- $C_4 \times C_2 = \langle a, b \mid a^4 = b^2 = e, a.b = b.a \rangle$
- $C_2 \times C_2 \times C_2 = \langle a, b, c \mid a^2 = b^2 = c^2 = e, ab = ba, ac = ca, bc = cb \rangle$

OPGAVE 37. Als G een niet-Abelse groep is van orde 8, toon aan dat ofwel G isomorf is met de **diheder groep van orde 8**

$$D_4 = \langle a, b \mid a^4 = b^2 = (ab)^2 = e \rangle$$

met vermenigvuldigingstabel

.	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

ofwel isomorf is met de **quaternionen groep**

$$Q = \langle a, b \mid a^4 = e, a^2 = b^2, ba = a^3b \rangle$$

met vermenigvuldigingstabel

.	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

Waarom noemen we deze groep de **quaternionen-groep**? De **Hamilton quaternionen** vormen een niet-commutatief lichaam

$$\mathbb{H} = \mathbb{R}1 + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$

met de vermenigvuldigingsregels

$$ji = -ij = k \quad \text{en} \quad i^2 = j^2 = k^2 = -1$$

en als we de afbeelding beschouwen

$$G \longrightarrow \mathbb{H} \quad a \mapsto i, b \mapsto j$$

zien we dat alle relaties van G gelden tussen i en j en dus kunnen we G opvatten als een eindige groep van omkeerbare quaternionen. We kunnen ook een **matrix-voorstelling** (of **representatie**) van G geven als 2×2 complexe matrices, via de afbeelding

$$G \longrightarrow GL_2(\mathbb{C}) \quad a \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

OPGAVE 38. Verifieer dat dit inderdaad groepmorfismen zijn.

OPGAVE 39. Toon aan dat de diheder groep D_4 de symmetrie groep is van een vierkant. Met a correspondeert rotatie tegenklokwijz over 90° en met b spiegeling over een middelloodlijn op twee zijden.

6. DE 14-15 PUZZEL

Definitie 25 Voor elementen $g_1, g_2, \dots, g_k$ van een groep G noteren we met

$$\langle g_1, g_2, \dots, g_k \rangle$$

de deelgroep van G **voortgebracht** door $\{g_1, g_2, \dots, g_k\}$, dat is de kleinste deelgroep van G die alle g_i bevat. Indien

$$\langle g_1, g_2, \dots, g_k \rangle = G$$

dan noemen we $\{g_1, g_2, \dots, g_k\}$ een **voortbrengend stel** voor G .

Uit de stelling van Cayley volgt dat iedere eindige groep isomorf is met een deelgroep

$$\langle \sigma_1, \sigma_2, \dots, \sigma_k \rangle \subset S_n$$

voor een natuurlijk getal n en permutaties $\sigma_i \in S_n$.

OPGAVE 40. Toon aan dat de symmetrie-groep D_n van een regelmatige n -hoek voortgebracht wordt door een rotatie r en een spiegeling s . Dwz.

$$D_n = \langle r, s \rangle$$

voor r de rotatie met hoek $360^\circ/n$ en s een willekeurige spiegeling.

Definitie 26 Twee elementen g_1 en g_2 van een groep G noemen we **geconjugueerd** indien er een $g \in G$ bestaat zodat

$$g_2 = g \cdot g_1 \cdot g^{-1}$$

De verzameling van alle elementen geconjugueerd met $g_1 \in G$ noemen we de **conjugatie klas** van g_1 en noteren we met (g_1) .

We gaan nu de conjugatie klassen van S_n bepalen en een voortbrengend stel voor S_n vinden.

OPGAVE 41. Toon aan dat twee cycles $\sigma = (a_1, \dots, a_r)$ en $\tau = (b_1, \dots, b_s)$ met elkaar *commuteren* dwz. voldoen aan

$$\sigma \circ \tau = \tau \circ \sigma$$

indien ze disjunct zijn, dwz. als $\{a_1, \dots, a_r\} \cap \{b_1, \dots, b_s\} = \emptyset$.

Definitie 27 Indien een permutatie $\sigma \in S_n$ de cycle decompositie heeft

$$\sigma = (a_1, a_2, \dots, a_{i_1})(b_1, b_2, \dots, b_{i_2}) \dots (x_1, x_2, \dots, x_{i_x})$$

dan noemen we de verzameling $\{i_1, i_2, \dots, i_x\}$ de **cycle-lengten** van σ .

Stelling 11 Twee permutaties $\sigma, \tau \in S_n$ zijn geconjugerd als en alleen als ze dezelfde cycle-lengten hebben.

Bewijs. Neem een cycle

$$h = (a_1, a_2, \dots, a_r) = \begin{pmatrix} a_1 & a_2 & \dots & a_r \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}$$

en een willekeurige permutatie

$$g = \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix}$$

Toon aan dat het geconjugeerde element $g.h.g^{-1}$ gelijk is aan

$$\begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & \dots & a_r \\ a_2 & a_3 & \dots & a_1 \end{pmatrix} \cdot \begin{pmatrix} g(1) & g(2) & \dots & g(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

en deze permutatie is gelijk aan

$$\begin{pmatrix} g(a_1) & g(a_2) & \dots & g(a_r) \\ g(a_2) & g(a_3) & \dots & g(a_1) \end{pmatrix} = (g(a_1), g(a_2), \dots, g(a_r))$$

en dus dezelfde cycle-lengte heeft. Voor meerdere cycles herhalen we dit argument voor elk van de cycles afzonderlijk omdat we tussen alle cycles termen $g^{-1} \circ g$ kunnen plaatsen.

Omgekeerd, neem twee permutaties met zelfde cycle-lengten

$$\begin{cases} \sigma = (a_1, \dots, a_{i_1})(b_1, \dots, b_{i_2}) \dots (z_1, \dots, z_{i_k}) \\ \tau = (\alpha_1, \dots, \alpha_{i_1})(\beta_1, \dots, \beta_{i_2}) \dots (\zeta_1, \dots, \zeta_{i_k}) \end{cases}$$

Merk op dat $\tau = g.\sigma.g^{-1}$ wanneer we als permutatie nemen

$$g = \begin{pmatrix} a_1 & \dots & b_1 & \dots & z_1 & \dots & z_{i_k} \\ \alpha_1 & \dots & \beta_1 & \dots & \zeta_1 & \dots & \zeta_{i_k} \end{pmatrix}$$

(pas de rekenregels toe en zie wat er met elk getal gebeurt)

□

Als we de 1-cycles terug in de cycle-decompositie stoppen zien we dus dat het aantal conjugatieklassen in S_n gelijk is aan het aantal **partities** van n . Een partitie van een positief geheel getal n is een dalende rij positief gehele getallen

$$p = p_1 \geq p_2 \geq p_3 \geq \dots p_k \geq p_{k+1} = 0 \quad \text{zodat} \quad n = p_1 + p_2 + p_3 + \dots + p_k$$

OPGAVE 42. Hoeveel conjugatie klassen zijn er in S_5 ?

Definitie 28 Een **verwisseling** is een permutatie in S_n met cycle-decompositie

$$\sigma = (a, b)$$

Dus, σ stuurt alle elementen uit $\{1, \dots, n\} - \{a, b\}$ naar zichzelf en *verwisselt* a en b . De symmetrische groep S_n bevat juist $\frac{1}{2}n(n-1)$ verschillende verwisselingen en deze vormen juist één conjugatieklasse.

Stelling 12 De $n - 1$ verwisselingen

$$\{(1, 2), (1, 3), \dots, (1, n)\}$$

zijn een voortbrengend stel voor S_n .

Bewijs. We kunnen iedere cycle schrijven als een product van verwisselingen. Immers,

$$(a_1, a_2, a_3, \dots, a_{k-1}, a_k) = (a_1, a_k) \circ (a_1, a_{k-1}) \circ \dots \circ (a_1, a_3) \circ (a_1, a_2)$$

zoals blijkt als we het rechter-lid uitwerken met de rekenregels.

Rest dus enkel aan te tonen dat we elke verwisseling kunnen schrijven als een product in de voortbrengers. Maar, als $a \neq 1 \neq b$,

$$(a, b) = (1, a) \circ (1, b) \circ (1, a)$$

en dus zijn we klaar. $\square$

Laat $\{x_1, \dots, x_n\}$ een verzameling zijn van n variabelen, en $\sigma \in S_n$ een permutatie, dan permuteert σ ook deze verzameling via de actie op de indices

$$\sigma.x_i = x_{\sigma(i)}$$

maar dan werkt σ ook op veeltermen in de variabelen x_i via

$$\sigma.p(x_1, \dots, x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

Bvb. als $p(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ dan is

$$\begin{aligned} (1, 2, 3).p(x_1, x_2, x_3) &= (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \\ &= -(x_1 - x_2)(-(x_1 - x_3))(x_2 - x_3) = p(x_1, x_2, x_3) \end{aligned}$$

en bvb.

$$\begin{aligned} (1, 2).p(x_1, x_2, x_3) &= (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = \\ &= -(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = -p(x_1, x_2, x_3) \end{aligned}$$

Definitie 29 De symmetrie groep van een veelterm $p(x_1, \dots, x_n)$ is n -variabelen is de deelgroep van S_n bestaande uit alle permutaties σ zodat

$$\sigma.p(x_1, \dots, x_n) = p(x_1, \dots, x_n)$$

We noteren deze deelgroep met $\text{sym}(p(x_1, \dots, x_n))$.

OPGAVE 43. Toon aan dat de symmetrie groep $\text{sym}(p(x_1, \dots, x_n))$ van een veelterm inderdaad een deelgroep is van S_n .

OPGAVE 44. Toon aan dat voor $p(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ de symmetrie groep

$$\text{sym}(p(x_1, x_2, x_3)) \simeq C_3$$

isomorf is met de cyclische groep van orde drie, voortgebracht door $(1, 2, 3)$.

Bekijk de veelterm in n variabelen

$$\begin{aligned}\Delta &= \prod_{i < j} (x_i - x_j) \\ &= (x_1 - x_2)(x_1 - x_3) \dots (x_1 - x_n)(x_2 - x_3) \dots (x_{n-1} - x_n)\end{aligned}$$

Omdat een permutatie elk van de factoren naar een andere factor stuurt, eventueel op een tekenverschil na, geldt dat voor alle $\sigma \in S_n$

$$\sigma.\Delta = \pm\Delta$$

We noemen een permutatie σ **even** indien $\sigma.\Delta = \Delta$ en **oneven** indien $\sigma.\Delta = -\Delta$. Voorbeelden van oneven permutaties zijn de verwisselingen (i, j) .

Definitie 30 De **alternerende groep** A_n is de symmetrie groep $\text{sym}(\Delta)$, dwz. de deelgroep van S_n bestaande uit alle even permutaties.

Stelling 13 De alternerende groep A_n heeft orde $\frac{1}{2}n!$ en is voortgebracht door devolgende 3-cycles

$$\{(1, 2, 3), (1, 2, 4), \dots, (1, 2, n)\}$$

A_n is de deegroep van S_n bestaande uit alle permutaties σ die geschreven kunnen worden als product van een even aantal verwisselingen.

Bewijs. We weten al dat we elke permutatie $\sigma \in S_n$ kunne schrijven als een product in de verwisselingen $(1, i)$, bvb.

$$\sigma = (1, i_1) \circ (1, i_2) \circ \dots \circ (1, i_k)$$

Omdat een verwisseling oneven is (dat is $(i, j).\Delta = -\Delta$) volgt dus dat $\sigma \in A_n$ als het aantal verwisselingen k in een schrijfwijze *even* is. Als $\sigma \in A_n$ dan kunnen we in zulke schrijfwijze de verwisselingen twee aan twee samennemen

$$\sigma = \underbrace{(1, i_1) \circ (1, i_2)} \circ \underbrace{(1, i_3) \circ (1, i_4)} \circ \dots \circ \underbrace{(1, i_{k-1}) \circ (1, i_k)}$$

en dus zien we dat A_n voortgebracht is door de permutaties

$$(1, j) \circ (1, i) = (1, i, j)$$

Als $i \neq 2 \neq j$ dan hebben we dat

$$(1, 2, j)^{-1} \circ (1, 2, i) \circ (1, 2, j) = (j, 2, 1) \circ (1, 2, i) \circ (1, 2, j) = (1, i, j)$$

Als $i = 2$ dan is $(1, i, j) = (1, 2, j)$ al van de gewenste vorm en tenslotte als $j = 2$ hebben we

$$(1, i, j) = (1, i, 2) = (1, 2, i) \circ (1, 2, i)$$

en bijgevolg is A_n inderdaad voortgebracht door alle 3-cycles van de vorm $(1, 2, i)$.

Tenslotte geeft de correspondentie

$$\sigma \leftrightarrow (1, 2) \circ \sigma$$

een bijjectie tussen de even en de oneven permutaties. Omdat de orde van S_n gelijk is aan $n!$ en er evenveel even als oneven permutaties zijn geldt dus dat de orde van A_n gelijk is aan $\frac{1}{2}n!$. $\square$



Deze puzzel, waarvoor Sam Loyd een beloning van 1000\$ uitloofde, is waarschijnlijk de populairste puzzel uit de 19de eeuw.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

→ ?

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Gevraagd wordt of je vanuit de beginpositie door te schuiven kan komen tot de situatie met enkel de velden 14 en 15 verwisseld.

Om te beginnen kunnen we iedere positie voorstellen door een element van S_{16} , nl. de permutatie die aan het i -de veld in de beginpositie (het lege vak noteren we met 16) het getal toe te kennen dat in de positie op het i -de veld staat. Een voorbeeld

3	7	5	6
9	1	15	14
12		8	2
4	13	10	11

correspondeert met de permutatie

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 7 & 5 & 6 & 9 & 1 & 15 & 14 & 12 & 16 & 8 & 2 & 4 & 13 & 10 & 11 \end{pmatrix}$$

of in cycle-notatie

$$(1, 3, 5, 9, 12, 2, 7, 15, 10, 16, 11, 8, 14, 13, 4, 6)$$

Een schuifoperatie is een verwisseling van een getal met het lege veld (nummer 16). Dus bvb. de 1 naar onder schuiven is de verwisseling $(1, 16)$ en we krijgen de nieuwe positie door deze verwisseling met de vorige positie te vermenigvuldigen. Immers,

$$(1, 16) \circ (1, 3, 5, 9, 12, 2, 7, 15, 10, 16, 11, 8, 14, 13, 4, 6)$$

geeft de permutatie

$$(1, 3, 5, 9, 12, 2, 7, 15, 10)(4, 6, 16, 11, 8, 14, 13)$$

die wederom devolgende positie voorstelt

3	7	5	6
9		15	14
12	1	8	2
4	13	10	11

Als we vervolgens 9 naar rechts schuiven, passen we de verwisseling $(9, 16)$ toe en bekomen we dus de positie

$$(9, 16) \circ (1, 16) \circ (1, 3, 5, 9, 12, 2, 7, 15, 10, 16, 11, 8, 14, 13, 4, 6)$$

die gegeven wordt door de permutatie

$$(1, 3, 5, 16, 11, 8, 14, 13, 4, 6, 9, 12, 2, 7, 15, 10)$$

die inderdaad correspondeert met de positie

3	7	5	6
	9	15	14
12	1	8	2
4	13	10	11

Elke legale positie kunnen we dus krijgen uit de beginpositie (die correspondeert met de permutatie $()$) door een product te nemen van een aantal verwisselingen van de vorm $(16, i)$. Een legale positie wordt dus gegeven door een permutatie in S_{16} die geschreven kan worden als

$$(16, i_k) \circ \dots \circ (16, i_{j+1}) \circ (16, i_j) \circ \dots \circ (16, i_2) \circ (16, i_1)$$

waarbij op elk moment i_{j+1} een getal is dat aangrenzend ligt aan het lege vak (code 16) van de positie gerepresenteerd door $(16, i_j) \circ \dots \circ (16, i_2) \circ (16, i_1)$.

Bekijk nu de schaakbord kleuring van de 4×4 tabel

0	X	0	X
X	0	X	0
0	X	0	X
X	0	X	0

Na een even aantal zetten (verwisselingen) zal het lege vak op een 0 positie zijn, na een oneven aantal zetten (verwisselingen) op een X positie. Bekijk nu de probleem positie van Sam Loyd

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Het lege vak is terug onderaan rechts, dus als dit een legale positie is (één bekomen vanuit de beginpositie door enkel toelaatbare schuif-operaties uit te voeren) dan moet de bijhorende permutatie geschreven kunnen worden als een even aantal verwisselingen. Evenwel, de positie wordt voorgesteld door de verwisseling

$$(14, 15)$$

en is dus een oneven permutatie in S_{16} . Bijgevolg kan deze positie nooit verkregen worden vanuit de beginpositie!

OPGAVE 45. Is de positie die we voorheen hadden

3	7	5	6
9	1	15	14
12		8	2
4	13	10	11

een legale positie?

OPGAVE 46. Toon aan dat een permutatie even is als en alleen als er een even aantal cycles in de cycle-decompositie zijn van even lengte.

7. DE STELLING VAN CAUCHY (1846)

Augustin Louis Cauchy werd geboren op 21 augustus 1789 in Parijs (Frankrijk) en stierf op 67 jarige leeftijd op 23 mei 1857 in Sceaux nabij Parijs.



De **stelling van Cauchy**, die hij bewees op 57 jarige leeftijd, stelt dat er steeds een element van orde p bestaat voor elke *priemdelers* p van de orde van de groep G .

Definitie 31 Een **actie** van een groep G op een verzameling V is een bewerking

$$G \times V \longrightarrow V \quad (g, v) \mapsto g.v$$

die voldoet aan devolgende voorwaarden

1. voor alle elementen $v \in V$ geldt $e.v = v$
2. voor alle elementen $g, h \in G$ en alle $v \in V$ geldt $(g.h).v = g.(h.v)$

Definitie 32 De **orbit** van een element $v \in V$ onder een actie van de groep G is de deelverzameling van V

$$\mathcal{O}(v) = \{g.v \mid g \in G\}$$

De **stabilizator deelgroep** van een element $v \in V$ onder de actie van een groep G is de deelgroep van G

$$\text{Stab}(v) = \{g \in G \mid g.v = v\}$$

bestaande uit die groepselementen die v ter plaatse laten.

Lemma 1 De **orbits** van een actie van G op een verzameling V zijn de *equivalentie klassen* van de *equivalentie relatie* op V bepaald door

$$v \sim w \quad \text{als en slechts dan als} \quad v = g.w$$

voor een element $g \in G$.

Bewijs. $\sim$ is reflexief want $e.v = v$ dus $v \sim v$. $\sim$ is symmetrisch want als $v \sim w$ dan $v = g.w$ maar dan ook $w = g^{-1}.v$ en dus ook $w \sim v$. Tenslotte is ook $\sim$ transitief want als $v \sim w$ en $w \sim x$ dan hebben we groeps-elementen $g, h \in G$ zodat

$$v = g.w \quad \text{en} \quad w = h.x$$

maar dan geldt ook

$$v = g.w = g.(h.x) = (g.h).x$$

en bijgevolg $v \sim x$. Dus, $\sim$ is inderdaad een equivalentie relatie op V en de equivalentie klasse bepaald door een $v \in V$ is de deelverzameling

$$\{w \in V \mid w \sim v\} = \{g.v \mid g \in G\} = \mathcal{O}(v)$$

In het bijzonder geldt voor alle elementen $v, w \in V$ dat ofwel $\mathcal{O}(v) = \mathcal{O}(w)$ ofwel dat $\mathcal{O}(v) \cap \mathcal{O}(w) = \emptyset$. Verder, vormen de disjuncte orbits een partitie van V . $\square$

Lemma 2 Voor een actie van G op V geldt voor ieder element $v \in V$ dat de afbeelding

$$\mathcal{O}(v) \xrightarrow{\phi} G/\text{Stab}(v) \quad g.v \mapsto g\text{Stab}(v)$$

een bijjectie is tussen de orbit van v en de linker nevenklassen van de stabilizator deelgroep $\text{Stab}(v)$ in G .

Als G een eindige groep is gelden bijgevolg de gelijkheden

1. $\#\mathcal{O}(v) = [G : \text{Stab}(v)]$
2. $\#\mathcal{O}(v)\#\text{Stab}(v) = \#G$

In het bijzonder is het aantal elementen in een orbit steeds een deler van de orde van G .

Bewijs. We moeten eerst aantonen dat de afbeelding ϕ goed gedefinieerd is, d.w.z. dat ze niet afhangt van de gemaakte keuze van g . Immers, het kan zijn dat een punt in de orbit op meerdere manieren geschreven kan worden als $g.v$.

Stel $g.v = h.v$ dan geldt ook dat

$$h^{-1}.(g.v) = h^{-1}.(h.v) = (h^{-1}.h).v = e.v = v$$

en bijgevolg is $h^{-1}.g \in \text{Stab}(v)$ en dus $g \in h\text{Stab}(v)$ en dus ook $g\text{Stab}(v) = h\text{Stab}(v)$ en dus hangt de linker nevenklasse niet af van de gemaakte keuze en is dus ϕ goed gedefinieerd.

ϕ is duidelijk surjectief want als $h\text{Stab}(v)$ een linker nevenklasse is dan wordt het punt $h.v \in \mathcal{O}(v)$ daarop afgebeeld.

ϕ is ook injectief want als $g\text{Stab}(v) = h\text{Stab}(v)$ dan geldt $h^{-1}.g \in \text{Stab}(v)$ en bijgevolg uit de definitie van de stabilizator deelgroep volgt

$$(h^{-1}.g).v = v \quad \text{en dus ook} \quad g.v = h.v$$

dus bepalen $g.v$ en $h.v$ hetzelfde punt van de orbit.

De numerieke gevolgen volgen uit de stelling van Lagrange. $\square$

OPGAVE 47. Als de orde $\#G$ een even getal is, toon aan dat G een element van orde twee bevat.

Stelling 14 (Cauchy (1846)) Als p een priemgetal is dat de orde $\#G$ van een eindige groep G deelt, dan bestaat er een element $g \in G$ van orde p (en bijgevolg heeft G een deelgroep van orde p).

Bewijs. Stel dat $\#G = p \cdot m$ en beschouw devolgende eindige verzameling

$$V = \{(g_1, g_2, \dots, g_p) \mid g_i \in G \text{ en } g_1 \cdot g_2 \cdot \dots \cdot g_p = e\}$$

Hoeveel elementen heeft V ? Als we de eerste $p-1$ elementen $g_1, \dots, g_{p-1}$ vrij kiezen uit alle elementen van G dan moeten we als

$$g_p = (g_1 \cdot g_2 \cdot \dots \cdot g_{p-1})^{-1}$$

nemen. Bijgevolg heeft V juist

$$\#V = (\#G)^{p-1} = p^{p-1} m^{p-1}$$

elementen en, in het bijzonder, is het aantal elementen van V deelbaar door p .

Bekijk nu de cyclische groep van orde p , $C_p = \langle a \mid a^p = e \rangle$ en bekijk de actie van C_p op de verzameling V gedefinieerd door

$$a \cdot (g_1, g_2, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1)$$

dus door het cyclisch permuteren van de termen 1 plaats naar links. Merk op dat a^i op V werkt door alle termen i plaatsen naar links te verschuiven. Verder is $(g_2, \dots, g_p, g_1)$ opnieuw een element van V want

$$g_2 \cdot \dots \cdot g_p \cdot g_1 = g_1^{-1} \cdot (g_1 \cdot g_2 \cdot \dots \cdot g_p) \cdot g_1 = g_1^{-1} \cdot e \cdot g_1 = e$$

dus hebben we wel degelijk een actie van C_p op V .

Uit lemma 2 volgt dat het aantal elementen in elke C_p -orbit een deler moet zijn van de orde van C_p dus ofwel bestaat een orbit uit 1 element ofwel bestaat een orbit uit juist p elementen (hier gebruiken we dat p een priemgetal is).

Er is minstens één orbit met slechts 1 element nl. $\mathcal{O}(e, e, \dots, e)$ en verder weten we (omdat orbits equivalentieklassen zijn) dat

$$\#V = \#\{\text{orbits bestaande uit 1 element}\} + p \cdot \#\{\text{orbits bestaande uit } p \text{ elementen}\}$$

Omdat $\#V$ deelbaar is door p moet ook het aantal orbits dat bestaat uit 1 element deelbaar zijn door p en dus moet er nog een element $v = (g_1, g_2, \dots, g_p) \neq (e, e, \dots, e)$ bestaan met $\mathcal{O}(v) = \{v\}$. Maar dan moet

$$a \cdot (g_1, g_2, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1) = (g_1, g_2, \dots, g_{p-1}, g_p)$$

en bijgevolg $g_1 = g_2 = g_3 = \dots = g_{p-1} = g_p$. Dus, iedere $v \in V$ die een orbit van 1 element is, is van de vorm

$$v = (g, g, \dots, g)$$

Maar, omdat $v \in V$ moet dan ook gelden $g \cdot g \cdot \dots \cdot g = g^p = e$ en dus heeft G inderdaad elementen van orde p . $\square$

Definitie 33 De **conjugatie klasse** van een element $g \in G$ is de deelverzameling van G

$$(g) = \{h^{-1} \cdot g \cdot h \mid h \in G\}$$

De **centralizator deelgroep** van een element $g \in G$ is de deelgroep van G

$$C_G(g) = \{h \in G \mid h.g = g.h\}$$

bestaande uit alle elementen van G die **commuteren** met g .

