platform wiskunde nederland

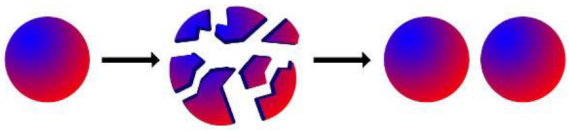
PLATFORM WISKUNDE VLAANDEREN

Banach-Tarski: hoe groepentheorie van één meloen er twee maakt

Syllabus Vakantiecursus 2024

(online versie)

Amsterdam, 23 en 24 augustus 2024
Antwerpen, 6 en 7 september 2024



platform wiskunde nederland

PLATFORM WISKUNDE VLAANDEREN

Banach-Tarski: hoe groepentheorie van één meloen er twee maakt

Syllabus Vakantiecursus 2024

(online versie)

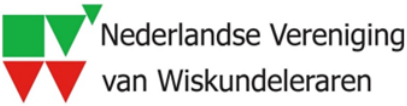
Amsterdam, 23 en 24 augustus 2024
Antwerpen, 6 en 7 september 2024

Programmacommissie

prof. dr. Wil Schilders (PWN, TU/e) (voorzitter)
dr. K.P. Hart (TUD) (eindredactie syllabus)
Joanne de Jager MSc (NVVW, Metis Montessori Lyceum)
prof. dr. Paul Levrie (UIA)
dr. Jeroen Spandaw (TUD)
Els Vanlommel (PWV, Heilig Hart van Maria Berlaar)
dr. Benne de Weger (TU/e) (eindredactie syllabus)

e-mail: `vakantiecursus@platformwiskunde.nl`

Sponsoren



Platform Wiskunde Nederland, Science Park 123, 1098 XG Amsterdam
Telefoon: 020-592 4006, Website: `https://platformwiskunde.nl`

Platform Wiskunde Vlaanderen
Website: `https://platformwiskunde.be`

Vakantiecursus 2024

De Vakantiecursus Wiskunde voor leraren in de exacte vakken op middelbare/hogere scholen en andere belangstellenden wordt al sinds 1946 jaarlijks gehouden, in eerste instantie door het in 1946 opgerichte Mathematisch Centrum (MC) in Amsterdam, tegenwoordig het Centrum Wiskunde en Informatica (CWI). Vanaf 2010 wordt de vakantiecursus georganiseerd door Platform Wiskunde Nederland (PWN) en werd de cursus steeds in twee opeenvolgende weekeinden gehouden, met als locaties Amsterdam en Eindhoven. Omdat er ook vaak Vlaamse deelnemers zijn, en om daarnaast de banden met het Platform Wiskunde Vlaanderen (PWV) te versterken[1], ontstond in 2022 het idee om de Vakantiecursus voortaan gezamenlijk te gaan organiseren. Vandaar dat vanaf 2023 de cursus ook in Vlaanderen plaatsvindt, namelijk aan de Universiteit van Antwerpen. We hopen dat dit jaar veel Vlaamse deelnemers acte-de-présence zullen geven, temeer omdat het thema rechtstreeks verband houdt met nieuwe richtlijnen van de Belgische regering voor het wiskundeonderwijs (aangaande abstractie). Daarnaast vindt de cursus natuurlijk ook weer plaats aan het CWI, zoals dat al sinds meer dan 75 jaar het geval is. Het thema dit jaar is wellicht enigszins abstract, anderzijds is het ook razend interessant, met wederom een aantal uitmuntende sprekers.

De Vakantiecursus wordt mede mogelijk gemaakt door een subsidie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO). De organisatie vindt plaats in nauwe samenwerking met het Centrum voor Wiskunde en Informatica (CWI) en de Universiteit van Antwerpen.

De presentaties van de sprekers zullen zo veel mogelijk beschikbaar komen op de PWN-website:
`https://www.platformwiskunde.nl/vakantiecursus`.

[1] Gedurende 2022-2023 organiseerden PWN en PWV ook samen de zeer succesvolle rondreizende tentoonstelling “Imaginary” (`www.imaginarymaths.nl` en `www.imaginarymaths.be`).

Historie

De eerste vakantiecursus wordt in het jaarverslag 1946 van het Mathematisch Centrum als volgt vermeld:

Op 29 en 31 Oct. '46 werd onder auspiciën van het M.C. een druk bezochte en uitstekend geslaagde vacantiecursus gehouden voor wiskundeleeraren in Nederland. Op 29 October stond de wiskunde, op 31 October de didactiek van de wiskunde op de voorgrond. De sprekers waren:

Prof. Dr. O. Bottema, "De prismoide",

Dr. A. Heyting, "Punten in het oneindige",

Mr. J. v. IJzeren, "Abstracte Meetkunde en haar betekenis voor de Schoolmeetkunde.",

Dr. H.D. Kloosterman, "Ontbinding in factoren",

Dr. G. Wielenga, "Is wiskunde-onderwijs voor alpha's noodzakelijk?",

Dr. J. de Groot, "Het scheppend vermogen van den wiskundige" en

Dr. N.L.H. Bunt, "Moeilijkheden van leerlingen bij het beginnend onderwijs in de meetkunde".

Aan het einde van de vacantiecursus werden diverse zaken besproken die het wiskunde-onderwijs in Nederland betroffen. Een Commissie werd ingesteld, die het M.C. over de verder te organiseren vakantiecursussen van advies zou dienen. Hierin namen zitting een vertegenwoordiger van de Inspecteurs van het V.H. en M.O. benevens vertegenwoordigers van de lerarenverenigingen Wimecos en Liwenagel.

Mede in verband met op deze vakantiecursus naar voren gekomen wenschen, werd ingesteld een colloquium over moderne Algebra, een dispuut over de didactiek van de wiskunde, beiden hoofdzakelijk bedoeld voor de leeraren uit Amsterdam en omgeving, terwijl tevens vanwege het M.C. een cursus over Getallenleer werd toegezegd te geven door de heeren v.d. Corput en Koksma. (Colloquium, dispuut en cursus zijn in 1947 gestart en verheugen zich in blijvende belangstelling).