Lemma 3 Voor ieder element g van een eindige groep G geldt

$$\#(g)\#C_G(g) = \#G$$

In het bijzonder is het aantal elementen van iedere conjugatieklasse een deler van de orde van G .

Bewijs. De groep G werkt op G door *conjugatie*

$$G \times G \longrightarrow V \quad (h, g) \mapsto h.'g \doteq h^{-1}.g.h$$

(we noteren de actie hier met $.$ ' om een onderscheid te maken met de gewone groepswerking in G). Toon aan dat dit inderdaad een actie is, dat de orbit $\mathcal{O}(g)$ de conjugatie klasse (g) is en dat de stabilizator deelgroep voor deze actie $Stab_G(g) = C_G(g)$. Het gestelde volgt dan uit lemma 2. $\square$

OPGAVE 48. Iedere groep G van orde p^2 waarbij p een priemgetal is moet Abels zijn.

Definitie 34 De **fixpunt verzameling** van een groeps-element $g \in G$ voor een actie op een verzameling V is de deelverzameling van V

$$V^g = \{v \in V \mid g.v = v\}$$

bestaande uit die elementen die door de actie van g ter plaatse blijven.

Lemma 4 (orbit tel-stelling) Voor een actie van een eindige groep G op een eindige verzameling V is het aantal orbits gelijk aan

$$\frac{1}{\#G} \sum_{g \in G} \#V^g$$

het gemiddelde van het aantal elementen in de verschillende fixpunt verzamelingen.

Bewijs. We bekijken de deelverzameling van $G \times V$

$$X = \{(g, v) \in G \times V \mid g.v = v\}$$

en gaan nu het aantal elementen $\#X$ op twee manieren berekenen.

Als we onze aandacht op de eerste component g vestigen dan is het aantal koppels (g, v) zodat $g.v = v$ juist gelijk aan de fixpunt verzameling V^g van g . Bijgevolg hebben we dat

$$\#X = \sum_{g \in G} \#V^g$$

Anderzijds, als we de aandacht op de tweede component v vestigen, dan is het aantal koppels (g, v) met $g.v = v$ juist gelijk aan de stabilizator deelgroep $Stab(v)$ en daarom hebben we

$$\#X = \sum_{v \in V} \#Stab(v)$$

Alle elementen w van de orbit $\mathcal{O}(v)$ hebben een geconjugeerde stabilizator deelgroep en bijgevolg geldt voor deze elementen dat $\#Stab(v) = \#Stab(w)$. Immers, als $w = g.v$ dan is

$$g.Stab(v).g^{-1} \subset Stab(w)$$

(want als $h \in Stab(v)$ dan is $(g.h.g^{-1}).w = (g.h).v = g.v = w$). Omgekeerd is ook $Stab(w) \subset g.Stab(v).g^{-1}$ want als $h.w = w$ dan is dus $h.w = h.g.v = g.v = w$ waaruit $g^{-1}.h.g.v = v$.

Maar dan kunnen we de bovenstaande som ook uitschrijven over alle verschillende orbits $G = \mathcal{O}(v_1) \sqcup \dots \sqcup \mathcal{O}(v_t)$

$$\#X = \sum_{v \in V} \#Stab(v) = \sum_{i=1}^t \#\mathcal{O}(v_i) \#Stab(v_i) = \sum_{i=1}^t \#G$$

waar de laatste gelijkheid volgt uit lemma 2. Maar dan hebben we dus (voor t het aantal orbits voor de actie)

$$t\#G = \#X = \sum_{g \in G} \#V^g$$

waaruit het gestelde volgt. $\square$

Stelling 15 (Cauchy) Als $\sigma \in S_n$ een permutatie is met cycle-decompositie van de vorm

$$1^{e_1} 2^{e_2} \dots n^{e_n}$$

(dwz. er zijn juist e_i verschillende cycles van lengte i in de decompositie van σ) dan is het aantal permutaties in S_n dat in de conjugatie klasse $C(\sigma)$ van σ zit gelijk aan

$$\#C(\sigma) = \frac{n!}{1^{e_1} e_1! 2^{e_2} e_2! \dots n^{e_n} e_n!}$$

Bewijs. De cycle-decompositie van σ kan voorgesteld worden als

$$\underbrace{(\cdot)(\cdot) \dots (\cdot)}_{e_1} \underbrace{(\cdot\cdot)(\cdot\cdot) \dots (\cdot\cdot)}_{e_2} \dots$$

en als we deze n spots opvullen met de n elementen $\{1, \dots, n\}$ krijgen we een permutatie in S_n die geconjugerd is met σ . Er zijn $n!$ verschillende manieren om de invulling te doen maar deze corresponderen niet noodzakelijk met verschillende elementen van S_n . Bekijk de e_j verschillende cycles van lengte j . Om te beginnen mogen we die cycles op $e_j!$ verschillende wijzen permuteren en toch hetzelfde element in S_n krijgen. Verder kan ook iedere cycle

$$(a_1, a_2, \dots, a_j)$$

op j verschillende manieren geschreven worden in S_n . Immers is

$$(a_1, a_2, \dots, a_j) = (a_2, a_3, \dots, a_j, a_1) = \dots = (a_j, a_1, \dots, a_{j-1})$$

Dus als we enkel naar de cycles kijken van lengte j dan wordt ieder element van S_n juist $j^{e_j} e_j!$ keren geteld. Als we dit herhalen voor de verschillende cycle-lengten dat weten we dat ieder element van S_n juist $1^{e_1} e_1! 2^{e_2} e_2! \dots n^{e_n} e_n!$ keer voorkomt in onze invul-procedure, waaruit het gestelde volgt. $\square$

OPGAVE 49. Toon aan dat S_4 juist 5 conjugatie-klassen van elementen heeft met als representanten

$$\begin{cases} (1, 2, 3, 4) \text{ de conjugatie-klasse bevat 6 elementen} \\ (1, 2, 3)(4) \text{ de conjugatie-klasse bevat 8 elementen} \\ (1, 2)(3, 4) \text{ de conjugatie-klasse bevat 3 elementen} \\ (1, 2)(3)(4) \text{ de conjugatie-klasse bevat 6 elementen} \\ (1)(2)(3)(4) \text{ de conjugatie-klasse bevat 1 element.} \end{cases}$$

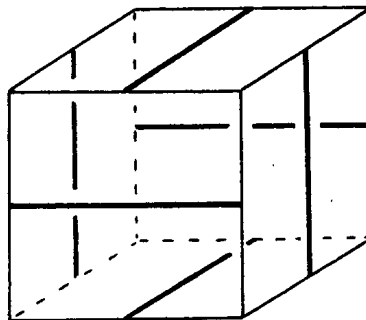
In termen van rotaties van de cubus, bewijs dat volgende rotaties corresponderen met devolgende conjugatie-klassen

$$\begin{cases} r \leftrightarrow (1, 2, 3, 4) \\ r^2 \leftrightarrow (1, 2)(3, 4) \\ s \leftrightarrow (1, 2, 3)(4) \\ t \leftrightarrow (1, 2)(3)(4) \\ I_3 \leftrightarrow (1)(2)(3)(4) \end{cases}$$

OPGAVE 50. Veronderstel dat twee kinderen Alice en Bob een voorraad kubussen hebben en twee verfpotten (rood en blauw). Zij kleuren de kubussen op volgende wijze

- (Alice) : kleur elke zijde van de kubus ofwel rood ofwel blauw.
- (Bob) : Verdeel elk zijvlak in twee gelijke delen met een horizontale of verticale rode of blauwe rechte zodat geen van deze rechten elkaar raakt.

Bob's kleur-regel kan beter begrepen worden met een tekening



Welk van beiden kan de meeste essentieel verschillende gekleurde kubussen produceren? Hierbij noemen we twee kleur-kubussen essentieel verschillend als ze niet door een rotatie-symmetrie in elkaar omgezet kunnen worden.

8. MICROSUDOKU

Micro-Sudoku is de baby-versie van de *klassieke* 9×9 *Sudoku* en bestaat erin een 4×4 tabel te vullen met getallen uit $\{1, 2, 3, 4\}$ zodat iedere rij, iedere kolom en elke 2×2 deeltabel elk van deze vier getallen juist eenmaal bevat. Een goed micro-Sudoku probleem moet een unieke oplossing toelaten.

OPGAVE 51. Toon aan dat het micro-Sudolu probleem links als unieke oplossing rechts heeft

2			3
			1
1			
3			2

2	1	4	3
4	3	2	1
1	2	3	4
3	4	1	2

a	d	b	c
b	c	a	d
4	3	2	1
1	2	3	4

a	b	4	1
c	d	2	3
d	c	3	2
b	a	1	4

1	2	3	4
3	4	1	2
2	1	4	3
4	3	2	1

4	1	d	c
2	3	b	a
3	2	a	b
1	4	c	d

c	b	d	a
a	d	b	c
b	c	a	d
d	a	c	b

4	3	2	1
1	2	3	4
a	d	b	c
b	c	a	d

Een volledig ingevuld micro-Sudoku probleem (bvb. rechts boven) noemen we een *oplossing*. We willen het aantal verschillende oplossingen berekenen voor micro-Sudoku. In 2005 berekende Bertram Felgenhauer het aantal oplossingen voor de klassieke 9×9 Sudoku en vond dat dit aantal gelijk is aan

$$6670903752021072936960 = 2^{20} \times 3^8 \times 5 \times 7 \times 27704267971$$

en de grootste priemdelers blijft een combinatorisch mysterie.

OPGAVE 52. Toon aan dat micro-Sudoku juist

$$288 = 24 \times 12 = 2^5 \times 3^2$$

verschillende oplossingen toelaat.

Er zijn echter buiten hernummeren nog andere verwissel-operaties op de verzameling van alle micro-Sudoku oplossingen.

- (r) : Verwissel de onderste twee rijen.
- (k) : Verwissel de rechter twee kolommen.
- (R) : Verwissel de twee rij-blokken.
- (K) : Verwissel de twee kolom-blokken.
- (S) : Spiegel ten opzichte van de diagonaal.
- (D) : Draai het bord kloksgewijs over 90° .

OPGAVE 53. Ga na dat deze operaties een oplossing naar een oplossing sturen. Toon aan dat de eerste vijf operaties *orde* twee hebben en de laatste *orde* vier. Toon aan dat samenstelling van deze operaties nog steeds een symmetrie-operatie geeft en dat er juist

$$128 = 2^7$$

zulke symmetrie-operaties worden voortgebracht. Vind nog enkele 'verborgen' operaties die niet van de vorm van de vijf basis-operaties zijn maar als een samenstelling van dergelijke kunnen geschreven worden.

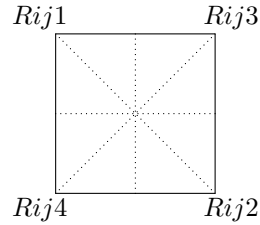
We zullen nu een meer conceptueel bewijs geven om deze orde te bepalen. Laat ons om te beginnen bepalen welke permutaties op de vier rijen een micro-Sudoku oplossing naar een micro-Sudoku oplossing sturen. Bvb. als we de eerste twee rijen verwisselen, bvb. als we de twee rij-blokken verwisselen en ook een combinatie van beiden, bvb. rij 1 naar rij 3, rij 3 naar rij 2, rij 2 naar rij 4 en rij 4 naar rij 1. Toch kunnen niet alle permutaties voorkomen. Bvb. de permutatie $(1, 2, 3)$ zou de oplossing links sturen naar het vierkant rechts dat geen micro-Sudoku oplossing is.

1	2	3	4		2	1	4	3
3	4	1	2		1	2	3	4
2	1	4	3		3	4	1	2
4	3	2	1	→	4	3	2	1

Bijgevolg zijn de toelaatbare rij-permutaties een echte deelgroep van S_4 .

Stelling 16 *De toelaatbare rij-permutaties die een micro-Sudoku oplossing naar een micro-Sudoku oplossing sturen vormen de deelgroep $D_4 \subset S_4$, de dihedrer group van orde 8 bestaande uit alle symmetrieën van een vierkant.*

Bewijs. De correspondentie tussen symmetrieën van een vierkant en toelaatbare rij-permutaties wordt gegeven in volgend diagram



en ga na dat elke symmetrie inderdaad een toelaatbare rij-permutatie geeft. Dit geeft een groep van 8 elementen. Stel dat de toelaatbare rij-permutaties strikt groter zouden zijn dan moesten ze een orde 3 element toelaten maar dan zou de groep S_4 zijn en we hebben al gezien dat dit niet het geval kan zijn. $\square$

Dezelfde argumentatie kunnen we natuurlijk ook toepassen op toelaatbare *kolom*-permutaties en dit geeft opnieuw een groep D_4 .

Stelling 17 *De deelgroep voortgebracht door alle toelaatbare rij- en kolom-permutaties is het directe product*

$$D_4 \times D_4$$

en heeft bijgevolg orde 64.

Bewijs. Het effect van eerst een toelaatbare rij-permutatie μ te doen en vervolgens een toelaatbare kolom-permutatie ν is hetzelfde als eerst ν doen en vervolgens μ . Bijgevolg commuteren de twee deelgroepen elementsgewijs met elkaar. Verder is hun doorsnede enkel $\{e\}$ en dus volgt het gestelde uit de product stelling. $\square$

Laat rij (resp. kol) de groep zijn van alle toelaatbare rij- (resp. kolom-) permutaties. We weten al dat op hernummeren na elke micro-Sudoku oplossing één van devolgende twaalf is

$A_1 =$

1	2	3	4
3	4	1	2
2	1	4	3
4	3	2	1

$A_2 =$

1	2	4	3
3	4	2	1
2	1	3	4
4	3	1	2

$A_3 =$

1	2	4	3
3	4	2	1
4	3	1	2
2	1	3	4

$A_4 =$

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

$B_1 =$

1	2	3	4
3	4	2	1
4	3	1	2
2	1	4	3

$B_2 =$

1	2	3	4
3	4	2	1
2	1	4	3
4	3	1	2

$B_3 =$

1	2	4	3
3	4	1	2
2	1	3	4
4	3	2	1

$B_4 =$

1	2	4	3
3	4	1	2
4	3	2	1
2	1	3	4

$$C_1 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & 3 \\ \hline 3 & 4 & 2 & 1 \\ \hline 4 & 1 & 3 & 2 \\ \hline 2 & 3 & 1 & 4 \\ \hline \end{array} \quad C_2 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 1 & 2 \\ \hline 2 & 3 & 4 & 1 \\ \hline 4 & 1 & 2 & 3 \\ \hline \end{array} \quad C_3 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & 3 \\ \hline 3 & 4 & 2 & 1 \\ \hline 2 & 3 & 1 & 4 \\ \hline 4 & 1 & 3 & 2 \\ \hline \end{array} \quad C_4 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 1 & 2 & 3 \\ \hline 2 & 3 & 4 & 1 \\ \hline \end{array}$$

We zien bvb. dat A_1 en A_2 kol-equivalent zijn maar niet rij-equivalent en dat A_1 en A_3 rij-equivalent zijn maar niet kol-equivalent. Verder is het duidelijk dat alle A_i (resp. B_i of C_i) met elkaar equivalent zijn onder actie van de product groep $\text{rij} \times \text{kol}$. Het is echter misschien minder duidelijk of A_1 equivalent is onder deze groep met B_1 of C_1 . Om dit probleem op te lossen voeren we **invarianten** toe aan een micro-Sudoku oplossing, dwz. data die we kunnen halen uit de oplossing en die hetzelfde blijft als we de oplossing variëren over de $\text{rij} \times \text{kol}$ -groep.

Definitie 35 Een **ongeordende permutatie** van de vier elementen $\{1, 2, 3, 4\}$ is één van devolgende verzamelingen

$$\alpha = \{\{1, 2\}, \{3, 4\}\} \quad \beta = \{\{1, 3\}, \{2, 4\}\} \quad \gamma = \{\{1, 4\}, \{2, 3\}\}$$

waarin we met de verzamelingstekens $\{-, -\}$ aanduiden dat de volgorde van de termen irrelevant is, dwz. bvb. $\{\{3, 4\}, \{1, 2\}\}$ is een andere schrijfwijze voor α .

Het **type** van een micro-Sudoku oplossing X bestaat een geordend paar van paren van ongeordende permutaties, waarbij het eerste paar ongeordende permutaties de rij permutaties geeft van de eerste (resp. tweede) rij-blok van X en het tweede paar ongeordende permutaties de permutaties geeft van de eerste (resp. tweede) kolom-blok van X . Bvb. de oplossingen A_1 resp. B_1 of C_1 zijn van volgend type

$$[A_1] = (\{\alpha, \alpha\}, \{\beta, \beta\}) \quad [B_1] = (\{\alpha, \alpha\}, \{\beta, \gamma\}) \quad [C_1] = (\{\alpha, \gamma\}, \{\beta, \beta\})$$

OPGAVE 54. Toon aan dat iedere micro-Sudoku oplossing een welbepaald type heeft.

OPGAVE 55. Toon aan dat als twee micro-Sudoku oplossingen X en Y equivalent zijn onder de groep $\text{rij} \times \text{kol}$, dan zijn hun types gelijk $[X] = [Y]$. Dwz. het type is een invariant voor de actie van de groep $\text{rij} \times \text{kol}$.

OPGAVE 56. Toon aan dat de oplossingen A_1, B_1 en C_1 niet equivalent met elkaar zijn onder actie van de groep $\text{rij} \times \text{kol}$.

OPGAVE 57. Toon aan dat S (de spiegel-operatie ten opzichte van de diagonaal) geen element is van de groep $\text{rij} \times \text{kol}$.

OPGAVE 58. Toon aan dat D (het bord draaien over 90°) en ook D^3 (het bord draaien over 270°) geen elementen zijn van $\text{rij} \times \text{kol}$, maar D^2 (draaien over 180°) wel.

We kunnen bijgevolg het orde twee element S toevoegen aan de groep $\text{rij} \times \text{kol}$ van orde 64 en krijgen dan een groep van orde tenminste 128. Omdat we al weten dat de orde van sudoku gelijk is aan 128 moeten we zo de hele groep krijgen.

Merk op dat S rijen en kolommen wisselt. Dus als $\sigma \in \text{rij}$ een toelaatbare rij-permutatie is dan is $S \circ \sigma = \tau \circ S$ voor een welbepaalde $\tau \in \text{kol}$ (nl. dezelfde permutatie maar nu op de kolommen ipv. op de rijen). Dus werkt S als een automorfisme van orde twee op $\text{rij} \times \text{kol}$ en krijgen we dat

$$\text{sudoku} = (\text{rij} \times \text{kol}) \rtimes \langle S \rangle \simeq (D_4 \times D_4) \rtimes C_2$$

het **semi-direct product** van $D_4 \times D_4$ met de cyclische groep van orde 2. Dit wil zeggen dat de vermenigvuldiging gegeven wordt door

$$((\sigma, \tau), S^i) \cdot ((\sigma', \tau'), S^j) = (((\sigma, \tau) \cdot S^i(\sigma', \tau')), S^{i+j}) \quad \text{met} \quad S(\alpha, \beta) = (\beta, \alpha)$$

en dus heeft sudoku inderdaad orde 128.

We willen nu ook een invariant bepalen voor micro-Sudoku oplossingen onder de actie van de sudoku groep.

Definitie 36 We noemen twee types $[X]$ en $[Y]$ **Sudoku-equivalent** als ofwel

$$[X] = [Y] \quad \text{ofwel} \quad [X] = [S(Y)]$$

OPGAVE 59. Toon aan dat als twee oplossingen X en Y equivalent zijn onder de actie van sudoku dat dan de types $[X]$ en $[Y]$ Sudoku-equivalent zijn.

OPGAVE 60. Toon aan dat A_1 , B_1 en C_1 niet equivalent met elkaar zijn onder de sudoku-actie.

OPGAVE 61. De **micro-Sudoku groep** is de groep van alle hernummer- en verwissel-operaties. Toon aan dat deze groep juist

$$3072 = 24 \times 128 = 2^{10} \times 3$$

elementen bevat. Verder is deze groep isomorf met

$$\text{sudoku} \times S_4 \simeq ((D_4 \times D_4) \rtimes C_2) \times S_4$$

Merk op dat voor klassieke Sudoku het aantal elementen van de corresponderende Sudoku-groep bepaald werd door Ed Russell en Frazer Jarvis en gelijk is aan

$$9! \times 3359232$$

Zij toonden ook aan dat er juist

$$5472730538$$

essenti el verschillende Sudoku oplossingen zijn, dat is op hernummeren en verwisselen na.

OPGAVE 62. Toon aan dat er juist 2 essenti el verschillende micro-Sudoku oplossingen zijn.

OPGAVE 63. Toon aan dat de micro-Sudoku groep werkt op alle oplossingen en juist 2 *orbits* heeft,   n bestaande uit 96 oplossingen en de andere uit 192 oplossingen.

Vanuit spel-oogpunt is het belangrijkste Sudoku-probleem : gegeven een oplossing, wat is het minimaal aantal 'gegevens' dat nodig is om uniek tot deze oplossing te leiden? Voor klassieke Sudoku is dit probleem nog altijd open. Er zijn oplossingen gekend waarvoor maar 17 gegevens nodig zijn maar niemand heeft een bewijs dat dit het minimale aantal is. Hier een voorbeeld van een Sudoku puzzel met maar 17 gegevens

						2	7
	5			6			
			3				
		7			5	4	
3			2				
4					6		
				4	8		
2		9					
	3						

OPGAVE 64. Toon aan dat voor micro-Sudoku het minimale aantal gegevens voor elke oplossing gelijk is aan 4.

9. DE STELLING VAN JORDAN-HÖLDER (1889)

Als $\{e\} \neq N \triangleleft G$ een niet-triviale normaaldeeler is dan hebben we een epimorfisme

$$G \xrightarrow{\pi} \overline{G} = G/N$$

naar een groep van strikt kleinere orde. Uiteindelijk zouden we graag de groep G opbouwen uit de bouwstenen $\overline{G}$ en N , beiden groepen van orde kleiner dan G . De meest elementaire bouwstenen, de 'elementaire deeltjes' van de groepen zijn die groepen die geen verdere vereenvoudiging door een quotient toelaten, dus groepen zonder niet-triviale normaaldelers. Zulke groepen noemen we *simpel*.

Definitie 37 Een groep G noemen we **simpel** indien G geen echte normaaldelers heeft (d.w.z. enkel G zelf en $\{e\}$ zijn normaaldelers).

OPGAVE 65. Toon aan dat een cyclische groep C_n simpel is als en alleen als n een priemgetal is. we kunnen bijgevolg simpele groepen opvatten als de priemgetallen onder de groepen.

Er zijn echter nog andere simpele groepen! We geven het eenvoudigste voorbeeld van een niet-cyclische simpele groep. Voor conjugatie in de symmetrische groep hebben we gezien dat wanneer

$$\phi = \begin{pmatrix} a_1 & a_2 & \dots & a_m \\ b_1 & b_2 & \dots & b_m \end{pmatrix}$$

dat dan de conjugatie met ϕ van de m -cycle $(a_1, \dots, a_m)$ gelijk is aan

$$\phi \circ (a_1, a_2, \dots, a_m) \circ \phi^{-1} = (b_1, b_2, \dots, b_m)$$

OPGAVE 66. Toon aan dat de alternerende groep A_5 op 5 elementen simpel is.

De alternerende groepen vormen een oneindige familie van simpele groepen.

Stelling 18 De alternerende groep A_n is simpel voor $n \geq 5$.