Docenten

prof. dr. Stefaan Vaes (hoofddocent)
Departement Wiskunde, Katholieke Universiteit Leuven,
web: `https://www.stefaanvaes.eu/`
e-mail: `stefaan.vaes@kuleuven.be`

dr. Jeroen Spandaw
Delft Institute of Applied Mathematics, Technische Universiteit Delft,
web: `https://edu.nl/n3mw4`
e-mail: `j.g.spandaw@tudelft.nl`

prof. dr. David Eelbode
Departement Wiskunde, Universiteit Antwerpen,
web: `https://www.uantwerpen.be/en/staff/david-eelbode/`
e-mail: `david.eelbode@uantwerpen.be`

Programma

Vrijdag 23 augustus 2024 / 6 september 2024

15.00–15.30		*Ontvangst, koffie*
15.30–15.35		*Welkomstwoord*
15.35–16.20	Jeroen Spandaw	Inleiding groepentheorie (deel 1)
16.20–16.45		*Pauze*
16.45–17:30	Jeroen Spandaw	Inleiding groepentheorie (deel 2)
17.30–18.30		*Diner*
18.30–19.15	Jeroen Spandaw	Inleiding groepentheorie (deel 3)
19.15–19.45		*Pauze*
19.45–20.30	David Eelbode	Waarom complex niet per se moeilijk is een introductie tot de groep SU(2)

Zaterdag 24 augustus 2024 / 7 september 2024

09.00–10.00		*Ontvangst, koffie*
10.00–10.45	Stefaan Vaes	De stelling die we een paradox noemen
10.45–11.15		*Pauze*
11.15–12.00	Stefaan Vaes	De vrije groep $\mathbb{F}_2$ en twee vrije rotaties
12.00–13.00		*Lunch*
13.00–13.45	Stefaan Vaes	Het bewijs van de Stelling van Banach-Tarski
13.45–14.30	Stefaan Vaes	In het tweedimensionale vlak is alles anders
14.30		*Afsluiting*

1 Inleiding groepentheorie

Jeroen Spandaw

1.1 Inleiding

Mathematics is not a spectator sport! G. Pólya

Deze colleges geven een inleiding in de groepentheorie. We geven veel voorbeelden en we laten de nodige voorbeelden 'doorrekenen' door de lezer zodat zij of hij enige intuïtie kan ontwikkelen voor de groepentheoretische begrippen. De nadruk ligt hierbij op eindige groepen. Met de begrippen die hier behandeld worden zal Stefaan Vaes in zijn deel van de vakantiecursus een bewijs geven van de verbluffende paradox van Banach en Tarski.

1.2 Groepen: eerste definities en voorbeelden

Mathematics is the cheapest science. Unlike physics or chemistry, it does not require any expensive equipment. All one needs for mathematics is a pencil and paper. G. Pólya

1.2.1 De rotatiegroep van een vierkant

We beginnen met een voorbeeld. We kijken naar de rotatiesymmetrieën van een vierkant $ABCD$. We hebben bijvoorbeeld de rotatie r over 90° tegen de klok in. Deze rotatie draait hoekpunt A naar B, B naar C, C naar D en D naar A. We schrijven dit als

$$r = (A, B, C, D).$$

Dit betekent dus dat $A \mapsto B \mapsto C \mapsto D \mapsto A$.

Als we r twee keer achter elkaar uitvoeren, krijgen we een rotatie over $2 \times 90^\circ = 180^\circ$. We noteren dit als $r \circ r$ of als r^2. Het symbool '$\circ$' heet 'compositie' of 'samenstelling'. Dit kent u misschien uit de theorie van

functies: als $f(x) = x^2$ and $g(x) = x + 5$, dan is

$$(f \circ g)(x) = f(g(x)) = f(x + 5) = (x + 5)^2$$

maar

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 5.$$

We zien hier dat

$$f \circ g \neq g \circ f.$$

We zeggen dat f en g niet *commuteren*. In de groepentheorie zullen we dit ook vaak tegenkomen.

Terug naar de rotatie $r^2 = r \circ r$ van het vierkant $ABCD$. Deze rotatie beeldt het hoekpunt A af op C, B op D, C op A en D op B. Dit schrijven we als

$$r^2 = (A, C)(B, D).$$

We kunnen r ook drie keer achter elkaar uitvoeren. We krijgen dan

$$r^3 = r \circ r \circ r = r^2 \circ r = r \circ r^2 = (A, D, B, C).$$

Dit is een rotatie van het vierkant over 270° tegen de klok in of van 90° met de klok mee.

Als we r vier keer achter elkaar uitvoeren, dan gaat A naar A, B naar B, C naar C en D naar D. Kortom, de rotatie r^4 is de *identiteitsafbeelding* van het vierkant, de afbeelding die ieder punt op zichzelf afbeeldt. We noteren de identiteitsafbeelding als e. Er geldt dus

$$r^4 = r \circ r \circ r \circ r = (A)(B)(C)(D) = e.$$

Als we twee rotaties r_1, r_2 hebben van het vierkant $ABCD$, dan is de samenstelling $r_1 \circ r_2$ ook een rotatie van het vierkant. (Let op: je past eerst r_2 toe en daarna r_1!) Bijvoorbeeld geldt

$$r^3 \circ r^2 = r^5 = r = (A, B, C, D).$$

De volgende 4×4-tabel bevat alle $4 \times 4 = 16$ composities:

$r_1 \circ r_2$	$r_2 = e$	$r_2 = r$	$r_2 = r^2$	$r_2 = r^3$
$r_2 = e$	e	r	r^2	r^3
$r_2 = r$	r	r^2	r^3	e
$r_2 = r^2$	r^2	r^3	e	r
$r_3 = r^3$	r^3	e	r	r^2

Dit is ons eerste voorbeeld van een groep!

Definitie 1.2.1. Een *groep* is een verzameling G plus een afbeelding $G \times G \to G$ die aan ieder paar (g_1, g_2) een element $g_1 \circ g_2$ in G toevoegt zodat aan de volgende drie eisen is voldaan:

1. voor alle g_1, g_2, g_3 in G geldt: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$;
2. er is een element $e \in G$ zodat voor alle $g \in G$ geldt: $e \circ g = g \circ e = g$;
3. voor ieder element $g \in G$ is er een element $h \in G$ zodat $g \circ h = h \circ g = e$.

'$\circ$' wordt de *groepsbewerking* of *groepsvermenigvuldiging* genoemd. De eerste eigenschap wordt de *associativiteit* van de groepsbewerking genoemd. Het (unieke) element e wordt de *groepsidentiteit* of het *neutrale element* van de groep genoemd. Het (unieke) element h met $h \circ g = g \circ h = e$ wordt *de inverse van* g genoemd en genoteerd als g^{-1}.

Laten we verifiëren dat

$$G_1 = \{e, r, r^2, r^3\}$$

met de compositie $\circ$ een groep vormt met neutraal element e. De associativiteit van $\circ$ is duidelijk, want als f, g, en h afbeeldingen van een verzameling X naar zichzelf zijn, dan geldt voor iedere $p \in X$:

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

en

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

Het is ook duidelijk dat voor alle $g \in G$ geldt: $g \circ e = e \circ g = g$. Tot slot: je ziet snel in dat

$$e^{-1} = e \qquad r^{-1} = r^3 \qquad r^{-2} = r^2 \qquad r^{-3} = r.$$

Hier schrijven we r^{-3} voor

$$(r^3)^{-1} = (r^{-1})^3,$$

enzovoorts.

1.2.2 De symmetriegroep van een vierkant

Laten we nu de spiegelingen van het vierkant $ABCD$ bekijken. In de *cykelnotatie* die we hieronder zullen leren kennen, hebben we

$$s_1 = (AB)(CD) \qquad s_2 = (AD)(BC) \qquad s_3 = (AC) \qquad s_4 = (BD).$$

(In $s_3 = (AC)$ worden B en D niet genoemd; dat betekent dat s_3 deze twee punten op zichzelf afbeeldt. Soms schrijven we komma's in de cykelnotatie, bijvoorbeeld $s_1 = (A, B)(C, D)$, maar wanneer er geen verwarring

te verwachten valt laten we die komma's meestal weg.) De spiegelassen zijn respectievelijk: de middelloodlijn van AB, de middelloodlijn van AD, de diagonaal BD en de diagonaal AC. De vier spiegelingen vormen *geen* groep. Ten eerste bevat $\{s_1, s_2, s_3, s_4\}$ geen neutraal element e en ten tweede is bijvoorbeeld de samenstelling

$$s_3 \circ s_4 = (AC)(BD) = r^2$$

geen element van $\{s_1, s_2, s_3, s_4\}$. Maar de verzameling

$$G_2 = \{e, r, r^2, r^3, s_1, s_2, s_3, s_4\}$$

met de compositie $\circ$ als groepsbewerking is *wel* een groep!

Opgave 1.2.2. Schrijf de 8×8-vermenigvuldigingstabel op en verifieer dat G_2 met $\circ$ een groep is.

Definitie 1.2.3. Een ondergroep of deelgroep[1] van een groep $(G, \circ)$ is een deelverzameling H van G die het neutrale element e van G bevat zodat voor alle $h_1, h_2 \in H$ het product $h_1 \circ h_2$ ook in H ligt.

Opgave 1.2.4. Verifieer dat een ondergroep H van G een groep is met $\circ$ ingeperkt tot H als groepsvermenigvuldiging.

Opgave 1.2.5. Verifieer dat G_1 een ondergroep is van G_2.

1.2.3 Eerste elementaire eigenschappen van groepen

Opgave 1.2.6. Laat zien dat een groep G maar één neutraal element e bezit. (Hint: Neem aan dat $e_1, e_2 \in G$ neutrale elementen zijn en bekijk het product $e_1 \circ e_2$.)

Opgave 1.2.7. Laat G een groep zijn en $g \in G$. Laat zien dat g precies één inverse element h heeft.

1.2.4 Permutatiegroepen

Neem een verzameling X en definieer

$$S(X) := \{f \colon X \to X \mid f \text{ is bijectief}\}.$$

'Bijectief' wil zeggen: voor iedere $q \in X$ is er precies één $p \in X$ zodat $f(p) = q$. Equivalent: er is een $g \in S(X)$ zodat

$$f \circ g = g \circ f = e,$$

[1] Nederlands: ondergroep; Vlaams: deelgroep; Engels: subgroup; Duits: Untergruppe

waarbij e de identiteitsafbeelding $X \to X$ is, dus $e(p) = p$ voor iedere $p \in X$. Bijecties $X \to X$ worden vaak *permutaties van* X genoemd.

Opgave 1.2.8. Verifieer dat $S(X)$ met compositie $\circ$ als groepsbewerking een groep is met neutraal element e.

Meestal nemen we voor X een eindige verzameling. Als $X = \{1, \ldots, N\}$ dan schrijven we S_N in plaats van $S(X)$. Dit heet de *symmetrische groep van graad* N.

Opgave 1.2.9. Overtuig uzelf dat S_N precies $N!$ elementen bevat.

Er zijn twee gangbare notaties voor elementen van S_N. Voor $N = 6$ hebben we bijvoorbeeld

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}.$$

Dit betekent:

$$f(1) = 5 \quad f(2) = 2 \quad f(3) = 1 \quad f(4) = 6 \quad f(5) = 3 \quad f(6) = 4.$$

Dit wordt meestal genoteerd als

$$f = (153)(2)(46) = (153)(46).$$

Dit betekent dus: $1 \mapsto 5 \mapsto 3 \mapsto 1$, $2 \mapsto 2$ en $4 \mapsto 6 \mapsto 4$. Dit wordt *cykelnotatie* genoemd. Merk trouwens op dat de cykelnotatie van een permutatie niet uniek is vanwege

$$(153) = (531) = (315) \neq (135) \qquad (46) = (64) \qquad (153)(46) = (46)(153).$$

De factoren (153), (2) en (46) worden *cykels* genoemd, omdat ze respectievelijk 3, 1 en 2 elementen van X cyclisch permuteren. Cykels als (2) van lengte 1 worden meestal weggelaten, omdat ze 'niets doen'. Het neutrale element van S_6 is

$$e = (1)(2)(3)(4)(5)(6) = (1).$$

We hadden ook $e = (5)$ of $e = (4)(2)$ kunnen schrijven, etcetera. Het zijn allemaal manieren om 'de permutatie e die niets doet' te noteren. Persoonlijk ben ik gewend om $e = (1)$ te schrijven, maar soms zie je ook wel $e = ()$, bijvoorbeeld in de software GAP.

Opmerking 1.2.10. De cykelnotatie hebben we in wezen al gebruikt bij de groepen G_1 en G_2: symmetrieën van het vierkant beschreven we door hun werking op de vier hoekpunten. (We hadden natuurlijk ook andere beschrijvingen kunnen gebruiken in termen van rotatiehoeken en spiegellijnen.)

Opgave 1.2.11. Neem $N = 7$, $\sigma = (153)(46)$ en $\tau = (13)(2645)$. Bereken σ^2 en τ^{-1} en $\sigma \circ \tau$. Antwoorden: $\sigma^2 = (135)(4)(6) = (135)$, $\tau^{-1} = (13)(5462)$ en $\sigma \circ \tau = (1)(2435) = (2435)$.

Opgave 1.2.12. U kunt het bovenstaande verifiëren met de software GAP. Definieer bijvoorbeeld

```
s := (4,6)*(1,5,3);
t := (2,6,4,5)*(1,3);
s^2;
t^(-1);
t*s;
```


Let op: wat wij $s \circ t$ noemen ('s na t'), heet in GAP `t*s` ('eerst t, dan s'). GAP eist uiteraard komma's in de cykelnotatie. Bijvoorbeeld zou `(13)` geïnterpreteerd worden als de permutatie die het punt 13 op zichzelf afbeeldt. Dus als we de permutatie $(1, 3)$ bedoelen, moeten we in GAP `(1,3)` intikken.


Ook in GAP wordt het cykel $(2, 6, 4, 5)$ geïnterpreteerd als $2 \mapsto 6 \mapsto 4 \mapsto 5 \mapsto 2$.