Bewijs. Stel dat $N \triangleleft A_n$ een niet-triviale normaaldeeler is. We gaan aantonen dat N tenminste één 3-cycle (a_1, a_2, a_3) bevat. Als dit lukt dan volgt dat meteen alle 3-cycles in N zitten en dus moet $N = A_5$ wegens de voortbrengerstelling voor A_n . Immers, veronderstel dat de permutatie

$$\phi = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix} \in A_5$$

dan ook

$$\phi(a_1, a_2, a_3)\phi^{-1} = (b_1, b_2, b_3) \in N$$

Als ϕ geen even permutatie is dan zijn er getallen $c, d \notin \{a_1, a_2, a_3\}$ (hier gebruiken we dat $n \geq 5$) en omdat (c, d) commuteert met (a_1, a_2, a_3) en zowel ϕ als (c, d) oneven permutaties zijn is $\phi(c, d) \in A_5$ en we hebben ook in dit geval dat

$$(\phi(c, d))(a_1, a_2, a_3)(\phi(c, d))^{-1} = \phi(a_1, a_2, a_3)\phi^{-1} = (b_1, b_2, b_3) \in N$$

Rest dus aan te tonen dat N tenminste een drie-cycle bevat. Veronderstel $\gamma \in N$ met cycle decompositie

$$\gamma = (a_1, a_2, \dots, a_m)\lambda$$

met $m \geq 4$. Bekijk de 3-cycle $\sigma = (a_1, a_2, a_3)$ en merk op dat σ en λ met elkaar commuteren (disjuncte cycles). Maar dan zit ook hetvolgende element in N

$$\gamma^{-1} \cdot (\sigma\gamma\sigma^{-1}) = (a_m, a_{m-1}, \dots, a_2, a_1)(a_2, a_3, a_1, a_4, a_5, \dots, a_m) = (a_1, a_3, a_m)$$

en dan zijn we klaar. Dus, als N een element bevat waarvan de cycle-decompositie een cycle bevat met lengte ten minste 4 dan weten we al dat $N = A_n$.

Veronderstel dus dat elk element van N een cycle-decompositie heeft bestaande uit enkel 3-cycles en 2-cycles. Veronderstel $\gamma \in N$ met cycle-decompositie

$$\gamma = (a_1, a_2, a_3)(b_1, b_2, b_3)\lambda$$

en bekijk $\sigma = (a_2, a_3, b_1) \in A_n$, dan is ook hetvolgende element in N

$$\gamma^{-1} \cdot (\sigma\gamma\sigma^{-1}) = (a_3, a_2, a_1)(b_3, b_2, b_1)(a_1, a_3, b_1)(a_2, b_2, b_3) = (a_1, a_2, b_1, a_3, b_3)$$

en heeft dus N wel elementen met hogere cycle-lengte. Dus we mogen onderstellen dat in de cycle-decompositie van elementen van N tenhoogste één 3-cycle zit. Neem dus

$$\lambda = (a_1, a_2, a_3)\lambda \in N$$

waarbij λ enkel bestaat uit 2-cycles. Omdat $\lambda^2 = ()$ volgt dat

$$\gamma^2 = (a_1, a_2, a_3)(a_1, a_2, a_3) = (a_1, a_3, a_2) \in N$$

en zijn we opnieuw klaar. Tenslotte blijft het geval te onderzoeken dat ieder element van N een cycle-decompositie heeft enkel bestaande uit 2-cycles (en omdat het een even permutatie moet zijn, zijn er minstens twee 2-cycles). Schrijf dus

$$\gamma = (a_1, a_2)(b_1, b_2)\lambda \in N$$

en bekijk de 3-cycle $\sigma = (a_2, b_1, b_2)$ (die commuteert met λ). Dan zit ook $\gamma_1 \in N$ met

$$\gamma_1 = \gamma^{-1} \cdot (\sigma\gamma\sigma^{-1}) = (a_1, a_2)(b_1)(b_2)(a_1, b_1)(b_2, a_2) = (b_2, a_1)(a_2, b_1)$$

Neem nu een getal $c \notin \{a_1, a_2, b_1, b_2\}$ (hier gebruiken we wederom dat $n \geq 5$) en bekijk de 3-cycle $\tau = (a_1, b_2, c)$. Dan zit ook hetvolgende element in N

$$\gamma_1^{-1} \cdot (\tau\gamma_1\tau^{-1}) = (b_2, a_1)(a_2, b_1)(c, b_2)(a_2, b_1) = (c, a_1, b_2)$$

en dus zit er opnieuw een 3-cycle in N en zijn we echt klaar. $\square$

OPGAVE 67. Toon aan dat A_3 simpel is maar A_4 niet.

De stelling van Lagrange stelt dat de orde van een deelgroep H van een groep G steeds een deler is van de orde van G . Geldt het omgekeerde ook? Dwz. is er voor iedere

deler van de orde van G een deelgroep met deze orde? Het antwoord is neen. Om dit aan te tonen hebben we eerst een drastische veralgemening nodig van de stelling van Cayley.

Stelling 19 (Cayley on steroids) *Laat H een deelgroep zijn van G van index k , dwz. $[G : H] = k$ en laat S_k de symmetrie groep zijn op de k linker-nevenklassen van H in $G : \{x_1H, \dots, x_kH\}$. Toon aan dat de afbeelding*

$$\theta : G \longrightarrow S_k \quad a \mapsto \theta_a$$

waarbij θ_a de permutatie op de linker-nevenklasse is

$$\theta_a : x.H \mapsto ax.H$$

een groepsmorfisme is. De kern van θ de doorsnede is van alle deelgroepen van G die geconjugeerd zijn met H .

Bewijs. $\theta_{ab}(x.H)$ is de nevenklasse $abx.H$. Anderzijds is

$$abx.H = \theta_a(bx.H) = \theta_a(\theta_b(x.H)) = \theta_a \circ \theta_b(x.H)$$

Omdat dit geldt voor elke nevenklasse $x.H$ zijn dus de permutaties in S_k gelijk dus

$$\theta_{ab} = \theta_a \circ \theta_b$$

maar dit is juist de conditie dat θ een groepsmorfisme is.

De kern van θ bestaat uit die elementen $b \in G$ zodanig dat voor alle $x \in G$ geldt dat

$$bx.H = x.H \quad \text{en dus} \quad b \in x.H.x^{-1}$$

(immers, $x = x.1 = bxh_1$ en dus $b = x.h_1^{-1}.x^{-1}$). Dus moet

$$b \in \cap_{x \in G} x.H.x^{-1}$$

in de doorsnede van alle geconjugeerden van H zitten. Deze redenering omkerend zien we ook dat iedere b in die doorsnede ook een element van de kern van θ is. $\square$

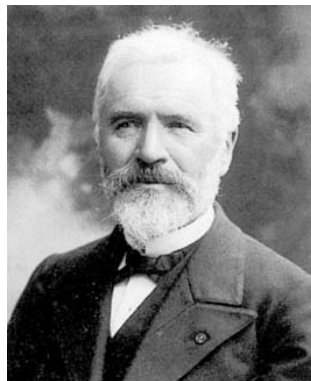
OPGAVE 68. Hoe volgt de gewone versie van Cayley uit deze stelling?

We zijn nu klaar voor de beloofde tegenvoorbeelden tegen het omgekeerde van de stelling van Lagrange.

OPGAVE 69. Toon aan dat de alternerende groep A_5 geen deelgroepen van ordes 30, 20 of 15 heeft en dus een tegenvoorbeeld vormt tegen het omgekeerde van de stelling van Lagrange.

OPGAVE 70. Als G een simpele groep is van orde 168 en H een echte deelgroep is van G . Toon aan dat $[G : H] \geq 6$. Bijgevolg heeft G geen deelgroepen van index 2 of 3.

Marie Ennemond Camille Jordan werd geboren op 5 januari 1838 in Lyon (Frankrijk) en stierf op 84-jarige leeftijd op 22 januari 1922 in Parijs (Frankrijk).



In 1869 bewees hij op 31-jarige leeftijd dat verschillende compositie-rijen dezelfde lengte hebben en dat de ordes van de compositiefactoren gelijk zijn op hernoemen na.

Otto Ludwig Hölder werd geboren op 22 december 1859 in Stuttgart (Duitsland) en stierf op 77-jarige leeftijd op 29 augustus 1937 in Leipzig (Duitsland).



In 1889, op 30-jarige leeftijd vervolgde hij wat we nu kennen als de **stelling van Jordan-Hölder** door aan te tonen dat de compositiefactoren isomorf zijn op hernoemen na.

Definitie 38 Een **compositie rij** van een groep G is een rij deelgroepen

$$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_{r-1} \supset G_r = \{e\}$$

zodanig dat

1. Voor elke $1 \leq i \leq r$ geldt dat $G_i \triangleleft G_{i-1}$ en
2. de bijhorende quotientgroep G_{i-1}/G_i is simpel.

De quotientgroepen G_{i-1}/G_i noemen we **compositie factoren** van de compositie rij (of van G).

Lemma 5 *Iedere eindige groep heeft een compositie rij.*

Bewijs. We doen inductie op $\#G$ (merk op dat als $\#G = 1$ de stelling triviaal voldaan is). Neem N een *maximale* normaaldeeler van G , d.w.z. $N \triangleleft G$ en er is geen echte normaaldeeler van G die N strict bevat.

We beweren dat G/N een simpele groep is. Zoniet bestaat er een echte normaaldeeler $\cup_{m \in M} N.m$ in G/N . Maar dan is $N.M$ een echte deelgroep van G en bovendien een normaaldeeler van G die N strict bevat. Immers, voor alle $g \in G$ en $m \in M$ geldt dat er een $m' \in M$ bestaat zodat

$$(N.g).(N.m) = (N.m').(N.g)$$

maar dan hebben we ook dat

$$g.(N.M) \subset N.M.N.g = N.M.g \quad \text{en} \quad N.M.g \subset N.g.N.M = g.N.N.M = g.N.M$$

Dit is een tegenspraak met de onderstelling dat N een maximale normaaldeeler in G is.

Omdat $\#N < \#G$ mogen we onderstellen dat N al een compositie rij heeft

$$N = G_1 \supset G_2 \supset \dots \supset G_r = \{1\}$$

en dus heeft ook G een compositierij. □

Simpele groepen corresponderen met priemgetallen. Ieder natuurlijk getal is op unieke manier te ontbinden in priemfactoren. De Jordan-Hölder stelling toont aan dat een groeptheoretisch analogon van de priemontbinding bestaat.

De Franse wiskundige C. Jordan bewees in 1869 dat twee compositierijen van een eindige groep gelijke lengte hebben en dat de ordes van de compositiefactoren op hernummen gelijk zijn. De Duitse wiskundige O. Hölder vervolledigde de stelling in 1889 door te bewijzen dat de compositiefactoren op hernummeren na isomorf zijn.

Stelling 20 (Jordan-Hölder (1889)) *De compositiefactoren van twee compositie rijen van een eindige groep G zijn op hernummeren na paarsgewijs isomorf.*

Bewijs. We dienen te bewijzen dat als

$$(1) \quad G = A_0 \supset A_1 \supset \dots \supset A_r = \{e\}$$

en

$$(2) \quad G = B_0 \supset B_1 \supset \dots \supset B_s = \{e\}$$

twee compositierijen zijn van G dat dan de *verzamelingen simpele groepen*

$$\{A_0/A_1, A_1/A_2, \dots, A_{r-1}/A_r\} \quad \text{en} \quad \{B_0/B_1, B_1/B_2, \dots, B_{s-1}/B_s\}$$

gelijk zijn en dus i.h.b. dat $r = s$. Omdat de stelling trivialeerwijs waar is voor alle simpele groepen G geldt ze voor alle groepen met $\#G \leq 3$ en kunnen we dus inductie op de orde $\#G$ van G gebruiken.

We onderscheiden twee gevallen : **(1)** $A_1 = B_1$: Vermits $\#A_1 < \#G$ weten we dat de twee compositierijen

$$A_1 \supset A_2 \supset \dots \supset A_r = \{e\} \quad \text{en} \quad A_1 \supset B_2 \supset \dots \supset B_s = \{e\}$$

dezelfde lengte hebben en dezelfde comositiefactoren op hernummering na. Maar omdat $G/A_1 \simeq G/B_1$ geldt dit dan ook voor G .

(2) $A_1 \neq B_1$: Omdat A_1 en B_1 allebei normaaldivisoren zijn in G geldt ook dat $A_1.B_1$ een normaaldivisor is in G die strict groter is dan zowel A_1 als B_1 , maar omdat beiden maximale normaaldivisoren zijn, weten we dat

$$G = A_1.B_1$$

Bekijk nu $D = A_1 \cap B_1$ dan volgt uit de derde isomorfisme stelling dat

$$(*) \quad G/A_1 \simeq B_1/D \quad \text{en} \quad G/B_1 \simeq A_1/D$$

Omdat G/A_1 en G/B_1 simpele groepen zijn geldt dit ook voor B_1/D en A_1/D en bijgevolg is D een maximale normaaldivisor in zowel A_1 als B_1 . Kies nu een compositie rij voor D

$$D = D_0 \supset D_1 \supset \dots \supset D_v = \{e\}$$

Vergelijken van de twee compositierijen voor A_1 (en inductie gebruiken omdat $\#A_1 < \#G$)

$$A_1 \supset A_2 \supset \dots \supset A_r = \{e\} \quad \text{en} \quad A_1 \supset D \supset D_1 \supset \dots \supset D_v = \{e\}$$

weten we dat $v + 2 = s$ en dat de verzamelingen factoren gelijk zijn

$$\{A_1/A_2, A_2/A_3, \dots, A_{r-1}/A_r\} = \{A_1/D, D/D_1, \dots, D_{v-1}/D_v\}$$

Analoog redeneren met B_1 i.p.v. A_1 levert dat $v + 2 = s$ en gelijkheid van de verzamelingen simpele compositiefactoren van B_1

$$\{B_1/B_2, B_2/B_3, \dots, B_{s-1}/B_s\} = \{B_1/D, D/D_1, \dots, D_{v-1}/D_v\}$$

Maar dan volgt, gebruikmakend van (*) dat ook de compositiefactoren van de twee compositierijen van G gelijk zijn

$$\begin{aligned} \{G/A_1, A_1/A_2, A_2/A_3, \dots, A_{r-1}/A_r\} &= \{G/A_1, A_1/D, D/D_1, \dots, D_{v-1}/D_v\} = \\ \{B_1/D, G/B_1, D/D_1, \dots, D_{v-1}/D_v\} &= \{G/B_1, B_1/D, D/D_1, \dots, D_{v-1}/D_v\} = \\ &= \{G/B_1, B_1/B_2, B_2/B_3, \dots, B_{s-1}/B_s\} \end{aligned}$$

wat we moesten aantonen! $\square$

Definitie 39 Een eindige groep noemen we **oplosbaar** indien al zijn compositiefactoren cyclisch zijn.

OPGAVE 71. Toon aan dat iedere Abelse groep oplosbaar is.

OPGAVE 72. Geef een compositie rij voor A_4 en bewijs dat A_4 (en S_4 oplosbaar zijn).

Definitie 40 Een p -groep is een eindige groep G met orde een macht van p , dus $\#G = p^e$ voor zekere $e \in \mathbb{N}$.

OPGAVE 73. Toon aan dat iedere p -groep oplosbaar is.

10. GALOIS GROEPEN

De notie van een *oplosbare groep* komt van de theorie van oplosbare vergelijkingen. In feite komt de hele groep-theorie voort uit de pogingen om wortels te vinden van vergelijkingen. Daarom is het nuttig om toch iets te weten over deze theorie. Later zul je in de cursus "Galois theorie" veel meer details hierover krijgen.

We beschouwen vergelijkingen met rationale coëfficiënten. Bvb. als $b, c \in \mathbb{Q}$ dan weten we allemaal dat de **wortels** van de **quadratische vergelijking**

$$x^2 + bx + c = 0$$

gegeven worden door

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

en deze wortels liggen enkel in $\mathbb{Q}$ als de **discriminant** van de vergelijking

$$D = b^2 - 4c$$

een kwadraat is in $\mathbb{Q}$. In het algemeen zullen de wortels x_1 en x_2 in een groter **deel-lichaam** liggen van de complexe getallen $\mathbb{C}$ liggen. Als de discriminant geen kwadraat is, dan is het kleinste deellichaam dat beide wortels bevat het **quadratisch lichaam**

$$\mathbb{Q}(\sqrt{D}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$$

elementen van dit lichaam zijn combinaties $r + s\sqrt{D}$ met $r, s \in \mathbb{Q}$ en we kunnen in dit lichaam rekenen doormiddel van de som- en product-regels

$$\begin{aligned}(r + s\sqrt{D}) + (r' + s'\sqrt{D}) &= (r + r') + (s + s')\sqrt{D} \\ (r + s\sqrt{D}) \cdot (r' + s'\sqrt{D}) &= (rr' + ss'D) + (rs' + sr')\sqrt{D}\end{aligned}$$

Dwz. we passen gewoon de rekenregels van complexe getallen toe. Meer algemeen definiëren we

Definitie 41 Een **getal lichaam** K is een deellichaam van de complexe getallen $\mathbb{C}$ dat de rationale getallen $\mathbb{Q}$ bevat en zodanig dat ieder element $k \in K$ een wortel is van een vergelijking met rationale coëfficiënten. Men kan aantonen dat K dan geschreven kan worden als

$$K = \mathbb{Q} \oplus \mathbb{Q}k_1 \oplus \dots \oplus \mathbb{Q}k_n$$

en dat alle $k_i \cdot k_j$ opnieuw van deze vorm zijn. Dit laat dan toe om som en product regels in K uit te werken.

Definitie 42 Een **automorfisme** van een getallichaam K is een bijectie

$$K \xrightarrow{\sigma} K$$

die de identiteit is op het deellichaam $\mathbb{Q}$ (dwz. als $r \in \mathbb{Q}$ dan is $\sigma(r) = r$ en zodanig dat σ sommen en producten respecteert. Dwz. σ voldoet aan

$$\sigma(k + k') = \sigma(k) + \sigma(k') \quad \text{en} \quad \sigma(k \cdot k') = \sigma(k) \cdot \sigma(k')$$

voor alle $k, k' \in K$. Het is duidelijk dat als σ en τ automorfismen zijn dat dan ook hun samenstelling $\sigma \circ \tau$ een automorfisme is.

Bijgevolg vormt de verzameling van alle automorfismen van een getallichaam K een groep : de **Galois groep van K** .

OPGAVE 74. Toon aan dat de Galois groep van het getallichaam $\mathbb{Q}(\sqrt{D})$ de cyclische groep is van orde twee met als voortbrenger

$$\sigma(r + s\sqrt{D}) = r - s\sqrt{D}$$

In volle renaissance periode in Italië werden wedstrijden georganiseerd tussen vergelijking-oplossers. Zo wist Pacioli al in 1494 dat de vergelijking

$$x^3 + px = q \quad \text{met } p, q \in \mathbb{Q}$$

een wortel heeft

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

en later vonden Scipio del Ferro en Niccolo Tartaglia formules voor de wortels van alle vergelijkingen van graad vier.

Definitie 43 We zeggen dat een n -de graadsvergelijking met rationale coëfficiënten

$$x^n + q_1 x^{n-1} + \dots + q_n = 0$$

oplosbaar is met behulp van radicalen als we alle wortels kunnen vinden door geïtereerd wortel-trekken.

Pas in 1824 toonde Niels Hendrik Abel aan dat een algemene 5-de graadsvergelijking niet opgelost kan worden met behulp van radicalen. Het algemene probleem kon pas aangepakt worden wanneer Evariste Galois het groep-concept invoerde. Hij bewees in 1832

Stelling 21 (Galois) Een n -de graadsvergelijking met rationale coëfficiënten

$$x^n + q_1 x^{n-1} + \dots + q_n = 0$$

is oplosbaar met behulp van radicalen als en slechts als de Galois groep van het getallichaam K , dat ontstaat door aan $\mathbb{Q}$ alle wortels van de vergelijking toe te voegen, een oplosbare groep is.

We zullen het basis-idee van Galois theorie illustreren aan de hand van een eenvoudig voorbeeld. Beschouw de vierde graads vergelijking

$$x^4 - 2 = 0$$

dan zijn de wortels van deze vergelijking

$$\zeta = \sqrt[4]{2} \quad i\zeta \quad -i\zeta \quad \text{en} \quad -\zeta$$

want over de complexe getallen hebben we

$$x^4 - 2 = (x - \zeta)(x - i\zeta)(x + i\zeta)(x + \zeta)$$

We willen nu het kleinste getallichaam construeren dat *alle* wortels bevat.

OPGAVE 75. Toon aan dat het lichaam $\mathbb{Q}(\sqrt[4]{2})$ dat ontstaat door aan $\mathbb{Q}$ alle machten van $\sqrt[4]{2}$ toe te voegen, dwz.

$$\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q} \oplus \mathbb{Q}\zeta \oplus \mathbb{Q}\zeta^2 \oplus \mathbb{Q}\zeta^3$$

niet alle wortels van $x^4 - 2 = 0$ bevat.

Bijgevolg moeten we minstens i nog toevoegen aan het lichaam $\mathbb{Q}(\sqrt[4]{2})$.

OPGAVE 76. Het minimale getallichaam dat alle wortels van $x^4 - 2 = 0$ bevat is het lichaam

$$K = \mathbb{Q}(i, \sqrt[4]{2}) = \mathbb{Q} \oplus \mathbb{Q}\zeta \oplus \mathbb{Q}\zeta^2 \oplus \mathbb{Q}\zeta^3 \oplus \mathbb{Q}i \oplus \mathbb{Q}i\zeta \oplus \mathbb{Q}i\zeta^2 \oplus \mathbb{Q}i\zeta^3$$

We noemen K het **splijtlichaam** van $x^4 - 2 = 0$.

We willen nu de Galois groep van het getallichaam $K = \mathbb{Q}(i, \zeta)$ bepalen. Een automorfisme stuurt de wortels van een vergelijking met rationale coëfficiënten naar eventueel andere wortels van dezelfde vergelijking. Omdat K over $\mathbb{Q}$ is **voortgebracht** door de twee elementen ζ en i volstaat het voor ieder automorfisme de beelden van ζ en i te kennen om de actie op elk element te kennen (gebruik dat automorfismen som, verschil, product en breuk respecteren). Nu heeft

$$x^4 - 2 = 0 \quad \text{als wortels } \{\zeta, i\zeta, -\zeta - i\zeta\} \quad \text{en} \quad x^2 - 1 = 0 \quad \text{als wortels } \{i, -i\}$$

en omdat we weten dat wortels naar eventueel andere wortels van dezelfde vergelijking dienen gestuurd te worden kunnen we volgende automorfismen bekijken.

$$\sigma : \sigma(i) = i, \sigma(\zeta) = i\zeta \quad \text{en} \quad \tau : \tau(i) = -i, \tau(\zeta) = \zeta$$

OPGAVE 77. Toon aan dat de Galois groep van $K = \mathbb{Q}(i, \zeta)$ voortgebracht is door σ en τ die voldoen aan de relaties

$$\sigma^4 = \tau^2 = id \quad \text{en} \quad (\sigma \circ \tau)^2 = id$$

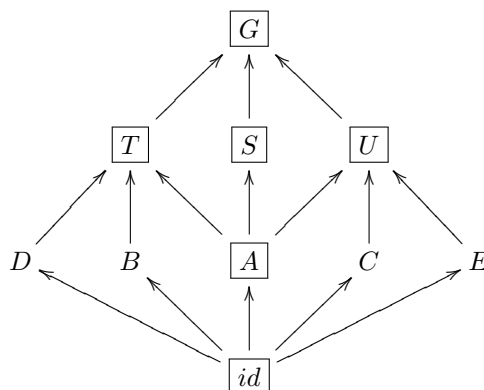
en bijgevolg is de Galois group

$$Gal(K/\mathbb{Q}) \simeq D_4$$

isomorf met de diheder groep op 8 elementen.

Het is natuurlijk geen toeval dat de orde van deze Galois groep gelijk is aan de dimensie van het splijtlichaam. Het verband tussen de Galois groep (en zijn deelgroepen) en het splijtlichaam (en zijn deellichamen) is nog veel sterker.

OPGAVE 78. Geef alle deelgroepen van de Galois group $G = \text{Gal}(K/\mathbb{Q})$ en toon aan dat devolgende inclusies gelden



waarbij de geboxte entries de normaaldelers van G zijn.

Stelling 22 (Hoofdstelling Galois theorie) Laat K een splijtlichaam zijn van een veelterm met coëfficiënten in $\mathbb{Q}$. Dan bestaat er een bijectie tussen

- Deelgroepen $H \subset \text{Gal}(K/\mathbb{Q})$ van orde k , en
- Deellichamen $\mathbb{Q} \subset L \subset K$ zodat $\dim_L(K) = k$

Deze Galois correspondentie wordt gegeven door aan een deelgroep het **invarianten lichaam** te corresponderen

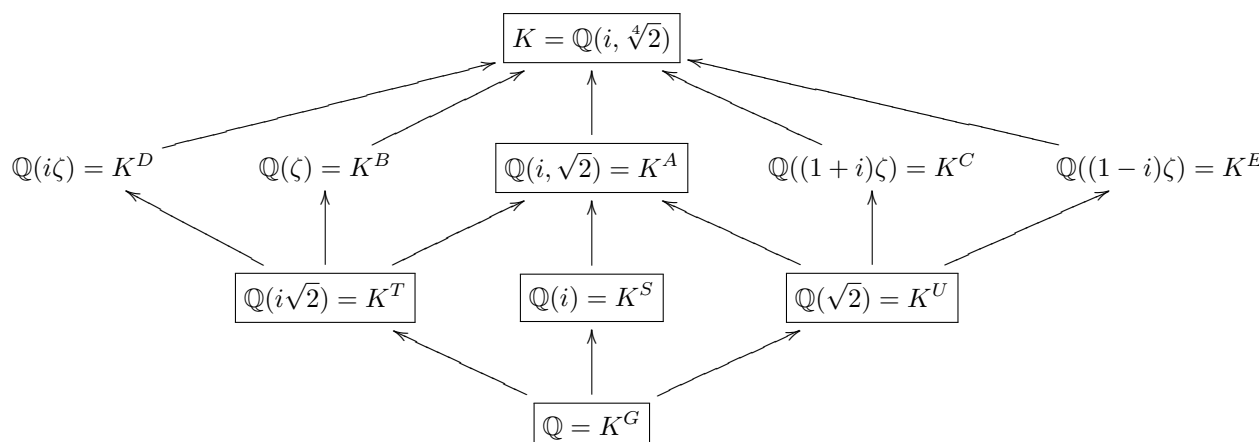
$$K^H = \{k \in K \mid \sigma(k) = k \forall k \in H\}$$

Onder deze correspondentie corresponderen normaaldelers N met splijtlichamen L zodanig dat de bijhorende Galois groep

$$\text{Gal}(L/\mathbb{Q}) = \text{Gal}(K/\mathbb{Q})/N$$

de quotient-groep is.

Bijgevolg is de Galois correspondentie omkerend. Laat ons de invarianten lichamen geven in het voorbeeld



OPGAVE 79. Voor $C = \{1, \sigma\tau\}$ toon aan dat

$$K^C = \mathbb{Q}((1+i)\zeta)$$

Tenslotte kan men aantonen dat als een splijtlichaam $L \subset K$ een cyclische Galois groep heeft, we dan K kunnen krijgen door aan L een wortel toe te voegen. Hieruit volgt het Galois criterium voor oplosbaarheid door radicalen.

Ook het bewijs van Abels resultaat dat er graad vijf vergelijkingen zijn die niet oplosbaar zijn met behulp van radicalen gebruikt groep-theorie.

Stelling 23 (Abel) *De algemene vijfde graads vergelijking met rationale coëfficiënten is niet oplosbaar door middel van radicalen.*

Bewijs. Neem als 5-de graads vergelijking

$$x^5 - 6x + 3 = 0$$

Uit functie onderzoek blijkt dat deze 3 reële wortels heeft en twee (noodzakelijk complex toegevoegde) complexe wortels. Bekijk nu het splijtlichaam K van deze vergelijking. Een automorfisme stuurt wortels naar eventueel andere wortels en omdat er juist 5 wortels zijn weten we dat de Galois groep een deelgroep is

$$\text{Gal}(K/\mathbb{Q}) \subset S_5$$

van alle permutaties op de 5 wortels. Voeg nu 1 van de wortels toe aan $\mathbb{Q}$, dan krijgen we een lichaam $\mathbb{Q} \subset L \subset K$ waarvan de dimensie over $\mathbb{Q}$ juist gelijk is aan 5, maar dan is de totale dimensie

$$5 | \dim_{\mathbb{Q}}(K)$$

en omdat deze dimensie gelijk is aan de orde van de Galois groep, is vijf een deler van de orde van $\text{Gal}(K/\mathbb{Q})$. Uit de stelling van Cauchy volgt dan dat er een automorfisme moet zijn van orde vijf. Eventueel op hernummeren na van de wortels mogen we dus veronderstellen dat

$$c = (1, 2, 3, 4, 5) \in \text{Gal}(K/\mathbb{Q}) \subset S_5$$

Er is nog een ander automorfisme : complex toevoegen laat de reële wortels vast en verwisselt te twee complexe wortels, dus is er ook minstens één verwisseling

$$s = (i, j) \in \text{Gal}(K/\mathbb{Q}) \subset S_5$$

Maar dan is

$$\langle c, s \rangle = S_5 \subset \text{Gal}(K/\mathbb{Q}) \subset S_5$$

en dus is de Galois groep gelijk aan S_5 . Evenwel, S_5 is niet oplosbaar vermits er de simpele groep A_5 als normaaldeeler inzit. Dus, de gegeven 5-de graads vergelijking is niet oplosbaar met radicalen. $\square$

OPGAVE 80. Als bvb. $s = (1, 2)$, toon aan dat inderdaad

$$\langle s = (1, 2), c = (1, 2, 3, 4, 5) \rangle = S_5$$

Laat ons eindigen met een open probleem : **Is iedere eindige groep G de Galois groep van een splijtlichaam van een vergelijking met rationale coëfficiënten?** Dit wordt het inverse Galois probleem genoemd en is één van de belangrijkste openstaande problemen in de wiskunde.

11. DE STELLINGEN VAN SYLOW (1872)

Peter Ludwig Mejdell Sylow werd geboren op 12 december 1832 in Cristiania, nu Oslo (Noorwegen) en stierf er op 85-jarige leeftijd op 7 september 1918.



De **stelling van Sylow**, die hij op 40-jarige leeftijd bewees, stelt dat een partiële omgekeerde van de stelling van Lagrange geldt. Als p^a de hoogste p -macht is die de orde van een eindige groep G deelt, dan heeft G een deelgroep van orde p^a . Dit resultaat heeft verschillende belangrijke gevolgen in de theorie van eindige groepen.

Definitie 44 Voor een priemgetal p dat de orde $\#G = p^a k$ van een eindige groep G deelt zodat k niet deelbaar is door p , noemen we een deelgroep $S \subset G$ een **p -Sylow deelgroep** als de orde van S gelijk is aan $\#S = p^a$.

In 1872 bewees de Noorse wiskundige L. Sylow het bestaan en essentieel uniciteit (op conjugatie na) van p -Sylow deelgroepen voor alle priemdelers van de orde van G .

Lemma 6 Als G een eindige groep is en p een priemgetal zodat p^b (met b een positief getal) de orde $\#G$ deelt, dan heeft G deelgroepen van orde p^b en het aantal m verschillende zulke deelgroepen voldoet aan $m \equiv 1 \pmod{p}$.

Bewijs. Schrijf $\#G = n = p^b z$ (het mag dat p een deler is van z) en bekijk de verzameling

$$\mathcal{K} = \{K_1, K_2, \dots, K_r\}$$

van alle deelverzamelingen van G die bestaan uit juist p^b elementen. Uit elementaire combinatoriek weten we dat het aantal elementen van $\mathcal{K}$ gelijk is aan

$$\#\mathcal{K} = r = \binom{n}{p^b} = \frac{n!}{p^b!(n - p^b)!}$$

Omdat voor elke deelverzameling $K \subset G$ en ieder element $g \in G$ we hebben dat $\#K = \#K.g$ hebben we een actie van G op $\mathcal{K}$ gegeven door

$$G \times \mathcal{K} \longrightarrow \mathcal{K} \quad (g, K_i) \mapsto K_i.g = K_j$$

en we gaan de orbits van deze actie bestuderen.

Om te beginnen, als $g \in K$ dan is $K.g^{-1} \in \mathcal{O}(K)$ en $e \in K.g^{-1}$. We mogen dus veronderstellen dat

$$\mathcal{K} = \mathcal{O}(K_{i_1}) \sqcup \dots \sqcup \mathcal{O}(K_{i_s})$$

met voor alle $1 \leq j \leq s$ dat het eenheidselement $e \in K_{i_j}$. Neem nu K één van deze K_{i_j} . We weten al dat

$$\#\mathcal{O}(K) = [G : \text{Stab}(K)]$$

en omdat $K.\text{Stab}(K) = K$ en $e \in K$ hebben we dat $\text{Stab}(K) \subset K$. We kunnen nu een equivalentierelatie definiëren op K via

$$k \sim k' \quad \text{als en slechts dan als} \quad k' = k.s \text{ voor een } s \in \text{Stab}(K)$$

(ga na dat dit inderdaad een equivalentierelatie is). Omdat $K = K.\text{Stab}(K)$ hebben we dus een partitie

$$K = k_1.\text{Stab}(K) \sqcup \dots \sqcup k_t.\text{Stab}(K)$$

Elk van deze $k_i.\text{Stab}(K)$ heeft juist $\#\text{Stab}(K)$ elementen (immers, als $k_i.s = k_i.s'$ dan $s = k_i^{-1}.k_i.s = k_i^{-1}.k_i.s' = s'$). Bijgevolg hebben we

$$p^b = \#K = t\#\text{Stab}(K)$$

dus is $\#\text{Stab}(K) = p^c$ met $c \leq b$.

Als $c < b$ dan kan $\mathcal{O}(K)$ geen deelgroep van G bevatten. Veronderstel immers dat dit wel het geval is en laat $K' \in \mathcal{O}(K)$ een deelgroep zijn, dan is $\mathcal{O}(K) = \mathcal{O}(K')$ en $\#\text{Stab}(K) = \#\text{Stab}(K')$ (want beiden zijn geconjugeerd). Maar, omdat K' een deelgroep is geldt $K'.K' = K'$ en dus $K' \subset \text{Stab}(K')$ dus heeft de stabilizator tenminste orde p^b , een tegenspraak.

Als $c = b$ en omdat $\text{Stab}(K) \subset K$ hebben we dat $\text{Stab}(K) = K$ en dus is K een deelgroep van G van orde p^b . Bijgevolg is

$$\#\mathcal{O}(K) = [G : \text{Stab}(K)] = [G : K] = z$$

en dus is het aantal elementen in zo'n orbit *minimaal*. De orbit $\mathcal{O}(K)$ in $\mathcal{K}$ bestaat uit rechternevenklassen

$$\mathcal{O}(K) = \{K.w_1, K.w_2, \dots, K.w_z\}$$

van K in G en slechts één van deze (nl. K) kan een deelgroep zijn.

Bijgevolg hebben we dat het aantal deelgroepen m van orde p^b in G gelijk is aan het aantal minimale orbits voor de G -actie op $\mathcal{K}$. (We hebben nog *niet* bewezen dat $m > 0$).

Merk op dat het aantal elementen van $\mathcal{K}$ in minimale orbits gelijk is aan mz en dat het aantal elementen in elke niet-minimale orbit deelbaar is door pz , bijgevolg is

$$\#\mathcal{K} = r \equiv mz \pmod{pz}$$

Merk op dat r niet afhangt van de groep G zolang die van orde p^bz is. Als we de rol van de groep G willen benadrukken kunnen we schrijven

$$r = m_G z + k_G p z$$

voor zekere $m_G, k_G \in \mathbb{N}$.

Bekijk nu de cyclische group $C = \langle x \mid x^{p^b z} \rangle$ van orde $p^b z$ dan heeft C een unieke deelgroep van orde p^b (nl. deze voortgebracht door x^z) en bijgevolg is $m_C = 1$ en hebben we

$$r = z + k_C p z$$

Als we dit vergelijken met de gelijkheid voor de groep G krijgen we

$$m_G z + k_G p z = z + k_C p z$$

en we kunnen beide leden door z delen en verkrijgen

$$m_G + k_G p = 1 + k_C p$$

en dus is inderdaad m_G (het aantal minimale orbits en ook het aantal deelgroepen van G van orde p^b) congruent met 1 modulo p . $\square$

Stelling 24 (Sylow (1872)) *Zij G een eindige groep van orde $\#G = p^a k$ met k niet deelbaar door p , dan gelden volgende uitspraken*

1. *Er bestaat tenminste één Sylow p -deelgroep van orde p^a .*
2. *Alle p -Sylow deelgroepen van G zijn geconjugeerd aan elkaar.*
3. *Het aantal m van alle p -Sylow deelgroepen van G voldoet aan*

$$m \equiv 1 \pmod{p} \quad \text{en} \quad m \mid k$$

Bewijs. Uitspraak 1 en het eerste deel van uitspraak 3 volgen direct uit lemma 6. Voor de tweede uitspraak bewijzen we iets algemener: laat P een p -Sylow deelgroep zijn van G en laat H een deelgroep van G zijn van orde p^b , dan bestaat er een $g \in G$ zodat

$$H \subset g^{-1} P g$$

Laat V de verzameling van alle rechternevenklassen Pg van P in G zijn en bekijk op V de actie van H via

$$H \times V \longrightarrow V \quad (h, Pg) \mapsto Pgh$$

Omdat de orde van H een macht van p is, is het aantal elementen in iedere orbit voor deze actie ofwel 1 ofwel een macht van p . Anderzijds, is het totale aantal elementen van V gelijk aan $[G : P] = z$ en is dus niet deelbaar door p . Dus moet er minstens één orbit zijn bestaan uit slechts 1 element, dus er bestaat een $g \in G$ met

$$PgH = Pg$$

en omdat $e \in P$ volgt $gH \subset Pg$ of nog $H \subset g^{-1}Pg$ wat we wilden bewijzen.

Hieruit volgt 2 onmiddellijk omdat elke twee p -Sylow deelgroepen orde p^a hebben. Rest nog het tweede deel van 3 te bewijzen. Neem

$$\mathcal{P} = \{P_1, \dots, P_m\}$$

de verzameling van alle p -Sylow deelgroepen van G en beschouw de actie van G op $\mathcal{P}$ gegeven door

$$G \times \mathcal{P} \longrightarrow \mathcal{P} \quad (g, P) \mapsto g^{-1}Pg$$

Uit 2 volgt dat deze actie **transitief** is (d.w.z. er is slechts 1 orbit) maar dan moet m een deler zijn van $\#G = p^a k$ en omdat m geen deler is van p^a (want $m \equiv 1 \pmod{p}$) moet m een deler zijn van k en zijn we klaar! $\square$

OPGAVE 81. Toon aan dat een Abelse groep G isomorf is met het directe product van zijn p -Sylow deelgroepen.

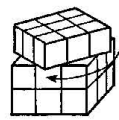
OPGAVE 82. Stel dat p en q priemgetallen zijn met $p < q$ en $q \not\equiv 1 \pmod{p}$. Toon aan dat als G een groep is van orde pq dat dan G een cyclische groep is.

OPGAVE 83. Toon aan dat er geen simpele groep van orde 200 bestaat.

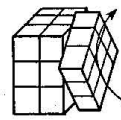
OPGAVE 84. Toon aan dat er geen simpele groep van orde 30 bestaat.

12. DE RUBIK KUBUS

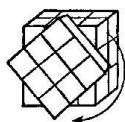
De Rubik kubus is een draai-puzzel die tot doel heeft de kubus terug te herstellen in de beginpositie waarin elk van de 6 zijvlakken een verschillende kleur heeft. De basis toegelaten draaiingen zijn devolgende die we steeds met de zgn. *Singmaster notatie* zullen aanduiden U, R, F, L, B, D



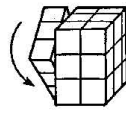
Up Clockwise



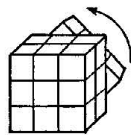
Right Clockwise



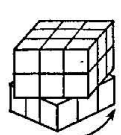
Front Clockwise



Left Clockwise



Back Clockwise



Down Clockwise

en hun inversen, bvb. de opper-laag een draai in tegenwijzerzin geven zullen we noteren met U^{-1} . Merk op dat onder deze toegelaten bewegingen de middelste vierkanten in ieder zijvlak niet veranderen. We kunnen dus steeds doorheen het spel vastleggen wat het opper (U), beneden (D), voor (F), achter (B), linker (L) en rechter (R) vlak is door vanaf het begin ze vast te leggen door de kleuren van deze middelste vierkanten.

OPGAVE 85. Hoeveel verschillende posities zijn mogelijk vanuit de beginpositie?

Los de Rubik cubus op!

Strategie : (dit is slechts één van de vele oplos strategieën voor de Rubik cubus)

We noteren een *cubicle* dat is wat zichtbaar is van een klein kubusje met de zichtbare zijvlakken. Bvb. uf noteert de cubicle in de bovenste laag en het meest naar voor. Een hoekpunt-cubicle wordt door drie zijvlakken genoteerd. Bvb. drb is het hoekpunt-cubus rechts vanonder. In deze notatie speelt de ordening van de zijvlakken soms een rol in

operaties. Als we schrijven

$$rb \longrightarrow uf \quad \text{danwel} \quad rb \longrightarrow fu$$

bedoelen we in het eerste geval dat de rechter-zijvlak kleur gaat naar de u -positie van uf (in het tweede geval gaat ze naar de f -positie). Analoog voor hoekpunt-kubussen is er soms een essentieel verschil tussen bvb. drb en dbr . In ons algoritme zal het al dan niet cyclisch zijn van de gewenste operatie belangrijk zijn.

stap 1 : breng 1 vlak (bvb. wit) in orde behalve 1 hoek. Dit vlak zal het ondervlak D worden en de niet herstellde hoek zal de drb cubicle zijn. Deze operatie moet voor iedereen doenbaar zijn zonder bijkomende uitleg.

stap 2 : We gaan de 3 cubicles berstellen in de middelste laag die liggen boven de herstellde onderste hoekpunt-cubicles. Als de gewenste cubicle al op de top layer ligt doen we

- roteer middenlaag zodat de te veranderen cubicle in fl positie is.
- roteer onderste laag zodat de niet herstellde cubicle in fld ligt.
- roteer bovenlaag zodat de gewenste cubicle in ur ligt.
- Indien $ur \longrightarrow fl$ doe $L^{-1}U^2L$. Indien $ru \longrightarrow fl$ doe FUF^{-1} .

Indien de gewenste cubicle in de middelste laag ligt breng je die naar de bovenlaag door de operaties

- roteer middenlaag zodat gewenste cubicle in fl positie is.
- roteer onderlaag zodat niet herstellde cubicle in fld is.
- doe FU^2F^{-1} .

stap 3 : UL, UF en UB herstellen (in die volgorde). De niet herstellde onder cubicle wordt steeds veronderstelt in de positie rd te liggen. We gaan eerst gewenste cubicle in rb leggen door de operaties

- $ul \longrightarrow rb$ door $BUB^{-1}U^{-1}$
- $uf \longrightarrow rb$ door $BU^2B^{-1}U^2$
- $ub \longrightarrow rb$ door $U^{-1}BUB^{-1}$
- $ur \longrightarrow rb$ door $BU^{-1}B^{-1}U$

Daarna brengen we de rb cubicle naar de gewenste positie door de operaties

- $rb \longrightarrow uf$ door $U^2BU^2B^{-1}$
- $rb \longrightarrow fu$ door $U^{-1}R^{-1}UR$
- $rb \longrightarrow ul$ door $UBU^{-1}B^{-1}$
- $rb \longrightarrow lu$ door $U^2R^{-1}U^2R$

- $rb \longrightarrow ub$ door $BU^{-1}B^{-1}U$
- $rb \longrightarrow bu$ door $UR^{-1}U^{-1}R$

stap 4 : UR in orde brengen. Hiervoor zijn enkele mogelijkheden :

- ur en rb zitten al goed. Ga naar volgende stap.
- ur en rb zitten op juiste cubicle maar geflipt. Doe dan eerst $ru \longrightarrow br$ door $BU^{-1}B^{-1}U$ en vervolgens $br \longrightarrow ur$ door $R^{-1}URU^{-1}$.
- ur zit op cubicle rb . Dan zijn er twee mogelijkheden :
 - $rb \longrightarrow ur$ door $BUB^{-1}UBUB^{-1}U^2$
 - $br \longrightarrow ur$ door $U^{-1}R^{-1}U^{-1}RU^{-1}R^{-1}U^{-1}RU^{-1}$

stap 5 : We brengen de top-hoek cubicles op de juiste positie, eventueel geflipt!

- niet herstellende ondercubicle in drb positie.
- draai bovenlaag zodat gewenste cubicle in ufl positie ligt en doe

$$ufl \longrightarrow rbd \quad \text{door} \quad F^{-1}D^2F$$

- draai bovenlaag zodat de doelcubicle in ufl positie is en doe

$$rdb \longrightarrow ufl \quad \text{door} \quad F^{-1}D^2F$$

stap 6 : Herstel de geflipte hoekcubicles. Dit moet in PAREN gedaan worden, steeds een hoekcubicle die cyclisch hersteld moet worden (bv $ufl \longrightarrow flu$) en een hoekcubicle die acyclisch hersteld moet worden (bv $ufl \longrightarrow luf$). De gehele operatie bestaat uit

- roteer de cubus zodat beide cubicles in de bovenlaag liggen en de cubicle die cyclisch getwist moet worden in de ufl positie ligt.
- $ufl \longrightarrow flu$ door $LD^2L^{-1}F^{-1}D^2F$
- roteer de bovenlaag zodat de cubicle die acyclisch getwist moet worden in de ufl positie ligt.
- $ufl \longrightarrow luf$ door $F^{-1}D^2FLD^2L^{-1}$

Herhaal deze paarsgewijze operatie tot alle hoekcubicles hersteld zijn.

OPGAVE 86. Er zijn 8 hoek cubicles and 12 zijde cubicles, dus kunnen we aan elke operatie in de Rubik groep Rubik een permutatie in S_{20} associëren. Toon aan dat het beeld van dit groepsmorfisme

$$\text{Rubik} \longrightarrow S_{20}$$

bevat is in de alternerende deelgroep A_{20} .

OPGAVE 87. In de oplos strategie komen we vaak **commutatoren**

$$[\sigma, \tau] = \sigma \cdot \tau \cdot \sigma^{-1} \cdot \tau^{-1}$$

van operaties tegen. De reden hiervoor is dat commutatoren vaak slechts enkele cubicles verplaatsen en de rest onverandert laat. Noteer met $\text{supp}(\sigma)$ de verzameling van cubicles die door σ van plaats veranderen. Toon aan dat als

$$\text{supp}(\sigma) \cap \text{supp}(\tau) = \{x\}$$

dat dan de commutator $[\sigma, \tau]$ een 3-cycle is in S_{20} (dus juist 3 cubicles permuteert. Wat gebeurt er als $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$?

OPGAVE 88. We kunnen ook de acties van Rubik-operaties bekijken op de acht hoek cubicles en op de twaalf zijde cubicles apart. Toon aan dat deze groepmorfismen

$$\text{Rubik} \xrightarrow{\phi} S_8 \quad \text{en} \quad \text{Rubik} \xrightarrow{\psi} S_{12}$$

epimorfismen zijn. Toon tevens aan dat voor iedere $g \in \text{Rubik}$ geldt

$$\text{sgn}(\phi(g)) = \text{sgn}(\psi(g))$$

en dus is het groepsmorphisme $\text{Rubik} \xrightarrow{(\phi, \psi)} S_8 \times S_{12}$ geen epimorfisme.

OPGAVE 89. Toon aan dat de compositiefactoren van de Rubik groep bestaan uit C_2 , C_3 en de alternerende groepen A_8 en A_{12} . Hoeveel factoren zijn er van elk type?

13. ALLE GROEPEN VAN ORDE ≤ 30

Als test-materiaal geven we hier de isomorfie klassen van alle groepen van orde ten hoogste 30. We gebruiken devolgende notatie

- C_n : de cyclische groep van orde n , $\langle x \mid x^n = e \rangle$.
- D_n : de **diheder groep** van orde $2n$,

$$D_n = \langle x, y \mid x^n = y^2 = (xy)^2 = e \rangle$$

Dit is de symmetrie groep van een regelmatige n -hoek. (Ga na!)

- S_n : de symmetrische groep op n letters van orde $n!$. Dit is de groep van alle permutaties (bijecties) op n elementen met de samenstelling als groepsbewerking.
- A_n : de alternerende groep op n letters van orde $\frac{n!}{2}$. Dit is de deelgroep van S_n bestaande uit alle even permutaties.