Omdat de cykels $(4, 6)$ en $(1, 5, 3)$ disjunct zijn, geldt

$$(4, 6)(1, 5, 3) = (1, 5, 3)(4, 6).$$

In dit geval kun je in GAP het vermenigvuldigingssterretje weglaten. Bij vermenigvuldiging van niet-disjuncte cykels, bijvoorbeeld $(1, 2)(2, 3) = (1, 2, 3)$, is het vermenigvuldigingssterretje verplicht in GAP.

Opgave 1.2.13. Check $(1, 2)(2, 3) = (1, 2, 3)$ in GAP. Is het `(1,2)*(2,3)` of `(2,3)*(1,2)` in GAP?

Definitie 1.2.14. Een groep G heet *commutatief* of *abels* (naar de Noorse wiskundige Niels Henrik Abel) als $g_1 g_2 = g_2 g_1$ voor alle groepselementen $g_1, g_2 \in G$. Hierbij hebben we de gebruikelijke afkorting

$$g_1 g_2 = g_1 \circ g_2$$

gebruikt.

Opgave 1.2.15. De kleinste groep die niet commutatief is, is de permutatiegroep S_3 met $3! = 6$ elementen. De 6 elementen zijn $e = () = (1) = (1)(2)(3)$, $(12) = (12)(3)$, $(13) = (13)(2)$, $(23) = (23)(1)$, (123) en $(321) = (132)$. Controleer dat

$$(12)(13) = (132) \qquad (13)(12) = (123)$$

en schrijf de hele 6×6-vermenigvuldigingstabel op.

1.2.5 Even versus oneven permutaties

Een permutatie is ofwel *even* ofwel *oneven*. We noemen dit de *pariteit* van de permutatie.

Definitie 1.2.16. Laat σ een permutatie zijn van $X = \{1, \ldots, n\}$. Een *inversie* van σ is een paar (i, j) met $i, j \in X$, $i < j$ en $\sigma(i) > \sigma(j)$. De permutatie σ heet *(on)even* als het aantal inversies van σ (on)even is.

Opgave 1.2.17. Is de eenheidspermutatie e (met $e(i) = i$ voor alle $i \in X$) even of oneven?

Opgave 1.2.18. Laat zien dat de permutatie $(2, 5)$ van $X = \{1, \ldots 6\}$ oneven is.

Opgave 1.2.19. Laat zien dat de permutaties $(1, n)$ oneven zijn voor $n = 2, 3, 4, \ldots$.

De volgende stelling vertelt ons dat pariteit zich gedraagt onder de groepsvermenigvuldiging van de permutatiegroep (d.w.z. onder compositie van permutaties) zoals je hoopt. Bewijzen vindt u in vrijwel ieder boek over elementaire groepentheorie. We geven hier alleen een schets van een bewijs.

Stelling 1.2.20. *Het product (de compositie) van twee even permutaties of van twee oneven permutaties is even. Het product (de compositie) van een even en een oneven permutatie of van een oneven en een even permutatie is oneven.*

Bewijs. Bij iedere permutatie σ van $X = \{1, \ldots, n\}$ hoort een $n \times n$-matrix $A = A_\sigma$ zodat $A_{i,j} = 1$ als $\sigma(i) = j$ en $A_{i,j}$ als $\sigma(i) \neq j$ voor $i, j \in X$. De determinant van A_σ is ± 1. Er geldt: $\det(A_\sigma) = 1$ als σ even is en $\det(A_\sigma) = -1$ als σ oneven is. Als $\sigma, \tau \in S_n$, dan is de matrix $A_{\sigma\tau}$ die hoort bij de permutatie $\sigma\tau$ gelijk aan het matrixproduct $A_\sigma A_\tau$. Daarom geldt $\det(A_{\sigma\tau}) = \det(A_\sigma)\det(A_\tau)$. □

Opgave 1.2.21. Verifieer dat (a) $A_{\sigma\tau} = A_\sigma A_\tau$ en (b) $\det(A_\sigma) = 1$ precies dan als σ even is.

Definitie 1.2.22. We definiëren de *alternerende groep van graad n* als

$$A_n := \{\sigma \in S_n \mid \sigma \text{ is even}\}.$$

Opgave 1.2.23. Verifieer dat A_n een ondergroep is van de symmetrische groep S_n.

Opgave 1.2.24. Neem $n \geq 2$. Bewijs dat de orde van A_n gelijk is aan $\frac{1}{2}n!$. (Hint: vermenigvuldiging met de permutatie $(1, 2)$ geeft een bijectie tussen

de verzameling A_n van even permutaties in S_n en de verzameling $S_n \setminus A_n$ van oneven permutaties in S_n.)

Opgave 1.2.25. Schrijf alle 12 elementen van A_4 in cykelnotatie. Verifieer dat alleen de cykeltypes $1+1+1+1$, $2+2$ en $3+1$ voorkomen. Hoe vaak komt ieder cykeltype voor?

1.2.6 Enkele oneindige groepen

De groepen G_1 en G_2 zijn *eindig*: ze hebben een eindig aantal elementen:

$$|G_1| = 4 \qquad |G_2| = 8.$$

Dit aantal wordt de *orde* van de groep genoemd.

Er bestaan echter ook oneindige groepen.

Opgave 1.2.26. Welke van de volgende structuren zijn groepen?

1. de reële getallen $\mathbf{R}$, de rationale getallen $\mathbf{Q}$, de gehele getallen $\mathbf{Z}$, de even natuurlijke getallen $2\mathbf{Z}$, de natuurlijke getallen $\mathbf{N}$ met optelling als groepsbewerking en $e = 0$;
2. de reële getallen $\mathbf{R}$, de rationale getallen $\mathbf{Q}$, de gehele getallen $\mathbf{Z}$, de even natuurlijke getallen $2\mathbf{Z}$, de natuurlijke getallen $\mathbf{N}$ met vermenigvuldiging als groepsbewerking en $e = 1$;
3. $\mathbf{R}^* := \mathbf{R} \setminus \{0\}$, $\mathbf{Q}^* := \mathbf{Q} \setminus \{0\}$, $\mathbf{Z}^* := \mathbf{Z} \setminus \{0\}$ met vermenigvuldiging als groepsbewerking en $e = 1$;
4. de translaties van het vlak $\mathbf{R}^2$ met samenstelling als groepsbewerking;
5. de rotaties van het vlak $\mathbf{R}^2$ (met een vast rotatiecentrum of met een variabel rotatiecentrum) met samenstelling als groepsbewerking;
6. de translaties en rotaties van het vlak $\mathbf{R}^2$ met samenstelling als groepsbewerking;
7. de spiegelingen van het vlak $\mathbf{R}^2$ met samenstelling als groepsbewerking;
8. de translaties, rotaties en spiegelingen van het vlak $\mathbf{R}^2$ met samenstelling als groepsbewerking;
9. de rotaties van $\mathbf{R}^3$ die $O = (0, 0, 0)$ vasthouden met samenstelling als groepsbewerking.

1.3 De rotatiegroep van een kubus

It is better to solve one problem five different ways, than to solve five problems one way. G. Pólya

In dit hoofdstuk bestuderen we de rotatiegroep van een kubus. We zullen de elementen van de groep op verschillende manieren tellen en beschrijven. Zo maken we kennis met het belangrijke fenomeen *de werking van een groep op een verzameling*[2]. De rotatiegroep van de kubus is een mooi oefenvoorbeeld: de groep heeft al enige complexiteit, waardoor je kennis kunt maken met typische groepentheoretische verschijnselen, maar de groep is toch nog steeds goed behapbaar. Bovendien zijn er interessante verbindingen tussen groepentheoretische eigenschappen van de rotatiegroep van de kubus en meetkundige eigenschappen van de kubus zelf.

1.3.1 Enkele groepswerkingen

We hebben al een voorbeeld van een groepswerking gezien: een symmetrie van een vierkant hebben we beschreven door de werking van die symmetrie op de 4 hoekpunten van het vierkant. Analoog kunnen we een rotatie (of een spiegeling) van een kubus beschrijven door de werking van die symmetrie op de 8 hoekpunten van de kubus.

De rotatiegroep G_1 en de symmetriegroep G_2 van het vierkant $ABCD$ werkt ook op de verzameling $\{\alpha, \beta\}$, waarbij α en β de diagonalen AC respectievelijk BD zijn. Bijvoorbeeld beeldt de rotatie $r = (ABCD)$ de diagonaal α op de diagonaal β af en omgekeerd. De spiegeling $s_4 = (BD) = (A)(C)(BD)$ daarentegen beeldt beide diagonalen op zichzelf af. (De diagonaal β wordt weliswaar gespiegeld, maar toch geldt $s_4(\beta) = \beta$, omdat we met α en β diagonalen 'zonder richting' bedoelden.)

Opgave 1.3.1. Verifieer tabel 1.1

We zien dat de werking van een rotatie of een spiegeling op de verzameling $\{\alpha, \beta\}$ niet voldoende is om die symmetrie vast te leggen. (De helft van de 8 symmetrieën van het vierkant houdt beide diagonalen vast en de overige 4 symmetrieën van het vierkant verwisselt ze.) Wiskundigen zeggen dat de werking van de symmetriegroep G_2 op $\{\alpha, \beta\}$ niet *trouw* is. (Merk op dat zelfs de werking van de kleinere rotatiegroep G_1 niet trouw is: de twee rotaties e en r^2 houden de diagonalen vast en de twee rotaties r en r^3 verwisselen ze.)

[2] In plaats van 'groepswerking' worden ook de woorden 'groepsactie' en 'groepsoperatie' gebruikt.

	α	β
$e = (A)(B)(C)(D) = ()$	α	β
$r = (ABCD)$	β	α
$r^2 = (AC)(BD)$	α	β
$r^3 = (ADCB)$	β	α
$s_1 = (AB)(CD)$	β	α
$s_2 = (AD)(BC)$	β	α
$s_3 = (AC)(B)(D) = (AC)$	α	β
$s_4 = (A)(C)(BD) = (BD)$	α	β

Tabel 1.1: Tabel bij opgave 1.3.1

De verzameling van 2 diagonalen van het vierkant is simpelweg te klein om de rotatiegroep G_1 van orde 4 en de symmetriegroep G_2 van orde 8 te kunnen beschrijven. De werkingen van de groepen G_1 en G_2 op de verzameling $\{A, B, C, D\}$ van de 4 hoekpunten van het vierkant zijn daarentegen wel trouw, want de werking van een element van G_2 op die verzameling legt dat element éénduidig vast.

Opgave 1.3.2. Laat $\mathcal{K}$ de rotatiegroep zijn van de kubus. Deze groep werkt op de verzameling H van hoekpunten van de kubus, de verzameling R van ribben van de kubus en de verzameling V van zijvlakken van de kubus. (Er geldt dus $|H| = 8$, $|R| = 12$ en $|V| = 6$.) Welke van deze drie groepswerkingen van $\mathcal{K}$ zijn trouw?

1.3.2 De rotaties van een kubus

Hoeveel rotaties heeft een kubus? (Hierbij rekenen we de identiteitsafbeelding e mee.) We geven 4 methoden om dit aantal te berekenen. Gelukkig geven ze allemaal hetzelfde resultaat!

Eerste methode: zijvlakken

Neem een Rubik-kubus met een wit, zwart, blauw, groen, rood en oranje zijvlak (W, Z, B, G, R, O). We kunnen een rotatie van de kubus gedeeltelijk beschrijven door te zeggen waar het witte zijvlak heengaat. Hiervoor zijn 6 mogelijkheden. Laten we bijvoorbeeld kijken naar de rotaties van de kubus die het witte zijvlak naar het rode zijvlak afbeelden. (We roteren de kubus in zijn geheel, dus we doen geen 'Rubik-bewegingen' met 'losse lagen'.) Door de informatie $W \mapsto R$ ligt de rotatie nog niet vast. Er

zijn nog 4 opties, want nadat we het witte naar het rode zijvlak hebben afgebeeld, kunnen we nog vier rotaties van de kubus (inclusief de identiteitsafbeelding) toepassen die het rode zijvlak naar zichzelf afbeelden. Het totale aantal rotaties is dus

$$6 \times 4 = 24.$$

(Merk op dat we iedere rotatie, inclusief de identiteit, precies één keer hebben geteld.)

Tweede methode: hoekpunten

Opgave 1.3.3. Pas dezelfde denkwijze toe op hoekpunten in plaats van zijvlakken. Als het goed is, krijgt u opnieuw 24 rotaties van de kubus.

Derde methode: ribben

Opgave 1.3.4. Pas dezelfde denkwijze toe op ribben in plaats van zijvlakken of hoekpunten. Als het goed is, krijgt u opnieuw 24 rotaties van de kubus.

Intermezzo: de orde van groepselementen

Voordat we naar de vierde methode gaan om de rotaties van de kubus te tellen, moeten we eerst iets zeggen over de orde van een groepselement. Als we een groep G hebben en een element $g \in G$, dan kunnen we kijken naar de rij

$$g, g^2, g^3, g^4, \ldots.$$

Als g bijvoorbeeld een rotatie is van het vlak over 30°, dan geldt $g^{12} = g^{24} = g^{36} = \cdots = e$, terwijl $g, \ldots, g^{11}$ allemaal verschillend van e zijn.

Definitie 1.3.5. Laat G een groep zijn en $g \in G$. Stel dat er een positief geheel getal n bestaat zodat $g^n = \underbrace{g \circ \cdots \circ g}_{n} = e$. Het kleinste positieve gehele getal met deze eigenschap wordt de *orde* van het element g genoemd.