Orde 1 of een priemgetal p (1 groep, 1 Abelse en 0 niet-Abels)

- C_p

Orde 4 (2 groepen, 2 Abelse en 0 niet-Abels)

- C_4
- $C_2 \times C_2 = V$, de Klein Vierergruppe

Orde 6 (2 groepen, 1 Abelse en 1 niet-Abels)

- C_6
- $S_3 \simeq D_3$

Orde 8 (5 groepen, 3 Abelse en 2 niet-Abels)

- C_8
- $C_4 \times C_2$
- $C_2 \times C_2 \times C_2$
- D_4

- $Q = \langle s, t \mid s^4 = e, s^2 = t^2, sts = t \rangle$, de Quaternionen-groep

Orde 9 (2 groepen, 2 Abelse en 0 niet-Abels)

- C_9
- $C_3 \times C_3$

Orde 10 (2 groepen, 1 Abelse en 1 niet-Abels)

- C_{10}
- D_5

Orde 12 (5 groepen, 2 Abelse en 3 niet-Abels)

- C_{12}
- $C_6 \times C_2$
- A_4
- $D_6 \simeq S_3 \times C_2 \simeq D_3 \times C_2$
- $T = \langle s, t \mid s^6 = e, s^3 = t^2, sts = t \rangle$

Orde 14 (2 groepen, 1 Abelse en 1 niet-Abels)

- C_{14}
- D_7

Orde 15 (1 groep, 1 Abelse en 0 niet-Abels)

- C_{15}

Orde 16 (14 groepen, 5 Abelse en 9 niet-Abels)

- C_{16}
- $C_8 \times C_2$
- $C_4 \times C_4$
- $C_4 \times C_2 \times C_2$
- $C_2 \times C_2 \times C_2 \times C_2$
- D_8
- $D_4 \times D_2$
- $Q \times C_2$

- $\langle s, t \mid s^8 = t^2 = e, st = ts^3 \rangle$ (de quasihedral of semihedral groep van orde 16)
- $\langle s, t \mid s^8 = t^2 = e, st = ts^5 \rangle$ (de modulaire groep van orde 16)
- $\langle s, t \mid s^4 = t^4 = e, st = ts^3 \rangle$
- $\langle a, b, c \mid a^4 = b^2 = c^2 = e, cbca^2b = e, bab = a, cac = a \rangle$
- $G_{4,4} = \langle s, t \mid s^4 = t^4 = e = (st)^2, ts^3 = st^3 \rangle$
- $\langle s, t \mid s^8 = e, s^4 = t^2, sts = t \rangle$ (veralgemeende quaternionen groep)

Orde 18 (5 groepen, 2 Abelse en 3 niet-Abels)

- C_{18}
- $C_6 \times C_3$
- D_9
- $S_3 \times C_3$
- $\langle x, y, z \mid x^2 = y^3 = z^3 = e, yz = zy, yxy = x, zxz = x \rangle$

Orde 20 (5 groepen, 2 Abelse en 3 niet-Abels)

- C_{20}
- $C_{10} \times C_2$
- D_{10}
- $\langle s, t \mid s^4 = t^5 = 1, tst = s \rangle$
- $\langle s, t \mid s^4 = t^5 = e, ts = st^2 \rangle$ (Frobenius groep van orde 20)

Orde 21 (2 groepen, 1 Abelse en 1 niet-Abels)

- C_{21}
- $\langle a, b \mid a^3 = b^7 = e, ba = ab^2 \rangle$ (Frobenius groep van orde 21)

Orde 22 (2 groepen, 1 Abelse en 1 niet-Abels)

- C_{22}
- D_{11}

Orde 24 (15 groepen, 3 Abelse en 12 niet-Abels)

- C_{24}
- $C_{12} \times C_2$
- $C_6 \times C_2 \times C_2$

- S_4
- $S_3 \times C_4$
- $D_4 \times C_3$
- $Q \times C_3$
- $A_4 \times C_2$
- $T \times C_2$
- $D_6 \times C_2$
- D_{12}
- $Q_{12} = \langle a, b \mid a^{12} = e, b^2 = a^6, aba = b \rangle$
- $SL_2(\mathbb{F}_3) = \langle a, b, c \mid a^4 = c^3 = e, b^2 = a^2, aba = b, ac = cb, bc = cab \rangle$
- $\langle a, b \mid a^3 = b^8 = e, aba = b \rangle$
- $\langle a, b, c \mid a^3 = b^4 = c^2 = 1, bcb = c, aba = b, ac = ca \rangle$

Orde 25 (2 groepen, 2 Abelse en 0 niet-Abels)

- C_{25}
- $C_5 \times C_5$

Orde 26 (2 groepen, 1 Abelse en 1 niet-Abels)

- C_{26}
- D_{13}

Orde 27 (5 groepen, 3 Abelse en 2 niet-Abels)

- C_{27}
- $C_9 \times C_3$
- $C_3 \times C_3 \times C_3$
- $\langle s, t \mid s^9 = t^3 = e, st = ts^4 \rangle$
- $\langle x, y, z \mid x^3 = y^3 = z^3 = e, yz = zyx, xy = yx, xz = zx \rangle$

Orde 28 (4 groepen, 2 Abelse en 2 niet-Abels)

- C_{28}
- $C_{14} \times C_2$
- D_{14}

- $D_7 \times C_2$

Orde 30 (4 groepen, 1 Abelse en 3 niet-Abels)

- C_{30}
- D_{15}
- $D_5 \times C_3$
- $D_3 \times C_5$

Oplossingen van de Opgaven

Opgave 1. eerste methode : Bekijk de *rotatie* r van het vlak over 72° in tegenwijzerzin, dan heeft r het volgende effect op de 5 vectoren

$$\vec{A} \longrightarrow \vec{B} \longrightarrow \vec{C} \longrightarrow \vec{D} \longrightarrow \vec{E} \longrightarrow \vec{A}$$

en bijgevolg wordt de som naar zichzelf gestuurd onder deze rotatie. De enige vlakke vector die zichzelf blijft onder een niet-triviale rotatie is de nulvector $\vec{0}$.

tweede methode : Bekijk de *spiegeling* s van het vlak met spiegelas de rechte bepaalt door $\vec{A}$. Dan heeft s het volgende effect op de 5 vectoren

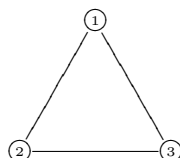
$$\vec{A} \longrightarrow \vec{A} \quad \vec{B} \longrightarrow \vec{E} \longrightarrow \vec{B} \quad \vec{C} \longrightarrow \vec{D} \longrightarrow \vec{C}$$

Bijgevolg stuurt s de som van de 5 vectoren naar zichzelf en de enige vlakke vectoren die onder een spiegeling naar zichzelf gestuurd worden zijn deze die op de spiegelas liggen, dus de som moet liggen op de rechte OA . Maar we kunnen dit argument herhalen voor de spiegeling s' met spiegelas de rechte OB , dan moet de som ook op de rechte OB liggen. Dus ligt de som in

$$OA \cap OB = \{\vec{0}\}$$

Opgave 1

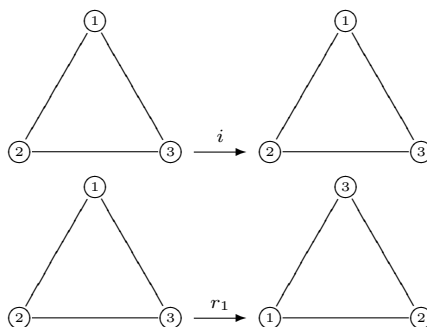
Opgave 2. Laat ons de hoekpunten van de gelijkzijdige driehoek als volgt nummeren

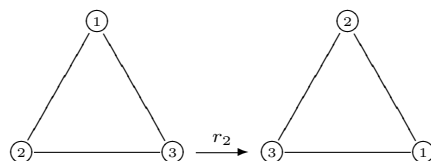


Elke symmetrie moet hoekpunten naar hoekpunten sturen. De enige *rotaties* met deze eigenschap hebben als *centrum* O het zwaartepunt (=middenpunt) van de gelijkzijdige driehoek en als mogelijke rotatiehoek

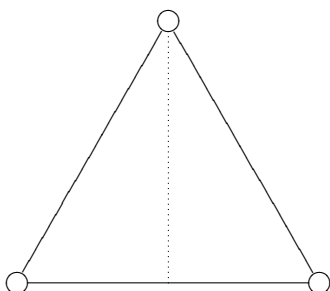
$$i = r(0, 0^\circ) \quad r_1 = r(0, 120^\circ) \quad r_2 = r(0, 240^\circ)$$

waar me met $r(P, h)$ noteren de rotatie van het vlak met als centrum het punt P en als rotatie-hoek h -graden in tegenwijzerzin. Merk op dat de rotatie met als hoek 0° alles op zijn plaats laat, we noemen dit de *identiteit*. Hier is het effect van de drie rotaties op de hoekpunten

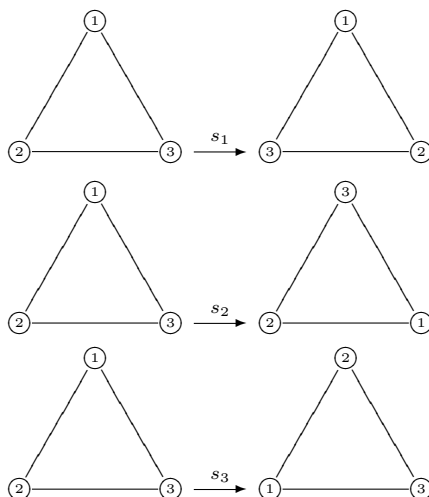




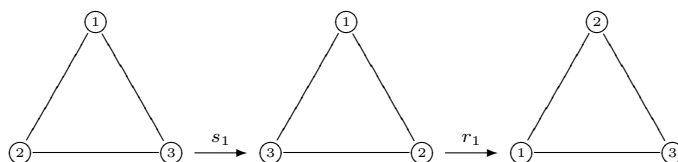
Een spiegeling-symmetrie moet een hoekpunt vast laten en de twee andere omwisselen, dus de enige spiegeling-symmetriën van de gelijkzijdige driehoek zijn deze met spiegelas de zwaartelijnen (=hoogtelijnen) van de driehoek s_i met $i = 1, 2$ of 3 al naargelang de hoogtelijn vanuit het hoekpunt i .



Hier het effect van deze drie spiegelingen op de hoekpunten

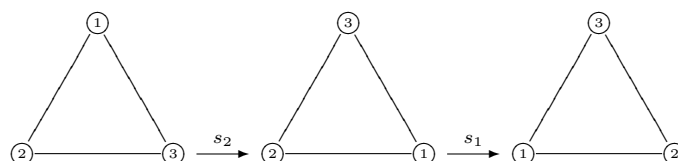


Om de samenstelling van twee symmetrieën te bepalen zien we naar het effect op de hoekpunten. Bvb. $r_1 \circ s_1$ levert



en we zien dat hoekpunt 3 ter plaatse blijft en de andere twee uitgewisseld werden. Bijgevolg is de samenstelling $r_1 \circ s_1$ gelijk aan de symmetrie s_3 .

Nog een voorbeeld, de samenstelling van de twee spiegelingen $s_1 \circ s_2$ doet



en de totale symmetrie komt dus overeen met een rotatie in tegenwijzerzin over 120° , bijgevolg is de samenstelling $s_1 \circ s_2$ gelijk aan de rotatie r_1 . Ga zelf de andere plaatsen na in devolgende tabel

$\circ$	i	r_1	r_2	s_1	s_2	s_3
i	i	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	i	s_3	s_1	s_2
r_2	r_2	i	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	i	r_1	r_2
s_2	s_2	s_3	s_1	r_2	i	r_1
s_3	s_3	s_1	s_2	r_1	r_2	i

Deze tabel wordt als volgt gelezen : in een samenstelling $f \circ g$ staat de eerste term f vertikaal links en de tweede term g horizontaal bovenaan. De symmetrie waaraan de samenstelling gelijk is staat dan op de positie in de tabel op de rij van f en de kolom van g . Bvb. de gevonden relatie

$$s_1 \circ s_2 = r_2$$

werd met een cirkel aangegeven.

Opgave 2

Opgave 3. De samenstelling van twee rotaties met hetzelfde centrum is opnieuw een rotatie met dat centrum en als rotatie hoek de som van de rotatiehoeken van de rotaties.

De samenstelling van twee vlakke spiegelingen $s \circ s'$ is een rotatie met als centrum het snijpunt van de twee spiegellijnen en als rotatiehoek tweemaal de hoek tussen de spiegellijnen in de richting van s' naar s .

De samenstelling $r \circ s$ is een spiegeling met spiegelas die door het centrum van de rotatie gaat en een hoek maakt met de as van s gelijk aan de rotatiehoek en met dezelfde oriëntatie als r . De samenstelling $s \circ r$ is een spiegeling met as die door het centrum van de rotatie gaat en een hoek maakt met de as van s gelijk aan de rotatie-hoek maar met de tegengestelde oriëntatie.

Verfieur dit op de tabel van de vorige opgave. In de linker-boven blok staan de samenstelling van twee rotaties, in de rechter-beneden blok de samenstellingen van twee spiegelingen. Samenstellingen van rotaties en spiegelingen staan in de overige twee blokken.

$\circ$	i	r_1	r_2	s_1	s_2	s_3
i	i	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	i	s_3	s_1	s_2
r_2	r_2	i	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	i	r_1	r_2
s_2	s_2	s_3	s_1	r_2	i	r_1
s_3	s_3	s_1	s_2	r_1	r_2	i

Opgave 3

Opgave 4. Stel dat e en f eenheidselementen van G zijn, dan volgt

$$e = e.f = f$$

Stel dat x^{-1} en y^{-1} inverse elementen zijn van g dan volgt

$$x^{-1} = x^{-1} \cdot (g \cdot y^{-1}) = (x^{-1} \cdot g) \cdot y^{-1} = y^{-1}$$

Opgave 4

Opgave 5. $G = \{i, r_1, r_2, s_1, s_2, s_3\}$ dus de orde van G is 6. Elke spiegeling s_i heeft orde twee want $s_i \circ s_i = i$ en de rotaties r_1 en r_2 hebben orde drie want $r_i \circ r_i = r_j \neq i$ en $r_i \circ r_i \circ r_i = i$. Tenslotte, de orde van het eenheidselement is 1 dus de orde van i is 1.

Opgave 5

Opgave 6.

$\circ$	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
e	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	e	s_4	s_3	s_1	s_2
r_2	r_2	r_3	e	r_1	s_2	s_1	s_4	s_3
r_3	r_3	e	r_1	r_2	s_3	s_4	s_2	s_1
s_1	s_1	s_3	s_2	s_4	e	r_2	r_1	r_3
s_2	s_2	s_4	s_1	s_3	r_2	e	r_3	r_1
s_3	s_3	s_2	s_4	s_1	r_3	r_2	e	r_2
s_4	s_4	s_1	s_3	s_2	r_1	r_3	r_2	e

e heeft orde 1, r_1 en r_3 hebben orde 4 maar r_2 heeft orde twee. Alle spiegelingen hebben orde twee.

Opgave 6

Opgave 7. Een regelmatige 5-hoek (resp. n -hoek) heeft juist 5 (resp. n) rotaties met als centrum het middelpunt van de veelhoek en als rotatie-hoek een veelvoud van 72° (resp. $360^\circ/n$). Verder heeft een regelmatige 5-hoek (resp. n -hoek) juist 5 (resp. n) spiegelingen met een as die door een hoekpunt en het middel van de overstaande zijde gaat (resp. als n oneven is dan gaat elke as door een hoekpunt en het midden van de overstaande zijde als n even is gaat elke as door de middens van tegenoverliggende zijden).

Bijgevolg is de orde van de symmetrie-groep van een regelmatige 5-hoek (resp. n -hoek) gelijk aan 10 (resp. gelijk aan $2n$).

Opgave 7

Opgave 8. De samenstelling (dat is het product in de groep) van twee rotaties is opnieuw een rotatie, daarentegen is de samenstelling van twee spiegelingen niet opnieuw een spiegeling maar een rotatie. Bekijk bvb. de groeptabel voor de regelmatige 4-hoek.

$\circ$	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
e	e	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	e	s_4	s_3	s_1	s_2
r_2	r_2	r_3	e	r_1	s_2	s_1	s_4	s_3
r_3	r_3	e	r_1	r_2	s_3	s_4	s_2	s_1
s_1	s_1	s_3	s_2	s_4	e	r_2	r_1	r_3
s_2	s_2	s_4	s_1	s_3	r_2	e	r_3	r_1
s_3	s_3	s_2	s_4	s_1	r_3	r_2	e	r_2
s_4	s_4	s_1	s_3	s_2	r_1	r_3	r_2	e

Dan is de tabel voor de producten van rotaties gegeven in de linker-boven blok en inspectie leert dat daar enkel rotaties voorkomen. De tabel voor het product van spiegelingen daarentegen is de rechter-beneden blok en die bevat niet opnieuw spiegelingen.

Een verder voorbeeld van een deelgroep van de symmetrie-groep van een regelmatige n -hoek wordt gegeven door de deelverzameling $\{e, s\}$ met e de identiteit en s een spiegeling (merk op dat $s \circ s = e$). De gecirkelde vakjes in de groep-tabel van het vierkant geven de tabel voor producten van een zulke deelgroep. Opgave 8

Opgave 9. e is het eenheidselement van G , dus kunnen we de e -rij en e -kolom invullen

$\circ$	e	r	r'	s	s'	s''
e	e	r	r'	s	s'	s''
r	r			s'		
r'	r'					
s	s					
s'	s'					
s''	s''					

We weten samenstellingen van rotaties met zelfde centrum opnieuw rotaties met dat centrum zijn, dus $H = \{e, r, r'\}$ moet een deelgroep zijn en kunnen we dus ook de Sudoku-eigenschap op de H -tabel toepassen (de linker-boven blok). Dus moet bv. $r \circ r = r'$ (indien $r \circ r = e$ dan zou $r \circ r' = r'$ moeten zijn en dat kan niet). Bijgevolg hebben we

$\circ$	e	r	r'	s	s'	s''
e	e	r	r'	s	s'	s''
r	r	r'	e	s'		
r'	r'	e	r			
s	s					
s'	s'					
s''	s''					

Dus is $r' = r^{-1}$ en bijgevolg volgt uit het gegeven $r \circ s = s'$ dat dan

$$r' \circ s' = r' \circ r \circ s = e \circ s = s$$

en als we dit invullen (box) kunnen we uit de Sudoku-eigenschap heel de rechter-bovenblok invullen

$\circ$	e	r	r'	s	s'	s''
e	e	r	r'	s	s'	s''
r	r	r'	e	s'	s''	s
r'	r'	e	r	s''	s	s'
s	s					
s'	s'					
s''	s''					

Spiegelingen hebben orde twee en dus omdat $r \circ s = s'$ hebben we

$$s' \circ s' = (r \circ s) \circ s' = r \circ (s \circ s')$$

en omdat $r^{-1} = r'$ hebben we dus $s \circ s' = r'$. Dit laat ons toe de rechten-onderblok in

te vullen

$\circ$	e	r	r'	s	s'	s''
e	e	r	r'	s	s'	s''
r	r	r'	e	s'	s''	s
r'	r'	e	r	s''	s	s'
s	s			e	r'	r
s'	s'			r	e	r'
s''	s''			r'	r	e

Tenslotte, omdat r orde drie heeft is de rotatiehoek 120° . We hebben gezien dat de samenstelling van een rotatie en een spiegeling geeft een nieuwe spiegeling die een hoek als de rotatie-hoek maakt met de oorspronkelijke as maar afhankelijk van de volgorde van de termen, bijgevolg is dus $r \circ s \neq s \circ r$ en dus moet $s \circ r = s''$ waaruit direct de linker-beneden hoek ingevuld wordt.

$\circ$	e	r	r'	s	s'	s''
e	e	r	r'	s	s'	s''
r	r	r'	e	s'	s''	s
r'	r'	e	r	s''	s	s'
s	s	s''	s'	e	r'	r
s'	s'	s	s''	r	e	r'
s''	s''	s'	s	r'	r	e

Opgave 9

Opgave 10. De samenstelling van bijecties is duidelijk associatief. Het eenheidselement e is dus de *identiteits map*

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

en het invers element van een bijectie (permutatie) σ is de *inverse map* σ^{-1}

$$\sigma^{-1} = \text{orden} \begin{bmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{bmatrix}$$

waarbij we met orden aangeven dat we de kolommen ordenen in stijgende volgorde van het eerste element. Dus b.v.b. als

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

dan is

$$\sigma^{-1} = \text{orden} \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

Dus S_n voldoet aan alle groep-eigenschappen. Het aantal elementen van S_n is het aantal bijecties van $\{1, 2, \dots, n\}$ en dat aantal is $n! = n(n-1)(n-2) \dots 2 \cdot 1$ (immers, je kan 1 naar n verschillende elementen sturen, maar dan kan je 2 nog maar naar $n-1$ elementen sturen en 3 naar $n-2$ enz.

Opgave 10

Opgave 11.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = () \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3) \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3) \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2) \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 3)$$

Opgave 11

Opgave 12.

$$\begin{cases} \sigma \circ \tau = (1, 4, 8, 10, 9, 12, 11, 7, 6, 5, 3) \\ \tau \circ \sigma = (2, 3, 7, 9, 10, 11, 12, 8, 5, 6, 4) \end{cases}$$

Opgave 12

Opgave 13.

$\circ$	$()$	$(1, 2, 3)$	$(1, 3, 2)$	$(2, 3)$	$(1, 3)$	$(1, 2)$
$()$	$()$	$(1, 2, 3)$	$(1, 3, 2)$	$(2, 3)$	$(1, 3)$	$(1, 2)$
$(1, 2, 3)$	$(1, 2, 3)$	$(1, 3, 2)$	$()$	$(1, 3)$	$(1, 2)$	$(2, 3)$
$(1, 3, 2)$	$(1, 3, 2)$	$()$	$(1, 2, 3)$	$(1, 2)$	$(2, 3)$	$(1, 3)$
$(2, 3)$	$(2, 3)$	$(1, 2)$	$(1, 3)$	$()$	$(1, 3, 2)$	$(1, 2, 3)$
$(1, 3)$	$(1, 3)$	$(2, 3)$	$(1, 2)$	$(1, 2, 3)$	$()$	$(1, 3, 2)$
$(1, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$	$(1, 3, 2)$	$(1, 2, 3)$	$()$

Opgave 13

Opgave 14. We weten al dat $1_G \in \ker(f)$ en $1_H = f(1_G) \in \text{im}(f)$ dus we hebben al eenheidselementen. We moeten nog aantonen dat deze deelverzameling gesloten zijn onder producten nemen en inversen nemen. Als $g, g' \in \ker(f)$ dan hebben we dat

$$f(g \cdot g') = f(g) * f(g') = 1_H * 1_H = 1_H$$

dus ook $g \cdot g' \in \ker(f)$. Als $g \in \ker(f)$ dan ook

$$f(g^{-1}) = f(g^{-1}) * 1_H = f(g^{-1}) * f(g) = f(g^{-1} \cdot g) = f(1_G) = 1_H$$

dus ook $g^{-1} \in \ker(f)$. Als $h, h' \in \text{im}(f)$ dan zijn er elementen $g, g' \in G$ zodat $h = f(g)$ en $h' = f(g')$ maar dan is

$$h * h' = f(g) * f(g') = f(g \cdot g')$$

dus ook $h * h' \in \text{im}(f)$. En als $h = f(g) \in \text{im}(f)$ dan ook

$$f(g^{-1}) * h = f(g^{-1}) * f(g) = f(g^{-1} \cdot g) = f(1_G) = 1_H$$

dus $f(g^{-1}) = f(g)^{-1} = h^{-1}$ dus ook $h^{-1} \in \text{im}(f)$.

Opgave 14

Opgave 15. Als de kern niet minimaal is dan zou er een $g \neq 1_G$ inzitten maar dan hebben g en 1_G hetzelfde beeld dus kan f nooit injectief zijn. Omgekeerd, stel dat $\ker(f) = \{1_G\}$ en veronderstel dat f niet injectief zou zijn. Dan zijn er $g \neq g'$ in G met hetzelfde beeld, dus

$$f(g) = f(g') = h \in H$$

maar dan is

$$f(g^{-1} \cdot g') = f(g^{-1}) * f(g') = f(g)^{-1} * f(g') = h^{-1} * h = 1_H$$

en dus is $g^{-1} \cdot g' \in \ker(f)$ dus $g^{-1} \cdot g' = 1_G$ maar dan is $g' = g$ wat een tegenspraak is.

Opgave 15

Opgave 16. We moeten aantonen dat de enige symmetrie s die onder f naar $()$ gestuurd wordt de identiteit-symmetrie is. Maar als $f(s) = ()$ wil dit zeggen dat s elk

hoekpunt naar zichzelf stuurt, dus kan s enkel de identiteit zijn. We weten dat $\text{in}(f)$ een deelgroep is van S_n en de afbeelding

$$D_n \xrightarrow{f} \text{im}(f) \subset S_n$$

is zowel injectief als surjectief dus is een bijectie. Bijgevolg is D_n isomorf met de deelgroep $\text{im}(f)$ van S_n . Opgave 16

Opgave 17. We weten al dat D_3 isomorf is met zijn beeld in S_3 maar beide groepen hebben 6 elementen, dus is het beeld alles en hebben we dus dat de afbeelding $D_3 \rightarrow S_3$ niet enkel injectief maar ook surjectief is dus een bijectie. Vergelijk de groep-tabellen van D_3 en S_3 die we voorheen uitwerkten. Voor D_3

$\circ$	i	r_1	r_2	s_1	s_2	s_3
i	i	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	i	s_3	s_1	s_2
r_2	r_2	i	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	i	r_1	r_2
s_2	s_2	s_3	s_1	r_2	i	r_1
s_3	s_3	s_1	s_2	r_1	r_2	i

en voor S_3

$\circ$	$()$	$(1, 2, 3)$	$(1, 3, 2)$	$(2, 3)$	$(1, 3)$	$(1, 2)$
$()$	$()$	$(1, 2, 3)$	$(1, 3, 2)$	$(2, 3)$	$(1, 3)$	$(1, 2)$
$(1, 2, 3)$	$(1, 2, 3)$	$(1, 3, 2)$	$()$	$(1, 3)$	$(1, 2)$	$(2, 3)$
$(1, 3, 2)$	$(1, 3, 2)$	$()$	$(1, 2, 3)$	$(1, 2)$	$(2, 3)$	$(1, 3)$
$(2, 3)$	$(2, 3)$	$(1, 2)$	$(1, 3)$	$()$	$(1, 3, 2)$	$(1, 2, 3)$
$(1, 3)$	$(1, 3)$	$(2, 3)$	$(1, 2)$	$(1, 2, 3)$	$()$	$(1, 3, 2)$
$(1, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$	$(1, 3, 2)$	$(1, 2, 3)$	$()$

We zien dat deze tabellen dezelfde structuur hebben als we i met $()$ identificeren, r_1 met $(1, 2, 3)$, r_2 met $(1, 3, 2)$, s_1 met $(2, 3)$, s_2 met $(1, 3)$ en s_3 met $(1, 2)$. Dus, twee groepen zijn isomorf als er een bijectie op hun elementen bestaat zodat de groep-tabel identiek wordt onder deze identificatie. Opgave 17

Opgave 18. Neem $g \neq e$ in G , dan is de orde van g gelijk aan p (de orde kan niet gelijk zijn aan 1 want anders was $g = e$). Bijgevolg zijn de elementen

$$\{e, g, g^2, g^3, \dots, g^{p-1}\}$$

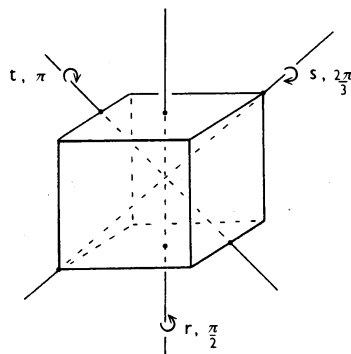
allen verschillend en vormen dus alle elementen van G . Neem nu een regelmatige p -hoek en laat r de rotatie in tegenwijzerzin zijn over $360^\circ/p$. De afbeelding

$$G \longrightarrow C_p \quad g \mapsto r, g^2 \mapsto r^2, \dots, g^{p-1} \mapsto r^{p-1}$$

is een groepsmorphisme en omdat het ook een bijectie is, een isomorfisme. Opgave 18

Opgave 19. Door rotaties kunnen we elk van de 6 zijvlakken als bovenvlak krijgen en vervolgens kunnen we door rotaties om 90 graden rond het middelpunt van dit vlak ieder van de 4 zijvlakken van voor krijgen. De positie van de kubus is uniek bepaald door boven- en voorvlak. Bijgevolg zijn er $6 \times 4 = 24$ verschillende rotaties van de

kubus. Deze rotaties komen in enkele families



- (type L) : Rotaties r met als as de rechte door de middelpunten van tegenoverliggende zijvlakken over een hoek van 90, 180 of 270 graden. Er zijn drie paar tegenoverliggende zijvlakken en voor elk van deze 3 rotaties dus heen we zo $3 \times 3 = 9$ rotaties.
- (type M) : Rotaties t met als as de rechten door middens van tegenoverliggende zijden en hoek 180 graden. Er zijn zes paar overliggende zijden dus ook zes zulke rotaties.
- (type N) : Rotaties s met als as de rechte door tegenoverliggende zijpunten (lichaamsdiagonalen) en als hoek 120 of 240 graden. Er zijn 4 lichaamsdiagonalen en twee mogelijke hoeken dus hebben we $4 \times 2 = 8$ zulke rotaties.

Samen met de identiteitsrotatie e hebben we dus in totaal

$$9 + 6 + 8 + 1 = 24$$

rotaties geïdentificeerd en dit moeten dus alle rotaties van de kubus zijn. Het isomorfisme van de rotatie groep van de kubus met de symmetrische groep S_4 wordt gegeven door de actie op de vier lichaamsdiagonalen te bekijken. Noem 1 de diagonaal door de hoekpunten 1 en 1', 2 de diagonaal door de hoekpunten 2 en 2' enz. Onder elke rotatie wordt een lichaamsdiagonaal naar een andere gestuurd dus kunnen we de rotatie beschrijven als een permutatie op deze 4 diagonalen. Bvb. voor de aangegeven rotaties r , s en t hebbe we

$$r \longrightarrow (1, 2, 3, 4) \quad s \longrightarrow (1, 4, 3) \quad t \longrightarrow (1, 2)(3, 4)$$

en je kan dit nagaan voor alle andere rotaties. We krijgen dan alle 24 permutaties en dus is de rotatie groep isomorf met S_4 .

Opgave 19

Opgave 20. We weten al dat de kern een deelgroep is van G . Neem nu $k \in \ker(\pi)$ (dus $\pi(k) = e_H$) en $g \in G$, dan moeten we aantonen dat $g.k.g^{-1} \in \ker(\pi)$ (dus dat dit element ook naat e_H gestuurd wordt. Nu is

$$\pi(g.k.g^{-1}) = \pi(g).\pi(k).\pi(g^{-1}) = \pi(g).e_H.\pi(g^{-1}) = \pi(g.g^{-1}) = \pi(e_G) = e_H$$

en zijn we klaar.

Opgave 20

Opgave 21. Uit de Sudoku-eigenschap van de groep-tabel van G volgt dat elke linker-nevenklas $H.g$ juist $\#H$ elementen bevat. Wederom volgt uit de deelgroep eigenschap

van H dat ofwel $H.g$ en $H.g'$ disjunkt zijn ofwel gelijk. Weer een element kiezen in elk van de disjuncte linker-nevenklassen leert ons dat

$$G = H.g_1 \sqcup H.g_2 \sqcup \dots \sqcup H.g_l$$

met l het aantal linker-nevenklassen. Maar dan volgt dat

$$\#G = l.\#H$$

en dus ook $l = \frac{\#G}{\#H}$,

Opgave 21

Opgave 22. Omdat $g^{-1}.g = e \in H$ volgt reflexiviteit. Als $g^{-1}.g' \in H$ dan ook het inverse element

$$(g^{-1}.g')^{-1} = (g')^{-1}.g$$

en dus volgt symmetrie van de relatie. Tenslotte, als $g^{-1}.g' \in H$ en ook $(g')^{-1}.g'' \in H$ dan ook hun product

$$(g^{-1}.g').((g')^{-1}.g'') = g^{-1}.g'.(g')^{-1}.g'' = g^{-1}.g'' \in H$$

en dus volgt ook transitiviteit van de relatie. Een element g' zit in de equivalentie klasse $[g]$ van g als en alleen als

$$g^{-1}.g' \in H \quad \text{en dus} \quad g' \in g.H$$

en bijgevolg $g'.H = g.H$, dus inderdaad geldt $[g] = \bar{g}$.

Opgave 22

Opgave 23. We hebben al gezien dat de equivalentie klassen van een equivalentie relatie een partitie van V bepalen. Omgekeerd, gegeven een partitie van V

$$V = \bigsqcup_i V_i$$

Definieer nu een relatie op V

$$\mathcal{R} = \{(v, w) \mid \exists i : v, w \in V_i\}$$

dan is $\mathcal{R}$ duidelijk een equivalentie relatie en we hebben voor de equivalentie klassen

$$[v] = V_i$$

als $v \in V_i$.

Opgave 23

Opgave 24. Hier is een truuk die dikwijls kan gebruikt worden. In gelijk welk groep-product mag je steeds tussen termen 'dummy termen' zoals $g.g^{-1}$ plaatsen zonder dat dit het resultaat beïnvloed. We moeten om te beginnen aantonen dat $g.[x, y].g^{-1}$ opnieuw in de commutator deelgroep zit. Maar,

$$g.[x, y].g^{-1} = g.x.y.x^{-1}.y^{-1}.g^{-1} = \underbrace{g.x.g^{-1}} \cdot \underbrace{g.y.g^{-1}} \cdot \underbrace{g.x^{-1}.g^{-1}} \cdot \underbrace{g.y^{-1}.g^{-1}}$$

maar dit is $x_1.y_1.x_1^{-1}.y_1^{-1}$ waarbij $x_1 = g.x.g^{-1}$ en $y_1 = g.y.g^{-1}$ en is dus opnieuw een commutator. We kunnen deze truuk ook gebruiken om aan te tonen dat de geconjugeerde van een product van commutatoren opnieuw van die vorm. Immers,

$$g.[x, y].[x', y'] \dots [x'', y''].g^{-1} = \underbrace{g.[x, y].g^{-1}} \cdot \underbrace{g.[x', y'].g^{-1}} \cdot \dots \cdot \underbrace{g.[x'', y''].g^{-1}}$$

maar wegens het eerste kunnen we deze termen herschrijven als

$$[x_1, y_1].[x'_1, y'_1] \dots [x''_1, y''_1]$$

waarbij bvb $x'_1 = g.x'.g^{-1}$.

Bekijk nu de quotientgroep $\overline{G} = G/G'$ en de quotientafbeelding

$$G \longrightarrow \overline{G} \quad x \mapsto \overline{x} = x.G'$$

We moeten aantonen dat voor alle elementen (linker-nevenklassen) $\overline{x}, \overline{y} \in \overline{G}$ geldt dat

$$\overline{x}.\overline{y} = \overline{y}.\overline{x}$$

of equivalent hiermee dat

$$\overline{x}.\overline{y}.\overline{x}^{-1}.\overline{y}^{-1} = \overline{e}$$

Maar het linker lid is wegens het feit dat de quotient afbeelding een groepmorfisme is gelijk aan

$$\overline{x.y.x^{-1}.y^{-1}}$$

en dat is duidelijk de nevenklasse $\overline{e}$ want $x.y.x^{-1}.y^{-1} \in G'$.

Opgave 24

Opgave 25. Om te beginnen is Z een deelgroep, want als $z, z' \in Z$ dan geldt ook

$$(z.z').g = z.(z'.g) = z.(g'.z') = (z.g).g' = (g.z).z' = g.(z.z')$$

en dus is ook het product $z.z' \in Z$. Als $z \in Z$ moeten we aantonen dat $g.z.g^{-1}$ opnieuw in Z zit, maar omdat z met g commuteert hebben we

$$g.z.g^{-1} = z.g.g^{-1} = z$$

en dus zijn we klaar.

Opgave 25

Opgave 26. Iedere $x \in G$ kan geschreven worden als $t^r.z$ met $z \in Z$ en t een voortbrenger van de cyclische groep G/Z . Voor een andere $y = t^s.z'$ in G volgt bijgevolg dat

$$x.y = (t^r.z).(t^s.z') = t^r.t^s.z.z' = t^{r+s}.z.z' = t^{r+s}.z'.z = t^s.z'.t^r.z = y.x$$

en dus is G inderdaad Abels.

Opgave 26

Opgave 27. We moeten aantonen dat $H.N$ gesloten is onder product.

$$(h.n).(h'.n') = h.(n.h').n' \stackrel{!}{=} h.(h'.n'').n' = (h.h').(n''.n') \in H.N$$

waar de gelijkheid $\stackrel{!}{=}$ volgt uit de normaaldeeler eigenschap van N . Verder is het inverse element van $h.n$ bevat in $H.N$, want

$$(h.n)^{-1} = n^{-1}.h^{-1} \stackrel{!}{=} h^{-1}.n' \in H.N$$

voor een zekere $n' \in N$ wederom omdat N een normaaldeeler is.

Als nu ook H een normaaldeeler is, dan is $H.N$ een normaaldeeler van G want voor alle $g \in G$ geldt

$$g.H.N.g^{-1} = g.H.g^{-1}.g.N.g^{-1} = (g.H.g^{-1}).(g.N.g^{-1}) \subset H.N$$

en we zijn klaar.

Opgave 27

Opgave 28. Laat $\pi : G \longrightarrow \overline{G} = G/N$ de quotient-afbeelding zijn. Voor iedere deelgroep A van $\overline{G}$ is het inverse beeld

$$\pi^{-1}(A) = \{g \in G \mid \pi(g) = \overline{g} \in A\}$$

een deelgroep van G (gebruik dat π een groepsmorfisme is) en omdat $\overline{e} \in A$ zit N in $\pi^{-1}(A)$. Anderzijds, als $N \subset H$ voor een deelgroep H van G dan is het beeld

$$\pi(H) = \{\overline{h} \mid h \in H\}$$

een deelgroep van $\overline{G}$ (wederom omdat π een groepsmorphisme is). Tenslotte is

$$\pi^{-1}(\pi(H)) = \{h.N \mid h \in H\} = H.N = H$$

als $N \subset H$ en dus zijn deze afbeeldingen bijecties. De uitspraak over normaaldelers volgt uit voorgaande oefening. Opgave 28

Opgave 29. Merk om te beginnen op dat de doorsnede van twee deelgroepen van G opnieuw een deelgroep is. Voor elke $h \in H$ geldt dat

$$h.(H \cap N).h^{-1} \subset h.H.h^{-1} \subset H \quad \text{en} \quad h.(H \cap N).h^{-1} \subset h.N.h^{-1} \stackrel{!}{\subset} N$$

waar we in $\stackrel{!}{\subset}$ gebruikt hebben dat N een normaaldeeler is van G , en dus is idd.

$$h.(H \cap N).h^{-1} \subset H \cap N$$

en dus een normaaldeeler in H . Opgave 29

Opgave 30. Neem $g = 1 \bmod n$ dan is de orde van g gelijk aan p want

$$\underbrace{g + g + \dots + g}_k = k \bmod n$$

en dus is g een voorbrenger van $\mathbb{Z}/n\mathbb{Z}$. Een andere manier om dit isomorfisme te zien is de 'logaritme' afbeelding te definiëren

$$C_p \xrightarrow{\log} \mathbb{Z}/n\mathbb{Z} \text{quad} g^i \mapsto i \bmod n$$

en vast te stellen dat dit een groepsmorphisme is. Immers,

$$\log(g^i \cdot g^j) = \log(g^{i+j}) = i + j \bmod n = i \bmod n + j \bmod n = \log(g^i) + \log(g^j)$$

Opgave 30

Opgave 31. Voor elke $g \in G$ geldt $g^2 = e$ en dus ook dat $g = g^{-1}$. Neem nu twee elementen g en h dan geldt dus ook dat

$$g.h = (g.h)^{-1} = h^{-1}.g^{-1} = h.g$$

en zijn we klaar. Opgave 31

Opgave 32. We weten al wegens vorige oefening dat G Abels is. Neem nu twee verschillende elementen g en h , geen van beiden e . Dan is $\langle g \rangle \simeq C_2 \simeq \langle h \rangle$ en de doorsnede van beide groepen is enkel $\{e\}$, dus is het directe product

$$\langle g \rangle \times \langle h \rangle = C_2 \times C_2$$

isomorf met een deelgroep van G (namelijk deze voortgebracht door g en h). Veronderstel nu dat we per inductie al een deelgroep H geconstrueerd hebben (deze voortgebracht door elementen $g_1, \dots, g_k$) die isomorf is met het directe product van cyclische groepen van orde twee

$$H \simeq \langle g_1 \rangle \times \dots \times \langle g_k \rangle \simeq C_2 \times \dots \times C_2$$

en veronderstel dat $H \neq G$. Dan is er een element $g \in G - H$. Maar dan is ook

$$H \cap \langle g \rangle = \{e\}$$

en bijgevolg is er een deelgroep H' (voortgebracht door $g_1, \dots, g_k$ en g) die isomorf is met

$$H' \simeq H \times \langle g \rangle \simeq C_2 \times \dots \times C_2 \times C_2$$

Zo voortgaan hebben we uiteindelijk dat $G \simeq C_2 \times \dots \times C_2$ en dus ook dat de orde van G een macht is van 2 (nl. de macht gelijk aan het aantal minimale voortbrengers voor G).

Opgave 32

Opgave 33. Uit de stelling van Lagrange volgt dat ieder element van G ofwel orde 4, 2 of 1 (het eenheidselement) heeft. Als er een element g is van orde 4, dan is de cyclische deelgroep $C_4 = \langle g \rangle$ gelijk aan G want ook G heeft vier elementen. Zoniet zijn alle elementen van G van orde twee en volgt uit de vorige opgave dat G isomorf is met het direct product van twee groepen C_2 .

Opgave 33

Opgave 34. De orde van een groeps-element is 1, 2 of 3. Omdat $6 \neq 2^n$ moet er minstens een element van orde 3 zijn (uit oefening 32), bvb. a . Als c een element is van G niet behorend tot $\{e, a, a^2\}$, dan is

$$G = \{e, a, a^2, c, c.a, c.a^2\}$$

(d.i. al deze elementen zijn verschillend). Immers, stel dat twee ervan gelijk zijn dan kunnen we door vermenigvuldigen met een inverse een tegenspraak krijgen. Bvb. stel $a^2 = c.a$ dan ook

$$a^2.a^{-1} = c.a.a^{-1} = c.e = c$$

en dan zou $c = a$ zijn een tegenspraak. Stel bvb. $c.a = c.a^2$ dan ook

$$a = c^{-1}.c.a = c^{-1}.c.a^2 = a^2$$

een tegenspraak met a van orde drie. Alle andere gevallen zijn analoog aan te tonen.

Als G Abels is hebben we $c.a = a.c$, dan is $G \simeq C_2 \times C_3 \simeq C_6$. Dit volgt ofwel uit de directe product stellingen ofwel door expliciet een map te definiëren

$$C_2 \times C_3 \longrightarrow G \quad (c^i, a^j) \mapsto c^i a^j$$

en te verifiëren dat dit een groepsmorfisme is dat injectief is (want $\langle a \rangle \cap \langle c \rangle = \{e\}$) en surjectief want we kennen alle elementen van G .

Bekijk c^2 en toon aan dat $c^2 \notin \{a, a^2, c.a, c.a^2\}$ (gebruik dat bovenstaande elementen verschillend zijn). Dus $c^2 = e$ en bekijk $a.c$ en toon aan dat $a.c \notin \{e, a, a^2, c\}$ dus ofwel

$$a.c = c.a \quad \text{ofwel} \quad a.c = c.a^2$$

In het eerste geval is G Abels en weten we het antwoord al. Het tweede geval is equivalent met $(a.c)^2 = e$ (ga na!). Dus dit geval geeft ons de groep

$$G = \langle a, c \mid a^3 = c^2 = (a.c)^2 = e \rangle$$

en dit stelt ons in staat de hele vermenigvuldigings tabel voor G op te stellen. Ga na dat de enige mogelijkheid is

.	e	a	a^2	c	ca	ca^2
e	e	a	a^2	c	ca	ca^2
a	a	a^2	e	ca^2	c	ca
a^2	a^2	e	a	ca	ca^2	c
c	c	ca	ca^2	e	a	a^2
ca	ca	ca^2	c	a^2	e	a
ca^2	ca^2	c	ca	a	a^2	e

Tenslotte tonen we aan dat deze groep isomorf is met S_3 door bvb. $a \mapsto (1, 2, 3)$ en $c \mapsto (1, 2)$ te sturen en te verifiëren dat deze afbeelding de groepsbewerking bewaart (een groepsmorfisme is).

Opgave 34

Opgave 35. De eerste en laatste mogelijkheid hebben we reeds besproken. Uit bovenstaande argumentatie mogen we onderstellen dat ofwel $b^2 = e$ of $b^2 = a^2$. In het eerste geval is $C_2 \simeq \langle b \rangle$ en hebben we een groepmorfisme (gebruik Abels)

$$C_4 \times C_2 \longrightarrow G \quad (a^i, b^j) \mapsto a^i \cdot b^j$$

die injectief is omdat $\langle a \rangle \cap \langle b \rangle = \{e\}$ en surjectief is omdat we zo alle 8 de elementen van G krijgen (zie boven) en we hebben dus een isomorfisme.

In het geval $b^2 = a^2$ kunnen we $c = ab^{-1}$ nemen en dan is

$$c^2 = a \cdot b^{-1} \cdot a \cdot b^{-1} = a^2 \cdot b^{-2} = e$$

(we gebruikten Abels). We kunnen dan de voortbrenger b door c vervangen en dan zitten we wederom in het eerste geval. Opgave 35

Opgave 36. In het geval $C_8 = \langle a \rangle$ met $a^8 = e$ hebben we

	e	a	a^2	a^3	a^4	a^5	a^6	a^7
e	e	a	a^2	a^3	a^4	a^5	a^6	a^7
a	a	a^2	a^3	a^4	a^5	a^6	a^7	e
a^2	a^2	a^3	a^4	a^5	a^6	a^7	e	a
a^3	a^3	a^4	a^5	a^6	a^7	e	a	a^2
a^4	a^4	a^5	a^6	a^7	e	a	a^2	a^3
a^5	a^5	a^6	a^7	e	a	a^2	a^3	a^4
a^6	a^6	a^7	e	a	a^2	a^3	a^4	a^5
a^7	a^7	e	a	a^2	a^3	a^4	a^5	a^6

In het geval $C_4 \times C_2 = \langle a, b \mid a^4 = e = a^2, a \cdot b = b \cdot a \rangle$

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	ab	a^2b	a^3b	e	a	a^2	a^3
ab	ab	a^2b	a^3b	b	a	a^2	a^3	e
a^2b	a^2b	a^3b	b	ab	a^2	a^3	e	a
a^3b	a^3b	b	ab	a^2b	a^3	1	a	a^2

en tenslotte voor $C_2 \times C_2 \times C_2 = \langle a, b, c \mid a^2 = b^2 = c^2 = 1, ab = ba, ac = ca, bc = cb \rangle$

	e	a	b	c	ab	ac	bc	abc
e	e	a	b	c	ab	ac	bc	abc
a	a	e	ab	ac	b	c	abc	bc
b	b	ab	e	bc	a	abc	c	ac
c	c	ac	bc	e	abc	a	b	ab
ab	ab	b	a	abc	e	bc	ac	c
ac	ac	c	abc	a	bc	e	ab	b
bc	bc	abc	c	b	ac	ab	e	a
abc	abc	bc	ac	ab	c	b	a	e

Opgave 36

Opgave 37. We weten al uit vorige opgave dat ofwel $b^2 = 1$ ofwel $b^2 = a^2$. Bekijk nu $b.a$, dit moet een element van G zijn en kan geen a -macht of b zijn. Blijven over

$$b.a \in \{ab, a^2b, a^3b\}$$

De eerste mogelijkheid kan niet (want dan zou G Abels zijn en deze kennen we al). De tweede mogelijkheid is ook onmogelijk. Immers, als $ba = a^2b$ dan volgt

$$b^{-1}a^2b = a \quad \text{maar dan volgt} \quad a^2 = b^{-1}a^2bb^{-1}a^2b = b^{-1}a^4b = b^{-1}b = e$$

en a had orde vier. Blijft dus enkel over $ba = a^3b$ wat we kunnen herschrijven als

$$(ab)^2 = e$$

Stel nu dat $b^2 = 1$ dan krijgen we de groep

$$G = \langle a, b \mid a^4 = b^2 = e, (ab)^2 = e \rangle$$

en dat is de diheder groep D_4 . In het tweede geval, dat $b^2 = a^2$ krijgen we de quaternionen groep

$$Q = \langle a, b \mid a^4 = e, a^2 = b^2, ba = a^3b \rangle$$

Opgave 37

Opgave 38. Als $i^2 = -1$ dan is $i^4 = 1$. Verder is $i^2 = j^2 = -1$ en tenslotte moeten we nog checken dat

$$ji = i^3j = -ij$$

dus is het een groepmorfisme. Voor de complexe matrixen geldt

$$A^2 = B^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

en rekenen levert tenslotte dat

$$BA = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = A^3B$$

Opgave 38

Opgave 39. Duidelijk is rotatie over $4 \times 90^\circ = 360^\circ$ de identiteit. Een spiegeling is een orde twee element. Tenslotte verifieer dat spiegeling na rotatie dezelfde operatie is als eerst spiegelen en dan roteren in tegenovergestelde richting.

Opgave 39

Opgave 40. Als we r met minimale rotatie-hoek $360^\circ/n$ nemen, dan heeft r orde n in D_n (en brengt dus de deelgroep C_n voort van alle rotaties). We weten dat de samenstelling van een rotatie en een spiegeling s een spiegeling is. Alle elementen

$$\{s, r \circ s, r^2 \circ s, r^3 \circ s, \dots, r^{n-1} \circ s\}$$

zijn verschillend wegens de Sudoku eigenschap. Bijgevolg zijn dit dus alle n de spiegelingen van de n -hoek. Bijgevolg kunnen we alle elementen van D_n schrijven als producten van r en s en is dus D_n voortgebracht door r en s .