De rotatie van het vlak over 30° heeft dus orde 12. Niet alle groepselementen hebben een (eindige) orde. Neem bijvoorbeeld de rotatie r van het vlak over 1 radiaal. De rotatie r^n is de rotatie over n radialen en dit is precies dan de eenheidsrotatie als $n = 2\pi k$ voor een positief geheel getal k. Maar zulke positieve gehele getallen n en k bestaan niet, omdat π een irrationaal getal is. In *eindige* groepen hebben alle groepselementen *wel* een orde.

Lemma 1.3.6. *Als G een eindige groep is en $g \in G$, dan is er een positief natuurlijk getal n zodat $g^n = e$.*

Bewijs. Kijk naar de rij $g, g^2, g^3, \ldots, g^{N+1}$, waarbij $N = |G|$. In dit rijtje van lengte $N+1$ moet een herhaling zitten, want al die elementen zitten in de verzameling G van grootte N. Als $g^i = g^j$ met $i < j$, dan geldt $g^{j-i} = e$ en $j - i > 0$. □

Het bewijs laat zien dat de orde van een element hoogstens gelijk is aan de orde van de groep. (Het is gemakkelijk om voorbeelden te vinden van groepen en elementen wier orde gelijk is aan de orde van de groep. Neem bijvoorbeeld de rotaties van de regelmatige N-hoek in het vlak (met $N \geq 3$) en een rotatie over $360°/N$.) We zullen later zien dat in eindige groepen de orde van de elementen delers zijn van de orde van de groep. Bijvoorbeeld hebben de rotaties van de regelmatige 10-hoek ordes 1, 2, 5 en 10. Uiteraard is in iedere groep e het enige element met orde 1.

Vierde methode: typen rotaties

Nu we het begrip 'orde van een groepselement' kennen, kunnen we de vierde methode beschrijven om de rotaties van een kubus te tellen. Deze methode vergt meer werk, maar levert meer op dan alleen maar het aantal 24, namelijk een beschrijving van de 24 rotaties, hun ordes en een opdeling in een aantal typen.

Allereerst hebben we de identiteitsafbeelding e. Vanaf nu kijken we alleen naar rotaties r van de kubus met $r \neq e$, dus rotaties 'die echt iets doen'. Zo'n rotatie heeft (volgens een stelling van Euler) een rotatieas, die door het centrum van de kubus gaat. Er zijn 3 typen rotatieassen:

(v) rotatieassen die tegenoverliggende middens van zijvlakken verbinden;

(h) rotatieassen die tegenoverliggende hoekpunten van de kubus verbinden;

(r) rotatieassen die tegenoverliggende middens van ribben verbinden.

Er zijn 6 zijvlakken, dus er zijn 3 rotatieassen van type 'v'. Om ieder van die rotatieassen hebben we twee rotaties van orde 4 over $\pm 90°$ en één rotatie van orde 2 over $\pm 180°$. (De rotatierichting doet er bij een rotatie over $\pm 180°$ niet toe, want we kijken niet naar het totale draaiproces, maar alleen naar de uitkomst. Bij rotaties over $\pm 90°$ doet de draairichting er natuurlijk *wel* toe.) Er zijn dus

$$6 + 3 = 9$$

rotaties van type 'v'.

Opgave 1.3.7. Laat zien dat er 8 rotaties van type 'h' zijn (van orde 3) en 6 rotaties van type 'r' (van orde 2).

We vinden dus:

- één identiteit van orde 1;
- 3 rotaties van type 'v' van orde 2;
- 6 rotaties van type 'v' van orde 4;
- 8 rotaties van type 'h' van orde 3;
- 6 rotaties van type 'r' van orde 2.

In totaal geeft dit

$$1 + 3 + 6 + 8 + 6 = 24$$

rotaties van de kubus.

We hebben nu vier keer de volgende stelling bewezen:

Stelling 1.3.8. *De groep $\mathcal{K}$ van rotaties van de 3-dimensionale kubus heeft precies 24 elementen.*

1.3.3 De permutatiegroep S_4

Behalve $\mathcal{K}$ kennen we nog een groep van orde 24: de groep S_4 van permutaties van $X = \{1, 2, 3, 4\}$. De elementen van S_4 schrijven we in cykelnotatie. We vinden dan vijf 'cykeltypes':

$$e = (1)(2)(3)(4) \quad (12) = (12)(3)(4) \quad (123) = (123)(4) \quad (12)(34) \quad (1234),$$

corresponderend met de vijf partities van het getal 4, namelijk $1+1+1+1$, $2+1+1$, $3+1$, $2+2$, respectievelijk 4.
Laten we het cykeltype $(123) = (123)(4)$ bekijken. Er zijn 8 permutaties van dit type:

$$(123), (132), (124), (142), (134), (143), (234), (243).$$

Al deze permutaties hebben orde 3.

Opgave 1.3.9. Werk voor ieder cykeltype in S_4 uit hoeveel permutaties van dat cykeltype bestaan en welke orde die permutaties hebben.

Opgave 1.3.10. Vergelijk dit met de tabel hierboven van rotatietypen van de kubus. Wat valt u op? Kunt u een vermoeden formuleren?

1.3.4 Het verband tussen de groepen $\mathcal{K}$ en S_4

We hebben ontdekt dat de groepen $\mathcal{K}$ en S_4 erg veel op elkaar lijken: ze hebben evenveel elementen in totaal, de ordes van de elementen zijn 1, 2, 3 en 4, en voor iedere orde zijn er evenveel elementen. Bovendien hebben ze een zelfde indeling in 'types' met steeds evenveel elementen per type die ook nog eens corresponderen in hun orde.[3]

We zullen laten zien dat de groepen $\mathcal{K}$ en S_4 inderdaad *isomorf* zijn. Dit betekent dat er een bijectie[4]

$$\Phi\colon \mathcal{K} \to S_4$$

bestaat die compatibel is met de groepsstructuren van $\mathcal{K}$ en S_4. Dit laatste betekent:

$$\Phi(g_1 \circ g_2) = \Phi(g_1) \circ \Phi(g_2)$$

voor alle $g_1, g_2 \in \mathcal{K}$. Merk op dat de groepsbewerking $\circ$ in $g_1 \circ g_2$ plaatsvindt in $\mathcal{K}$, terwijl de groepsbewerking $\circ$ in $\Phi(g_1) \circ \Phi(g_2)$ plaatsvindt in S_4. Zo'n groepsstructuurbehoudende bijectie heet een *isomorfisme van de groep $\mathcal{K}$ naar (of op) de groep S_4*. We zullen deze bijectie expliciet construeren, gebruikmakend van ons meetkundig begrip van de kubus. (We gaan dus meetkundig inzicht vertalen in groepentheoretische abstractie. Vergelijk met de voetnoot over 'typen': daar hebben we meetkundige intuïtie rondom typen rotaties van de kubus vertaald naar het puur groepentheoretische concept van conjungatie.)

Algemener hebben we de volgende definitie:

Definitie 1.3.11. Als G en G' groepen zijn, dan is een *groepshomomorfisme* F van G naar G' een afbeelding $F\colon G \to G'$ zodat

$$F(g_1 \circ g_2) = F(g_1) \circ F(g_2)$$

voor alle $g_1, g_2 \in G$. Merk weer op dat de groepsbewerking $\circ$ in $g_1 \circ g_2$ plaatsvindt in de groep G, terwijl de groepsbewerking $\circ$ in $F(g_1) \circ F(g_2)$ plaatsvindt in de groep G'.

Een groepshomomorfisme is dus net als een groepsisomorfisme een afbeelding die compatibel is met de groepsstructuren. Een groepsisomorfisme is een homomorfisme dat ook nog eens bijectief is.

[3] We hebben 'type' enigszins intuïtief gedefinieerd. De correcte groepentheoretische definitie betreft het begrip *conjungatie*. Twee elementen g_1 en g_2 in een groep G zijn geconjungeerd als er een $h \in G$ bestaat zodat $g_1 h = h g_2$. Je kunt verifiëren dat twee elementen in $\mathcal{K}$ of S_4 precies dan geconjungeerd zijn als ze hetzelfde type hebben.

[4] Een afbeelding $f\colon X \to Y$ is bijectief als er voor iedere $y \in Y$ precies één $x \in X$ bestaat met $f(x) = y$.

Opgave 1.3.12. Laat G een groep zijn. Welke van de volgende 3 afbeeldingen zijn groepshomomorfismen of zelfs groepsisomorfismen? (1) de afbeelding $G \to G$ die ieder element g op zichzelf afbeeldt; (2) de afbeelding $G \to G$ die ieder element g op het eenheidselement e afbeeldt; (3) de afbeelding $G \to G$ die ieder element g op zijn inverse g^{-1} afbeeldt.

Opgave 1.3.13. Laat $F\colon G \to G'$ een groepshomomorpfisme zijn. Laat zien dat $F(e_1) = e_2$, waarbij e_1 het neutrale element van G_1 is en e_2 het neutrale element van G'. Laat ook zien dat

$$(F(g))^{-1} = F\left(g^{-1}\right)$$

voor iedere $g \in G$.

Opgave 1.3.14. Laat G een groep zijn en laat $g \in G$. Laat $f\colon G \to G$ de afbeelding zijn die $x \in G$ op gxg^{-1} afbeeldt. (Dit heet 'conjungeren (van x) met g'. Als u wel eens met een Rubik's kubus heeft gespeeld, heeft u vermoedelijk vaak al vaak geconjungeerd.) Laat zien dat f een groepsisomorfisme is van G naar zichzelf. (Een isomorfisme van een groep naar zichzelf wordt ook wel een *automorfisme* genoemd.)

Opgave 1.3.15. Neem de groep S_n met $n \geq 2$, zeg S_5, en neem $g = (1, 2)$. Onderzoek voor een paar elementen $x \in S_n$ het verband tussen x en zijn geconjungeerde $(12)x(12)^{-1}$. Kunt u beschrijven wat er gebeurt? Kunt u dit bewijzen of plausibel maken?

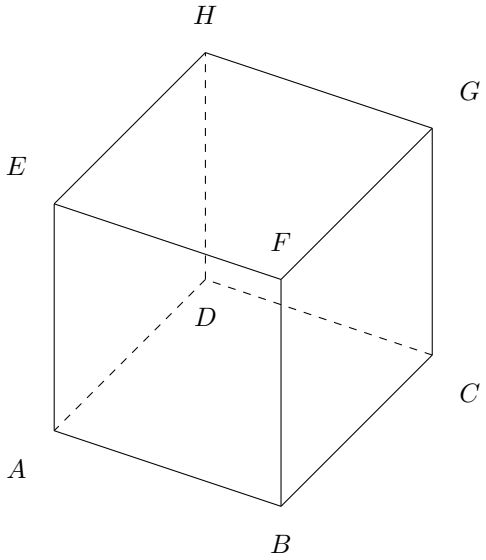
Constructie van het homomorfisme $\Phi\colon \mathcal{K} \to S_4$

Gegeven een rotatie $r \in \mathcal{K}$ van de kubus, willen we een permutatie $\Phi(r)$ construeren van $X = \{1, 2, 3, 4\}$. In plaats van 1, 2, 3 en 4, kunnen we ook 4 meetkundige 'dingen' nemen die bij de kubus $ABCD.EFGH$ in Figuur 1.1 horen.

Welke 4 meetkundige dingen in deze kubus worden gepermuteerd door de rotaties van de kubus? We hebben bijvoorbeeld 6 zijvlakken. Het is lastig om in te zien hoe we van die 6 naar 4 kunnen komen. De ribben dan misschien? We hebben er 12. Misschien kunnen we ze in 4 drietallen groeperen en misschien worden die 4 drietallen gepermuteerd door de kubusrotaties?

Opgave 1.3.16. Kunt u de 12 ribben van de kubus opdelen in 4 drietallen P, Q, R, S op zo'n manier dat alle rotaties van de kubus deze 4 drietallen permuteren?

Laten we naar de 8 hoekpunten kijken. Kunnen we die in 4 paren verdelen zodat die 4 paren worden gepermuteerd door de rotaties van de groep? Ja,



Figuur 1.1: De kubus

dat kan: neem antipodale paren, dus

$$\alpha := \{A, G\} \qquad \beta := \{B, H\} \qquad \gamma := \{C, E\} \qquad \delta := \{D, F\}.$$

Equivalent:

$$\mathcal{D} := \{\alpha, \beta, \gamma, \delta\}$$

is de verzameling van (ongeoriënteerde) diagonalen van de kubus.

Opgave 1.3.17. Neem de spiegeling

$$\sigma = (AB)(CD)(EF)(GH)$$

van de kubus. Laat zien dat deze spiegeling de diagonalen α en β verwisselt en de diagonalen γ en δ.

Definitie 1.3.18. We definiëren een afbeelding $\Phi\colon \mathcal{K} \to S(\mathcal{D})$ als volgt: als $r \in \mathcal{K}$, dan is $\Phi(r)$ de bijbehorende permutatie van de 4 diagonalen van de kubus, dus $\Phi(r)$ beeldt de diagonaal α af op $r(\alpha)$, enzovoorts.

Opgave 1.3.19. Laat zien dat Φ een groepshomomorfisme is.