Opgave 40

Opgave 41. Bereken $\sigma \circ \tau$ en $\tau \circ \sigma$ met behulp van de rekenregel voor permutaties en stel vast dat de verkregen permutatie dezelfde is en bestaat uit twee cycles nl. σ en τ .

Opgave 41

Opgave 42. De verschillende partities van 5 zijn

$$(5), (4, 1), (3, 2), (3, 11), (2, 2, 1), (2, 1, 1, 1), (1, 1, 1, 1, 1)$$

dus er zijn juist 7 verschillende conjugatie klassen in S_5 .

Opgave 42

Opgave 43. Als $\sigma, \tau \in \text{sym}(p(x_1, \dots, x_n))$ dan voldoet ook

$$(\sigma \circ \tau).p(x_1, \dots, x_n) = \sigma.(\tau.p(x_1, \dots, x_n)) = \sigma.p(x_1, \dots, x_n) = p(x_1, \dots, x_n)$$

hun product aan de voorwaarde. Bijgevolg is ook $\sigma \circ \tau \in \text{sym}(p(x_1, \dots, x_n))$.

Opgave 43

Opgave 44. We hebben al gezien dat $(1, 2, 3) \in \text{sym}(p(x_1, x_2, x_3))$ en dus ook alle permutaties die machten zijn van $(1, 2, 3)$. Dus ook

$$(1, 2, 3) \circ (1, 2, 3) = (1, 3, 2) \quad \text{en} \quad (1, 2, 3) \circ (1, 2, 3) \circ (1, 2, 3) = (1, 2, 3) \circ (1, 3, 2) = (1, 2, 3)$$

zitten in de symmetrie groep. De symmetrische groep S_3 heeft 6 elementen en buiten de drie bovenstaande zijn de resterende elementen verwisselingen namelijk

$$(1, 2), (1, 3) \quad \text{en} \quad (2, 3)$$

Zulke verwisseling verandert het teken in juist één van de factoren van $p(x_1, x_2, x_3)$ en dus zitten ze niet in de symmetrie groep.

Opgave 44

Opgave 45. We hebben al gezien dat deze positie correspondeert met de 16-cycle

$$\sigma = (1, 3, 5, 16, 11, 8, 14, 13, 4, 6, 9, 12, 2, 7, 15, 10)$$

en we weten ook hoe we een cycle kunnen schrijven als een product van verwisselingen. In dit geval kunnen we de cycle schrijven als

$$(1, 10) \circ (1, 15) \circ (1, 7) \circ (1, 2) \circ (1, 12) \circ (1, 9) \circ (1, 6) \circ (1, 4) \circ (1, 13) \circ (1, 14) \circ (1, 8) \circ (1, 11) \circ (1, 16) \circ (1, 5) \circ (1, 3)$$

dus een product van 15 verwisselingen. Bijgevolg is σ een oneven permutatie dus is dit een illegale positie.

Opgave 45

Opgave 46. Zie ook de vorige opgave. Een cycle van even (resp. oneven) lengte kan je schrijven als het product van een oneven aantal (resp. een even aantal) verwisselingen. Omdat het totaal aantal benodigde verwisselingen even moet zijn moet dus het aantal even cycles ook even zijn.

Opgave 46

Opgave 47. Bekijk de paring

$$g \leftrightarrow g^{-1}$$

in G . Ofwel is $g = g^{-1}$ (en dan is g een element van orde twee) ofwel is $g \neq g^{-1}$ (en dan is $(g^{-1})^{-1} = g$ dus vormt dit een paar disjunct van alle andere elementen). Stel nu dat er s elementen zijn met $g = g^{-1}$ en t elementen waar dit niet het geval is dan is

$$\#G = s + t \quad \text{en } t \text{ is een even getal}$$

Uit veronderstelling moet dus ook s een even getal zijn. En, $s \neq 0$ want minstens e_G heeft de eigenschap, bijgevolg moet er dus nog minstens een ander element $g \in G$ zijn met $g = g^{-1}$ maar dan heeft g orde twee.

Opgave 47

Opgave 48. We hebben al gezien dat iedere p -groep een niet-triviaal centrum Z heeft. Hiet is dus ofwel $\#Z = p$ ofwel $\#Z = p^2$. In het tweede geval zijn we klaar, dus veronderstel dat we in het eerste geval zitten. Dan is

$$\overline{G} = G/Z \simeq C_p$$

want de orde van dit quotient is p . Neem nu een voortbrenger t van G/Z en lift die tot een element T in G . Dan kunnen we elk element van G schrijven als

$$g = T^i z \quad \text{met } 0 \leq i < p \text{ en } z \in Z$$

Neem nu een ander element in deze schrijfwijze $g' = T^j z'$ dan hebben we

$$g \cdot g' = T^i z T^j z' = T^i T^j z z' = T^j T^i z' z = T^j z' T^i z = g' \cdot g$$

en bijgevolg is de groep G dus Abels.

Opgave 48

Opgave 49. We weten dat twee permutaties in S_n geconjugueerd zijn als en slechts als ze dezelfde cycle-decompositie hebben. Verder weten we dat de verschillende cycle-decomposities (als we ook de 1-cycles in rekening brengen) juist corresponderen met de verschillende partities van n . Voor $n = 4$ hebben we devolgende partities

$$[4] \quad [3, 1] \quad [2, 2] \quad [2, 1, 1] \quad \text{en} \quad [1, 1, 1, 1]$$

Representatieve permutaties met deze cycle-decomposities zijn dus als gegeven. Het aantal elementen volgt uit de bovenstaande stelling en de correspondentie met rotaties gebeurt weer door de actie te beschouwen op de 4 lichaamsdiagonalen.

Opgave 49

Opgave 50. Merk op dat de symmetrie-groep van het Alice-probleem de volledige rotatie-symmetrie groep S_4 is terwijl de symmetrie-groep van het Bob-probleem (dus die rotaties die de grid invariant laten) een deelgroep is van orde 12, waarvan de conjugatie-klassen gegeven worden door de rotaties

$$\begin{cases} r^2 & \text{de conjugatie-klasse bestaat uit 3 elementen} \\ s & \text{de conjugatie-klasse bestaat uit 4 elementen} \\ s^2 & \text{de conjugatie-klasse bestaat uit 4 elementen} \\ I_3 & \text{de conjugatie-klasse bestaat uit 1 element} \end{cases}$$

We gaan nu in beide gevallen na wat de fixpunt-verzamelingen zijn voor elk van de representanten van de conjugatie-klassen (d.w.z. het aantal gekleurde cubussen die door de symmetrie in elkaar worden omgezet).

Het Alice probleem : Een gekleurde kubus die onder r hetzelfde blijft heeft alle zijvlakken dezelfde kleur (dit geeft 2 mogelijkheden) en omdat de keuze van boven- en onder-vlak nog vrij zijn hebben we dat

$$\#X^r = 8$$

Voor de rotatie r^2 moeten enkel linker- en rechter zijvalk en voor- en achter-vlak dezelfde kleur hebben en we krijgen dus dat

$$\#X^{r^2} = 16$$

Onder s gaan de zes zijvlakken als volgt

$$\begin{cases} U \longrightarrow R \longrightarrow B \longrightarrow U \\ D \longrightarrow L \longrightarrow F \longrightarrow D \end{cases}$$

en alle zijvlakken in een van beide families moeten dus dezelfde kleur hebben, Bijgevolg is

$$\#X^s = 4$$

Tenslotte, de rotatie t wisselt voor- en achtervlak, boven-vlak met links zijvlak en ondervlak met rechter-zijvlak. Bijgevolg is

$$\#X^t = 2^3 = 8$$

en natuurlijk geldt dat $\#X^e = 64$. Via de orbit-stelling weten we dus dat het aantal orbits gegeven wordt door

$$\frac{1}{\#G} \sum_{conj} \#(C(g))\#X^g = \frac{1}{24}(6.8 + 3.16 + 8.4 + 1.64) = 10$$

Het Bob probleem : De groep van alle rotatie-symmetrieën van de kubus die de grid invariant laat is slechts de deelgroep A_4 van orde 12 waarvan de conjugatie klassen hierboven gegeven werden. Door eenzelfde argumentatie als voorheen weten we dat

$$\#X^{r^2} = 16, \quad \#X^s = 4, \quad \#X^{s^2} = 4 \quad \text{en} \quad \#X^e = 64$$

Door alle info te stoppen in de orbit-stelling krijgen we in dit geval dat het aantal orbits gelijk is aan

$$\frac{1}{12}(3.16 + 4.4 + 4.4 + 1.64) = 12.$$

Bijgevolg kan Bob dus twee kubussen meer kleuren dan Alice.

Opgave 50

Opgave 51. Ik ga ervan uit dat je dit zelf kan...

Opgave 51

Opgave 52. Gebruik dat *hernummeren* van de 4 getallen een symmetrie is op alle oplossingen. D.w.z. door toepassen van een *bijjectie* σ op $\{1, 2, 3, 4\}$ kunnen we er steeds voor zorgen dat bvb. de linkertop 2×2 tabel volgende vorm heeft

x	y		
u	v		

 $\xrightarrow{\sigma}$

1	2		
3	4		

Hoeveel zulke bijecties zijn er op 4 elementen? (Hoeveel op een verzameling van n elementen?) Dit verklaart de factor 24. Toon aan dat *samenstellen* van bijecties een bewerking of alle bijecties toelaat en dat dit een *groepsstructuur* vormt.

We moeten nu nog alle oplossingen bepalen met de opper 2×2 tabel in 'standaard-vorm'. Toon aan dat er juist 12 uniek bepaalde oplossingen zijn van de vorm

1	2		
3	4		
		a	b
		c	d

namelijk deze waarvoor de rechter onder 2×2 tabel één van de onderstaande mogelijkheden is

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad B = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix} \quad C = \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$$

$$\begin{array}{cccc}
 E = \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 3 & 2 \\ \hline \end{array} & F = \begin{array}{|c|c|} \hline 4 & 1 \\ \hline 2 & 3 \\ \hline \end{array} & G = \begin{array}{|c|c|} \hline 2 & 3 \\ \hline 4 & 1 \\ \hline \end{array} & H = \begin{array}{|c|c|} \hline 3 & 2 \\ \hline 1 & 4 \\ \hline \end{array} \\
 I = \begin{array}{|c|c|} \hline 4 & 3 \\ \hline 1 & 2 \\ \hline \end{array} & J = \begin{array}{|c|c|} \hline 3 & 4 \\ \hline 2 & 1 \\ \hline \end{array} & K = \begin{array}{|c|c|} \hline 2 & 1 \\ \hline 3 & 4 \\ \hline \end{array} & L = \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 4 & 3 \\ \hline \end{array}
 \end{array}$$

Opgave 52

Opgave 53. Geef elk van de 16 velden een getal van 1 tem. 16 en schrijf elke basis-operatie als een permutatie op 16 letters.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

dan corresponderen de basis-operaties met devolgende permutaties

$$\begin{cases}
 r \mapsto (9, 13)(10, 14)(11, 15)(12, 16) \\
 k \mapsto (3, 4)(7, 8)(11, 12)(15, 16) \\
 R \mapsto (1, 9)(2, 10)(3, 11)(4, 12)(5, 13)(6, 14)(7, 15)(8, 16) \\
 K \mapsto (1, 3)(5, 7)(9, 11)(13, 15)(2, 4)(6, 8)(10, 12)(14, 16) \\
 S \mapsto (2, 5)(3, 9)(4, 13)(7, 10)(8, 14)(12, 15) \\
 D \mapsto (1, 4, 16, 13)(2, 8, 15, 9)(3, 12, 14, 5)(6, 7, 11, 10)
 \end{cases}$$

Gebruik dan GAP om het aantal elementen van de groep voortgebracht door de basis-operaties te bepalen.

```

gap> a:=(9,13)(10,14)(11,15)(12,16);
(9,13)(10,14)(11,15)(12,16)
gap> b:=(3,4)(7,8)(11,12)(15,16);
(3,4)(7,8)(11,12)(15,16)
gap> c:=(1,9)(2,10)(3,11)(4,12)(5,13)(6,14)(7,15)(8,16);
(1,9)(2,10)(3,11)(4,12)(5,13)(6,14)(7,15)(8,16)
gap> d:=(1,3)(5,7)(9,11)(13,15)(2,4)(6,8)(10,12)(14,16);
(1,3)(2,4)(5,7)(6,8)(9,11)(10,12)(13,15)(14,16)
gap> e:=(2,5)(3,9)(4,13)(7,10)(8,14)(12,15);
(2,5)(3,9)(4,13)(7,10)(8,14)(12,15)
gap> f:=(1,4,16,13)(2,8,15,9)(3,12,14,5)(6,7,11,10);
(1,4,16,13)(2,8,15,9)(3,12,14,5)(6,7,11,10)
gap> sudoku:=Group(a,b,c,d,e,f);
<permutation group with 6 generators>
gap> Size(sudoku);
128

```

Opgave 53

Opgave 54. Wegens de Sudoku-eigenschap is het ongeordend permutatie type van de eerste en de tweede rij gelijk (en ook dat van de derde en vierde rij, of dat van de eerste en tweede kolom en tenslotte ook dat van de derde en vierde kolom).

Opgave 54

Opgave 55. De toelaatbare kolom-permutaties bewaren de ongeordende permutatie van een gegeven kolom. Bvb. alle acht de toelaatbare kolom-operaties geven op de eerste kolom van A_1 devolgende kolommen

1	1	3	3	2	4	2	4
3	3	1	1	4	2	4	2
2	4	2	4	1	1	3	3
4	2	4	2	3	3	1	1

en die zijn allemaal van ongeordend permutatie-type β . Hetzelfde geldt voor toelaatbare rij-operaties op een welbepaalde rij.

Opgave 55

Opgave 56. Ze hebben alle drie een verschillend type en gebruik dan de voorgaande opgave.

Opgave 56

Opgave 57. Als we S toepassen op A_1 krijgen we de oplossing

$$S(A_1) = \begin{array}{|c|c|c|c|} \hline 1 & 3 & 2 & 4 \\ \hline 2 & 4 & 1 & 3 \\ \hline 3 & 1 & 4 & 2 \\ \hline 4 & 2 & 3 & 1 \\ \hline \end{array}$$

en dit is van type $[S(A_1)] = (\{\beta, \beta\}, \{\alpha, \alpha\})$ en dit type is anders dat $[A_1]$. Bijgevolg kan S niet zitten in $\text{rij} \times \text{kol}$ want alle elementen ervan behouden het type.

Opgave 57

Opgave 58. D^2 is een operatie die kan verkregen worden door zowel rijen als kolommen op toelaatbare wijze te veranderen (dus is een element van de product groep). Als we D en D^3 toepassen op oplossing B_1 krijgen we de oplossingen

$$D(B_1) = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline 4 & 3 & 1 & 2 \\ \hline \end{array} \quad \text{en} \quad D^3(B_1) = \begin{array}{|c|c|c|c|} \hline 4 & 1 & 3 & 2 \\ \hline 3 & 2 & 4 & 1 \\ \hline 2 & 4 & 1 & 3 \\ \hline 1 & 3 & 2 & 4 \\ \hline \end{array}$$

en deze zijn van type

$$[D(B_1)] = [D^3(B_1)] = (\{\beta, \gamma\}, \{\alpha, \alpha\})$$

en dit is verschillend van $[B_1]$.

Opgave 58

Opgave 59. We weten al dat $[X] = [Y]$ als X en Y equivalent zijn onder $\text{rij} \times \text{kol}$. Als X en Y niet $\text{rij} \times \text{kol}$ -equivalent zijn maar wel sudoku-equivalent dan moeten X en $S(Y)$ equivalent zijn onder $\text{rij} \times \text{kol}$ wegens de constructie van sudoku maar dan volgt dat $[X] = [S(Y)]$.

Opgave 59

Opgave 60. Het volstaat wegens vorige opgave uit te rekenen dat

$$[S(A_1)] = (\{\beta, \beta\}, \{\alpha, \alpha\}) \quad [S(B_1)] = (\{\beta, \gamma\}, \{\alpha, \alpha\}) \quad [S(C_1)] = (\{\beta, \beta\}, \{\alpha, \gamma\})$$

Opgave 60

Opgave 61. Om te beginnen merken we op dat elke hernummer operatie *commuteert* met elke symmetrie-operatie. De groep van alle hernummeringen is S_4 en heeft orde $24 = 2^3 \cdot 3$. We hebben gezien dat de groep van alle verwissel-operaties sudoku orde $128 = 2^7$ heeft. We beweren nu dat

$$\text{sudoku} \cap S_4 = \{e\}$$

Wegens Lagrange kan een element in de doorsnede enkel orde 1, 2 of 4 hebben. Stel bvb. dat de hernummer-permutatie $(1, 2, 3, 4)$ in sudoku zou zitten. Op de ongeordende permutatie types wekt $(1, 2, 3, 4)$ als volgt

$$\alpha \xleftrightarrow{(1,2,3,4)} \gamma \quad \text{en} \quad \beta \xrightarrow{(1,2,3,4)} \beta$$

Neem nu een oplossing van type $(\{\alpha, \alpha\}, \{\beta, \gamma\})$ (bvb. B_1) dan is het type van de oplossing door hierop $(1, 2, 3, 4)$ toe te passen gelijk aan $(\{\gamma, \gamma\}, \{\beta, \alpha\})$ en is dus niet Sudoku-equivalent met de oorspronkelijke, dus kan $(1, 2, 3, 4)$ nooit in sudoku zitten. Analoge argumenten werken ovoor alle andere hernummer-permutaties van orde twee of vier. Maar dan volgt uit de product stelling dat de micro-Sudoku groep isomorf is met

$$\text{sudoku} \times S_4$$

en bijgevolg de gewenste orde heeft.

Opgave 61

Opgave 62. Door toepassen van hernummeren en de operaties k en r mogen we veronderstellen dat een oplossing in volgende vorm gebracht kan worden

1	2	3	4
3	4		
2		4	
4			a

met $a \in \{1, 2, 3\}$. De oplossingen $a = 3$ en $a = 2$ kunnen echter in elkaar omgezet worden door symmetrie-operaties uit de micro-Sudoku groep.

1	2	3	4
3	4		
2		4	
4			3

 $\xrightarrow{(2,3)}$

1	3	2	4
2	4		
3		4	
4			2

 $\xrightarrow{S}$

1	2	3	4
3	4		
2		4	
4			2

Opgave 62

Opgave 63. Op hernummeren na weten we al dat elke micro-Sudoku oplossing tot één van volgende 12 basisvormen herleid kan worden

$A_1 =$

1	2	3	4
3	4	1	2
2	1	4	3
4	3	2	1

$A_2 =$

1	2	4	3
3	4	2	1
2	1	3	4
4	3	1	2

$A_3 =$

1	2	4	3
3	4	2	1
4	3	1	2
2	1	3	4

$A_4 =$

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

$$B_1 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 2 & 1 \\ \hline 4 & 3 & 1 & 2 \\ \hline 2 & 1 & 4 & 3 \\ \hline \end{array} \quad B_2 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline 4 & 3 & 1 & 2 \\ \hline \end{array} \quad B_3 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline 2 & 1 & 3 & 4 \\ \hline 4 & 3 & 2 & 1 \\ \hline \end{array} \quad B_4 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline 2 & 1 & 3 & 4 \\ \hline \end{array}$$

$$C_1 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & 3 \\ \hline 3 & 4 & 2 & 1 \\ \hline 4 & 1 & 3 & 2 \\ \hline 2 & 3 & 1 & 4 \\ \hline \end{array} \quad C_2 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 1 & 2 \\ \hline 2 & 3 & 4 & 1 \\ \hline 4 & 1 & 2 & 3 \\ \hline \end{array} \quad C_3 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & 3 \\ \hline 3 & 4 & 2 & 1 \\ \hline 2 & 3 & 1 & 4 \\ \hline 4 & 1 & 3 & 2 \\ \hline \end{array} \quad C_4 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 1 & 2 & 3 \\ \hline 2 & 3 & 4 & 1 \\ \hline \end{array}$$

Het is duidelijk dat door rij- en kolom-verwisselingen we iedere A_i in A_1 (resp. iedere B_i in B_2 en iedere C_i in C_2) kunnen omzetten. Verder weten we uit vorige opgave dat B_2 en C_2 in elkaar kunnen opgezet worden door een spiegeling en een hernummering (2, 3) toe te passen.

Bijgevolg zitten alle A_i in de eerste orbit en de tweede orbit bevat alle B_i en C_i . Tenslotte merken we op dat als we hernaummeringen toelaten elk van deze oplossingen eigenlijk staat voor 24 micro-Sudoku oplossingen. Bijgevolg bevat de A-orbit $4 \times 24 = 96$ oplossingen en de BC-orbit $8 \times 24 = 192$ oplossingen. Opgave 63

Opgave 64. Uit voorgaande is het voldoende dit aan te tonen voor de twee representanten van de twee orbits

$$\begin{array}{ccc} \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & & \\ \hline 2 & & 4 & \\ \hline 4 & & & 1 \\ \hline \end{array} & \xrightarrow{\text{oplos}} & \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 1 & 2 \\ \hline 2 & 1 & 4 & 3 \\ \hline 4 & 3 & 2 & 1 \\ \hline \end{array} \\ \\ \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & & \\ \hline 2 & & 4 & \\ \hline 4 & & & 2 \\ \hline \end{array} & \xrightarrow{\text{oplos}} & \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 3 & 4 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 \\ \hline 4 & 3 & 1 & 2 \\ \hline \end{array} \end{array}$$

Deze oplossingen zijn te verkrijgen met slechts vier gegevens

$$\begin{array}{|c|c|c|c|} \hline 1 & & & \\ \hline & & & 2 \\ \hline & & 4 & \\ \hline & 3 & & \\ \hline \end{array} \quad \text{resp.} \quad \begin{array}{|c|c|c|c|} \hline 1 & & & \\ \hline & & 2 & \\ \hline & & 4 & \\ \hline & 3 & & \\ \hline \end{array}$$

Tenslotte gebruik je je kennis over de 12 basisoplossingen om te zien dat wanneer je maar drie gegevens ingeeft je minstens twee van die 12 als mogelijke oplossingen kan krijgen en dit dus geen geldige micro-Sudoku puzzel is. Opgave 64

Opgave 65. Iedere deelgroep van C_n is ook een normaaldeeler. Immers, voor alle $a, b \in C_n$ geldt dat

$$a.b.a^{-1} = b$$

want als g een voortbrenger is van C_n dan is $a = g^k$ en $b = g^l$ voor zekere gehele getallen k en l maar dan is

$$a.b.a^{-1} = g^k.g^l.g^{-k} = g^{k+l-k} = g^l = b$$

Als nu n geen priemgetal is maar een factorizatie als $n = uv$ toelaat dan is de deelgroep

$$N = \langle g^u \rangle = \{e, g^u, g^{2u}, \dots, g^{(v-1)u}\} \triangleleft C_n$$

een niet-triviale normaaldeeler (met als quotient groep een cyclische groep van orde v) en dus kan C_n niet simpel zijn.

Als daarentegen n een priemgetal is dan is iedere normaaldeeler $N \neq \{e\}$ de hele groep C_n . Immers weten we uit de stelling van Lagrange dat de orde van de deelgroep N een deler moet zijn van n en dus gelijk moet zijn aan n , maar een deelgroep heeft enkel dezelfde orde als de grote groep als ze aan elkaar gelijk zijn. Dus, als $n = p$ een priemgetal is, is de cyclische groep C_p simpel. Opgave 65

Opgave 66. We weten dat de orde van A_5 gelijk is aan $\frac{1}{2}5! = 60$ dus elke niet-triviale normaaldeeler moet als orde een getal $1 < k < 60$ hebben dat tevens een deler is van 60.

Iedere normaaldeeler is ook de unie van volledige conjugatieklassen (want als $g \in N$ dan moeten ook alle andere elementen in de conjugatieklasse van g ,

$$h.g.h^{-1} \in h.N.h^{-1} \subset N$$

in N moeten zitten. We dienen dus de conjugatieklassen van A_5 te bepalen en uit te rekenen hoeveel elementen er in iedere conjugatieklasse zitten.

Ga zelf na dat A_5 vijf conjugatieklassen heeft met representanten en aantal elementen

- $()$ met 1 element
- $(1, 2)(3, 4)$ met 15 elementen
- $(1, 2, 3)$ met 20 elementen
- $(1, 2, 3, 4, 5)$ met 12 elementen
- $(2, 1, 3, 4, 5)$ met 12 elementen

Gebruik hiervoor dat ieder element van A_5 een even permutatie moet zijn en dus een cycle decompositie moet hebben van de gegeven vormen. In S_n weten we dat de vorm van de cycle-decompositie de conjugatie vastlegt en tevens hebben we gezien hoe we het conjugerende element moeten bepalen (nl. gegeven door de permutatie die de cycles elementsgewijs in elkaar omzet). Zo zien we bvb. $(1, 2, 3, 4, 5)$ en $(2, 1, 3, 4, 5)$ hoewel geconjugeerd in S_5 niet geconjugeerd kunnen zijn in A_5 want het element dat de transformatie doet, nl. $(1, 2)$ immers

$$(1, 2)(1, 2, 3, 4, 5)(1, 2)^{-1} = (1, 3, 4, 5, 2)$$

is een verwisseling en dus geen element van A_5 . Voor de andere klassen kunnen we steeds een element in A_5 nemen dat de truuk doet. Bvb. $(1, 2, 3)$ en $(2, 1, 3)$ zijn geconjugeerd in A_5 . Het element dat de truuk doet is blijkbaar wederom de verwisseling $(1, 2)$ maar nu kunnen we deze verwisseling uitbreiden met de verwisseling $(4, 5)$ van elementen vastgelaten door beide permutaties. En inderdaad is

$$(1, 2)(4, 5).(1, 2, 3).(4, 5)^{-1}(1, 2)^{-1} = (2, 1, 3)$$

en ga dit ook na voor de andere vormen. Het aantal elementen in een bepaalde klasse wordt gegeven door elementaire combinatoriek.

Tenslotte merken we op dat geen enkele echte deelsom van de getallen

$$1, 15, 20, 12, 12$$

een deler is van 60. Dus kan A_5 geen echte normaaldeeler hebben (want die moest de disjuncte unie zijn van volledige conjugatieklassen). Bijgevolg is A_5 simpel.

Opgave 66

Opgave 67. De orde van $A_3 = \frac{1}{2}3! = 3$ en bijgevolg is $A_3 \simeq C_3$ de cyclische groep van orde drie en dus simpel (een voortbrenger van A_3 is de drie-cycle $(1, 2, 3)$).

Voor A_4 bekijk de volgende 4 elementen

$$N = \{(), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

en ga na dat dit een deelgroep is van A_4 . De groep-tabel is immers

$\circ$	$()$	$(1, 2)(3, 4)$	$(1, 3)(2, 4)$	$(1, 4)(2, 3)$
$()$	$()$	$(1, 2)(3, 4)$	$(1, 3)(2, 4)$	$(1, 4)(2, 3)$
$(1, 2)(3, 4)$	$(1, 2)(3, 4)$	$()$	$(1, 4)(2, 3)$	$(1, 3)(2, 4)$
$(1, 3)(2, 4)$	$(1, 3)(2, 4)$	$(1, 4)(2, 3)$	$()$	$(1, 2)(3, 4)$
$(1, 4)(2, 3)$	$(1, 4)(2, 3)$	$(1, 3)(2, 4)$	$(1, 2)(3, 4)$	$()$

Verder zijn dit juist alle elementen van S_4 met cycle-decompositie bestaande uit twee 2-cycles en vormd dus een volledige conjugatieklasse in S_4 , dwz. $g.N.g^{-1} \subset N$ voor alle $g \in S_4$. Maar dan geldt hetzelfde natuurlijk voor $g \in A_4$ en is N dus een niet-triviale normaaldeeler van A_4 .

Opgave 67

Opgave 68. Neem als deelgroep H de triviale deelgroep $H = \{e\}$. Dan is $G = G/H$ en is k de orde van G . Elke geconjugeerde $x.H.x^{-1} = \{x.e.x^{-1}\} = \{e\}$ dus de doorsnede van al deze deelgroepen is $\{e\}$ en dit zegt dat het morfisme $G \longrightarrow S_k$ injectief is.

Opgave 68

Opgave 69. Neem H een echte deelgroep van index k en bekijk bijhorend groepmorfisme gegeven door de veralgemening van de stelling van Cayley

$$\theta : A_5 \longrightarrow S_k$$

Omdat A_5 simpel is is de kern van θ ofwel alles (wat niet kan) ofwel $\{e\}$ dus is θ een injectie. Maar S_k heeft $k!$ elementen en $\#A_5 = 60$ dus moet $k \geq 5$.

Opgave 69

Opgave 70. Gebruik opnieuw de veralgemening van de stelling van Cayley. Als $[G : H] = k$ dan is er een groepmorfisme

$$G \xrightarrow{\theta} S_k$$

De rechtergroep heeft orde $k!$ en dit is ≤ 120 als $k \leq 5$ en ≥ 720 als $k \geq 6$. Omdat G simpel is moet de afbeelding injectief zijn en $120 < 168 < 720$.

Opgave 70

Opgave 71. In een Abelse groep is iedere deelgroep automatisch een normaaldeeler. Dus neem $g \neq e$ in G en stel dat de orde van g gelijk is aan m . Laat p een priemfactor zijn van m dan is de deelgroep van G

$$\langle h = g^{m/p} \rangle = \{e, h, h^2, \dots, h^{p-1}\} \simeq C_p$$

een cyclische groep van priemorde en dus simpel. Bijgevolg hebben we het begin van een compositierij

$$\{e\} \triangleleft C_p \triangleleft G$$

en de quotientgroep $\overline{G} = G/C_p$ is opnieuw Abels (en van kleinere orde nl. de orde van G gedeeld door p). We kunnen daarom het vorige argument herhalen op $\overline{G}$ enz. om uiteindelijk tot een hele compositierij te komen met alle compositie factoren cyclisch van priemorde.

Alternatief kunnen we inductie op de orde van G toepassen. Omdat $\overline{G}$ kleinere orde heeft en Abels is mogen we onderstellen dat $\overline{G}$ een compositierij heeft

$$\overline{e} \triangleleft \overline{G}_1 \triangleleft \overline{G}_2 \triangleleft \dots \triangleleft \overline{G}_k \triangleleft \overline{G}$$

met alle compositie factoren cyclisch van priemorde. Maar deze deelgroepen corresponderen met deelgroepen G_i van G die C_p bevatten en dus hebben we ook een geschikte compositierij van G

$$\{e\} \triangleleft C_p \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_k \triangleleft G$$

en is dus ook G oplosbaar.

Opgave 71

Opgave 72. We hebben al gezien dat A_4 een normaaldeler bevat, nl. de conjugatie klasse van elementen met cycledecompositie twee cycles van lengte twee samen met het identiteitselement

$$H = \{(), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

en we hebben de groeptable opgesteld en vastgesteld dat deze groep Abels is, dus oplosbaar (met twee factoren C_2), dus er is een compositie rij voor A_4 van de vorm

$$\{()\} \triangleleft \langle (1, 2)(3, 4) \rangle \triangleleft H \triangleleft A_4$$

want de orde van de quotientgroep A_4/H is $12/4 = 3$ en is dus C_3 en bijgevolg simple. We kunnen deze rij uitbreiden tot een compositierij voor S_4

$$\{()\} \triangleleft \langle (1, 2)(3, 4) \rangle \triangleleft H \triangleleft A_4 \triangleleft S_4$$

want de laatste factor heeft orde $24/12 = 2$ en is dus C_2 . Dus, zowel A_4 als S_4 hebben een compositie rij met alle factoren cyclische groepen van priemorde en zijn dus oplosbaar.

Opgave 72

Opgave 73. We weten dat het aantal elementen in een conjugatieklas $C(g) = \{hgh^{-1} : h \in G\}$ steeds een deler is van de orde van G . Bijgevolg is het aantal elementen

$$\#CV(g) = p^{a_g} \quad \text{voor zekere } a \in \mathbb{N}$$

De conjugatieklassen vormen een partitie van G , dwz. er zijn elementen $\{g_1, g_2, \dots, g_k\}$ in G zodanig dat

$$G = C(g_1) \sqcup C(g_2) \sqcup \dots \sqcup C(*g_k)$$

en bijgevolg geldt dat

$$\#G = p^e = p^{a_{g_1}} + p^{a_{g_2}} + \dots + p^{a_{g_k}}$$

Een van de elementen g_i moet het eenheidselement zijn want daarvan is de conjugatieklasse gewoon $C(e) = \{e\}$. Stel bvb. dat $e = g_1$ dan wordt het vorige

$$p^e = 1 + p^{a_{g_2}} + \dots + p^{a_{g_k}}$$

Aan de rechterkant staan ofwel termen gelijk aan 1 ofwel een echte macht van p . Er is minstens één 1-term dus moeten er zo minstens een p -voud 1-termen zijn. Dus, er is

nog een $g_i \neq e$ waarvoor $C(g_i) = \{g_i\}$. Maar dit zegt dat g_i in het centrum van G zit, dwz. g_i commuteert met elk element van G .

We hebben dus aangetoond dat een p -groep steeds een niet-triviaal centrum heeft. Het centrum is steeds een normaaldeler en bijgevolg is de quotient-groep

$$\overline{G} = G/Z(G)$$

opnieuw een p -groep (of triviaal). Bijgevolg zijn is enige simpele p -groep de cyclische groep C_p van orde p . Dus, alle Jordanm-Hölder componenten van G zijn isomorf met C_p en bijgevolg is G oplosbaar. Opgave 73

Opgave 74. Omdat ieder automorfisme sommen respecteert en de identiteit is op $\mathbb{Q}$ volstaat het om de mogelijke beelden van $\sqrt{D}$ te bepalen. Een automorfisme σ moet ook producten respecteren en daarom geldt

$$D = \sigma(D) = \sigma((\sqrt{D})^2) = \sigma(\sqrt{D}) \cdot \sigma(\sqrt{D}) = \sigma(\sqrt{D})^2$$

en dus zijn er maar twee mogelijkheden

$$\sigma_1(\sqrt{D}) = \sqrt{D} \quad \text{of} \quad \sigma_2(\sqrt{D}) = -\sqrt{D}$$

In het eerste geval volgt voor alle $k \in \mathbb{Q}(\sqrt{D})$ dat

$$\sigma_1(r + s\sqrt{D}) = r + s\sqrt{D}$$

en dus is σ_1 de identiteit. Voor het tweede geval hebben we

$$\sigma_2(r + s\sqrt{D}) = r - s\sqrt{D}$$

en dit is een echt automorfisme. Twee keer σ_2 toepassen levert

$$\sigma_2 \circ \sigma_2(r + s\sqrt{D}) = \sigma_2(r - s\sqrt{D}) = r + s\sqrt{D}$$

en dus is σ_2 een element van orde twee. Opgave 74

Opgave 75. Stek dat $i\zeta$ erin zit dan zou ook i in $\mathbb{Q}(\zeta)$ moeten zitten. Bekijk nu complexe conjugatie : die stuurt $i \mapsto -i$ en op machten van ζ werkt complexe conjugatie als de identiteit. Bijgevolg kunnen we i niet schrijven van de vorm

$$q_1 + q_2\zeta + q_3\zeta^2 + q_4\zeta^3$$

Opgave 75

Opgave 76. Als $\zeta \in K$ dan moeten ook alle machten van $\zeta \in K$ dus is $\mathbb{Q}(\zeta) \subset K$. In vorige opgave hebben we gezien dat $i \notin \mathbb{Q}(\zeta)$ maar i moet wel in het splijtlichaam zitten (want een breuk van twee wortels $i\zeta$ en ζ). We kunnen ook aantonen dat er geen $\mathbb{Q}$ -lineaire betrekkingen zijn tussen de elementen

$$\{1, \zeta, \zeta^2, \zeta^3, i, i\zeta, i\zeta^2, i\zeta^3\}$$

Want stel dat

$$a + b\zeta + c\zeta^2 + d\zeta^3 + ei + fi\zeta + gi\zeta^2 + hi\zeta^3 = 0$$

met $\{a, \dots, h\} \subset \mathbb{Q}$. Bekijk opnieuw de complexe conjugatie dan stuurt die het linkerlid naar

$$a + b\zeta + c\zeta^2 + d\zeta^3 - ei - fi\zeta - gi\zeta^2 - hi\zeta^3$$

maar de complex toegevoegde van 0 is natuurlijk 0 dus geldt

$$-(a + b\zeta + c\zeta^2 + d\zeta^3) = 2(ei + fi\zeta + gi\zeta^2 + hi\zeta^3)$$

maar dan zouden we i kunnen schrijven als een element van $\mathbb{Q}(\zeta)$ en dat weten we al dat onmogelijk is. Opgave 76

Opgave 77. We geven de beelden van ζ en i voor enkele automorfismen

	<i>auto</i>	ζ	i
id	ζ	i	
σ	$i\zeta$	i	
σ^2	$-\zeta$	i	
σ^3	$-i\zeta$	i	
σ^4	ζ	i	
τ	ζ	$-i$	
τ^2	ζ	i	
$\sigma \circ \tau$	$i\zeta$	$-i$	
$\sigma^2 \circ \tau$	$-\zeta$	$-i$	
$\sigma^3 \circ \tau$	$-i\zeta$	$-i$	
$\tau \circ \sigma^3$	$i\zeta$	$-i$	

We zien dat we alle mogelijke combinaties van wortels al hebben dus de groep is inderdaad voortgebracht door σ en τ . Verder merken we op dat σ^4 en τ^2 de identiteit is en dat $\sigma \circ \tau$ hetzelfde automorfisme is als $\tau \circ \sigma^3$ wat de relaties aantoont. Opgave 77

Opgave 78. Er zijn juist 5 deelgroepen van orde twee, namelijk

$$\begin{cases} A = \{1, \sigma^2\} \\ B = \{1, \tau\} \\ C = \{1, \sigma\tau\} \\ D = \{1, \sigma^2, \tau\} \\ E = \{1, \sigma^3\tau\} \end{cases}$$

allen isomorf met C_2 . Daar elementen toe te voegen krijgen we juist drie deelgroepen van orde 4, namelijk

$$\begin{cases} S = \{1, \sigma, \sigma^2, \sigma^3\} \simeq C_4 \\ T = \{1, \sigma^2, \tau, \sigma^2\tau\} \simeq C_2 \times C_2 \\ U = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\} \simeq C_2 \times C_2 \end{cases}$$

en men gaat na dat de beweringen over normaaldelers gelden. Opgave 78

Opgave 79. Neem een algemeen element van K

$$x = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4i + a_5i\zeta + a_6i\zeta^2 + a_7i\zeta^3$$

en bereken nu $\sigma\tau(x)$

$$\sigma\tau(x) = a_0 + a_1i\zeta + a_2(-\zeta^2) + a_3(i\zeta^3) - a_4i - a_5i(i\zeta) + a_6(-i)(-\zeta^2) + a_7(-i)(-i\zeta^3)$$

Als dus $\sigma\tau(x) = x$ levert dit devolgende voorwaarden op de coëfficiënten

$$\begin{cases} a_0 = a_0 \\ a_1 = a_5 \\ a_3 = -a_7 \\ a_6 = a_6 \\ a_2 = 0 \\ a_4 = 0 \end{cases}$$

en dus bestaat K^C uit de elementen van de vorm

$$x = a_0 + a_1(1+i)\zeta + a_3(1-i)\zeta^3 + a_6i\zeta^2 = a_0 + a_1(1+i)\zeta + \frac{a_6}{2}((1+i)\zeta)^2 - \frac{a_3}{2}((1+i)\zeta)^3$$

en we zijn klaar.

Opgave 79

Opgave 80. Bereken dat

$$csc^{-1} = (2, 3) \quad c(2, 3)c^{-1} = (3, 4) \quad c(3, 4)c^{-1} = (4, 5)$$

maar dan zitten ook volgende elementen in de groep

$$(1, 2)(2, 3)(1, 2) = (1, 3) \quad (1, 3)(3, 4)(1, 3) = (1, 4) \quad (1, 4)(4, 5)(1, 4) = (1, 5)$$

en we hebben al gezien dat S_5 voortgebracht is door

$$\{(1, 2), (1, 3), (1, 4), (1, 5)\}$$

Opgave 80

Opgave 81. In een Abelse groep is iedere deelgroep een normaaldeler. Verder weten we dat de doorsnede van een p - en een q -Sylow deelgroep enkel het eenheidselement kan zijn (want de orde van een element in de doorsnede moet zowel een p -macht als een q -macht zijn). Dus is de deelgroep van G voortgebracht door alle Sylow-deelgroepen isomorf met hun direct product en dus van orde gelijk aan het product van de ordes van de verschillende Sylows. Maar dit product is ook het aantal elementen van G en dus is G isomorf met dit direct product.

Opgave 81

Opgave 82. Laat r het aantal p -Sylow deelgroepen zijn, dan moet gelden

$$r = 1 + pt \quad \text{en} \quad r|q$$

Omdat q een priemgetal is is dus of $r = 1$ of $r = q$. De tweede mogelijkheid is onmogelijk per onderstelling, dus heeft G een normale deelgroep P van orde p (die noodzakelijk cyclisch is). Neem u een voortbrenger van P , dus

$$P = \langle u \rangle \triangleleft G$$

Neem nu s het aantal q -Sylow deelgroepen van G dan geldt wederom dat

$$s = 1 + qm \quad \text{en} \quad s|p$$

Omdat p een priemgetal is geldt $s = 1$ of $s = p$. Maar $p < q$ dus kan de mogelijkheid $s = p$ niet wegens $s = 1 + q.m$ tenzij $m = 0$ en dus $s = 1$. Er is dus ook een normale q -Sylow deelgroep $Q = \langle v \rangle$ die automatisch cyclisch is met bvb. voortbrenger v .

Omdat u en v coprieme ordes hebben volgt dat $P \cap Q = \{e\}$ (gebruik Lagrange) en dus commuteren elementen van P en Q met elkaar (zie bewijs van de vorige stelling). Maar dan is het groeps morfisme $P \times Q \rightarrow P.Q$ ook injectief (wegens $P \cap Q = \{e\}$ (want als $p.q = e$ dan is $p = q^{-1}$ maar dan is $p = e = q^{-1}$). Bijgevolg is dit een isomorfisme en omdat de orde van $P \times Q$ gelijk is aan $p.q$ wat ook de orde is van G volgt dat $G = P.Q$. Maar dan is aan alle voorwaarden van de directe product stelling voldaan en hebben we dat

$$G = P \times Q$$

De orde van het element $w = (u, v)$ is gelijk aan $p.q$ dus is w een voortbrenger van G .

Opgave 82

$$r = 1 + 5t \quad \text{en} \quad r|8$$

dus is $r \in \{1, 2, 4, 8\}$ en enkel de mogelijkheid $r = 1$ voldoet aan $r = 1 + 5t$. Maar dan moet G een normale 5-Sylow deelgroep hebben en vermits $200 \neq 5^k$ kan G niet simpel zijn.

Opgave 83

$$r = 1 + 5.t \quad \text{en} \quad r|6$$

Herhaal nu deze redenering voor 3. Als s het aantal 3-Sylows is, dan geldt

$$s = 1 + 3.t \quad \text{en} \quad s|10$$

$$24 + 20 + 1 = 45$$

elementen moeten hebben, maar $\#G = 30$ dus hebben we een tegenspraak.

Opgave 85. Merk op dat de kubus $6 \times 9 = 54$ kleine vierkantjes heeft waarvan we er 6 (de middelste van iedere zijde) vastleggen om de oriëntatie van de kubus te bepalen. Bijgevolg zullen we iedere beweging kunnen voorstellen als een permutatie op de resterende $54 - 8 = 48$ vierkantjes. We gebruiken hiervoor devolgende afspraak uit de beginpositie (omdat verschillende versies van de Rubik kubus verschillende kleuren kunnen gebruiken is het beter te spreken over de fysieke oriëntatie van de zijvlakken ipv. hun kleur).

			1	2	3						
			4	U	5						
			6	7	8						
9	10	11	17	18	19	25	26	27	33	34	35
12	L	13	20	F	21	28	R	29	36	B	37
14	15	16	22	23	24	30	31	32	38	39	40
			41	42	43						
			44	D	45						
			46	47	48						

We gaan dan na dat de elementaire bewegingen voorgesteld worden door devolgende permutaties in S_{48} .

$$\begin{cases} F &= (17, 19, 24, 22)(18, 21, 23, 20)(6, 25, 43, 16)(7, 28, 42, 13)(8, 30, 41, 11) \\ B &= (33, 35, 40, 38)(34, 37, 39, 36)(3, 9, 46, 32)(2, 12, 47, 29)(1, 14, 48, 27) \\ L &= (9, 11, 16, 14)(10, 13, 15, 12)(1, 17, 41, 40)(4, 20, 44, 37)(6, 22, 46, 35) \\ R &= (25, 27, 32, 30)(26, 29, 31, 28)(3, 38, 43, 19)(5, 36, 45, 21)(8, 33, 48, 24) \\ U &= (1, 3, 8, 6)(2, 5, 7, 4)(9, 33, 25, 17)(10, 34, 26, 18)(11, 35, 27, 19) \\ D &= (41, 43, 48, 46)(42, 45, 47, 44)(14, 22, 30, 38)(15, 23, 31, 39)(16, 24, 32, 40) \end{cases}$$

Gebruik nu **GAP** of **sage** om de orde van de deelgroep van S_{48} te berekenen voortgebracht door deze 6 permutaties en check dat deze orde gelijk is aan

$$43252003274489856000 = 2^{27}3^{14}5^37^211$$

Opgave 85

Opgave 86. Elk van de voortbrengers van Rubik kan beschreven worden als een permutatie op deze 20 elementen en permuteert cyclisch 4 hoekkubussen en 4 zijde kubussen dus bestaat uit twee cycles van lengte vier en is bijgevolg een element van A_{20} .

Opgave 86

Opgave 87. Toon aan dat als $z \notin \{x, \sigma(x), \tau(x)\}$ dat dan z door $[\sigma, \tau]$ op zijn plaats gelaten wordt. Dus $[\sigma, \tau]$ is een 2- of een 3-cycle. Gebruik nu voorgaande oefening.

Opgave 87

Opgave 88. Orden de hoek-cubicles als volgt

$$(1, 2, \dots, 8) = (urf, urb, ulb, ulf, drf, drb, dlb, dlf)$$

dan zijn de ϕ -waarden van de voortbrengers van Rubik

$$\begin{cases} \phi(F) &= (1, 5, 8, 4) \\ \phi(R) &= (1, 2, 6, 5) \\ \phi(L) &= (3, 7, 8, 4) \\ \phi(U) &= (3, 2, 1, 4) \\ \phi(D) &= (5, 6, 7, 8) \\ \phi(B) &= (2, 3, 7, 6) \end{cases}$$

en met GAP berekenen we dat de orde van de deelgroep van S_8 voortgebracht door deze permutaties gelijk is aan $40320 = 8!$. Bijgevolg is ϕ surjectief. Analoog voor ψ : orden de zijde-cubicles als volgt

$$(1, 2, \dots, 12) = (uf, ur, ub, ul, df, dr, db, dl, fr, br, bl, fl)$$

dan zijn de ψ -beelden van de voortbrengers gegeven door de permutaties

$$\begin{cases} \psi(F) &= (1, 9, 5, 12) \\ \psi(R) &= (2, 10, 6, 9) \\ \psi(L) &= (4, 12, 8, 11) \\ \psi(U) &= (3, 2, 1, 4) \\ \psi(D) &= (5, 6, 9, 8) \\ \psi(B) &= (3, 11, 7, 10) \end{cases}$$

Wederom met GAP brengen deze permutaties een deelgroep van S_{12} voort van orde $479001600 = 12!$ en is dus ψ surjectief. De rest volgt uit oefening 86 of uit inspectie dat het teken van elk van de voortbrengers onder ϕ en ψ hetzelfde is. Opgave 88

Opgave 89. We hebben al gezien dat er epimorfismen bestaan

$$G \twoheadrightarrow A_8 \quad \text{en} \quad G \twoheadrightarrow A_{12}$$

door de actie op de hoekcubicles (resp. de midden-cubicles) te bekijken. Deze alternerende groepen zijn simpel en komen dus al voor als Jordan-Holder componenten. De orde van de Rubik groep heeft als priemdecompositie

$$\#G = 2^{27}3^{14}5^27^211$$

en deze van A_8 en A_{12} zijn

$$\#A_8 = 2^63^257 \quad \text{en} \quad \#A_{12} = 2^83^55711$$

Bijgevolg zijn de ordes van alle andere Jordan-Hölder factoren delers van

$$2^{13}3^7$$

en dus volgt uit de stelling van Burnside (zie volgend jaar) dat deze componenten oplosbaar zijn en dus ofwel C_2 of C_3 zijn. De Jordan-Hölder factoren (en multipliciteiten) zijn bijgevolg

$$A_8(1), A_{12}(1), C_2(13) \quad \text{en} \quad C_3(7)$$

Opgave 89