Bewijs dat $\Phi\colon \mathcal{K} \to S(\mathcal{D})$ een isomorfisme is

We hebben nu een groepshomomorfisme $\Phi\colon \mathcal{K} \to S(\mathcal{D})$. Om te bewijzen dat Φ een isomorfisme is, hoeven we alleen nog maar te bewijzen dat Φ bijectief is. Omdat we weten dat

$$|\mathcal{K}| = 24$$

en

$$|S(\mathcal{D})| = 4! = 24,$$

is het voldoende om ofwel surjectiviteit ofwel injectiviteit[5] van Φ te bewijzen. In de geest van Pólya zullen we beide doen.

Lemma 1.3.20. *Een groepshomomorfisme $F\colon G \to G'$ is precies dan injectief als de* kern van F*, dat wil zeggen de verzameling*

$$\mathrm{Ker}(F) := \{g \in G \mid F(g) = e'\},$$

gelijk is aan $\{e\}$. (Hierbij is e het neutrale element van G en e' het neutrale element van G'.

Bewijs. Voor ieder homomorfisme $F\colon G \to G'$ geldt $F(e) = e'$, dus $e \in \mathrm{Ker}(F)$. Als F injectief is, is er voor iedere $g' \in G'$ hoogstens één $g \in G$ met $F(g) = g'$, dus als F injectief is, dan geldt $\mathrm{Ker}(F) = \{e\}$.
Omgekeerd, als F niet injectief is, dan zijn er $g_1, g_2 \in G$ met $g_1 \neq g_2$ en met $F(g_1) = F(g_2)$. Uit $g_1 \neq g_2$ volgt dat $g := g_1 g_2^{-1} \neq e$. Verder geldt:

$$F(g) = F(g_1 g_2^{-1}) = F(g_1)F(g_2^{-1}) = F(g_1)\left(F(g_2)\right)^{-1},$$

dus uit $F(g_1) = F(g_2)$ volgt dat $F(g) = e'$. Daarmee is $g \in G$ een element in $\mathrm{Ker}(F)$ ongelijk aan e. □

Opgave 1.3.21. Bewijs dat $\mathrm{Ker}(F)$ een ondergroep is van G voor ieder groepshomomorfisme $F\colon G \to G'$.

Definitie 1.3.22. Een ondergroep H van G heet een *normale ondergroep* of een *normaaldeler* van G als voor iedere $h \in H$ en voor iedere $g \in G$ het (geconjungeerde) element ghg^{-1} ook in H ligt.

Opgave 1.3.23. Laat $F\colon G \to G'$ een groepshomomorfisme zijn. Laat zien dat $\mathrm{Ker}(F)$ een normale ondergroep van G is. (Hint: Je moet dus laten zien dat als $g, h \in G$ met $F(h) = e'$, dan ook $F(ghg^{-1}) = e'$.)

[5] Een afbeelding $f\colon X \to Y$ heet *surjectief* als er voor iedere $y \in Y$ een $x \in X$ bestaat met $f(x) = y$. De afbeelding $f\colon X \to Y$ heeft *injectief* als $f(x_1) \neq f(x_2)$ voor alle $x_1, x_2 \in X$ met $x_1 \neq x_2$.

Terug naar ons streven om te bewijzen dat ons groepshomomorfisme Φ van $\mathcal{K}$ naar $S(\mathcal{D})$ injectief is. Volgens het lemma hierboven is het voldoende om te bewijzen dat $\mathrm{Ker}(\Phi)$ geen andere elementen dan e bevat.

Eerder hebben we gezien dat er behalve e precies vier typen rotaties van de kubus bestaan. Neem bijvoorbeeld de rotatie

$$r = (ABCD)(EFGH)$$

van type 'v' over 90°. Deze stuurt de diagonaal $\alpha = AG$ naar de diagonaal $\beta = BH$. Daarmee zien we al dat de permutatie $\Phi(r)$ van $\mathcal{D} = \{\alpha, \beta, \gamma, \delta\}$ niet de triviale permutatie e' is. (In feite geldt natuurlijk $\Phi(r) = (\alpha\beta\gamma\delta)$.) We concluderen dat r *niet* in $\mathrm{Ker}(\Phi)$ ligt. Deze berekening laat uiteraard zien dat geen enkele van de rotaties van type 'v' over $\pm 90°$ in $\mathrm{Ker}(\Phi)$ ligt, want al deze rotaties zijn 'gelijkwaardig'. (In preciezere groepentheoretische taal: al die rotaties zijn geconjungeerd in $\mathcal{K}$.) De rotatie

$$r^2 = (AC)(BD)(EG)(FH)$$

verwisselt de diagonalen $\alpha = AG$ en $\gamma = CE$ en de diagonalen $\beta = BH$ en $\delta = DF$, dus $\Phi(r^2) = (\alpha\gamma)(\beta\delta)$. Dus ook r^2 ligt *niet* in $\mathrm{Ker}(\Phi)$. Uiteraard laat dit ook zien dat geen enkele van de rotaties van type 'v' over $\pm 180°$ in $\mathrm{Ker}(\Phi)$ ligt.

Opgave 1.3.24. Verifieer dat geen enkele rotatie van type 'r' of type 'h' in $\mathrm{Ker}(\Phi)$ ligt.

Hiermee is bewezen dat $\mathrm{Ker}(\Phi)$ alleen uit e bestaat! Daarmee hebben we dus de injectiviteit bewezen. Vanwege $|\mathcal{K}| = 24 = |S(\mathcal{D})|$ hebben we daarmee bewezen dat het groepshomomorfisme $\Phi\colon \mathcal{K} \to S(\mathcal{D})$ bijectief is en dus een *isomorfisme* tussen de groepen $\mathcal{K}$ en $S(\mathcal{D})$.

Gevolg 1.3.25. *Het groepshomomorfisme $\Phi\colon \mathcal{K} \to S(\mathcal{D})$ is een isomorfisme.*

Zoals beloofd bewijzen we dit resultaat ook door juist de surjectiviteit van Φ te bewijzen.

Definitie 1.3.26. Het *beeld* van een groepshomomorfisme $F\colon G \to G'$ is gedefinieerd als

$$F(G) = \{g' \in G \mid \text{er is een } g \in G \text{ met } F(g) = g'\}.$$

Surjectiviteit van Φ is dus equivalent met $\Phi(G) = G'$.

Opgave 1.3.27. Het beeld $F(G)$ van een groepshomomorfisme $F\colon G \to G'$ is een ondergroep van G'.

Neem de ribben AB en GH van de kubus en noem hun middens P en Q. De rotatie r_1 om PQ over 180° doet het volgende met de hoekpunten:

$$r_1 = (AB)(CE)(DF)(GH).$$

Er geldt dus

$$\Phi(r_1) = (\alpha\beta)(\gamma)(\delta) = (\alpha\beta).$$

Analoog kunnen we een rotatie r_2 vinden met $\Phi(r_2) = (\beta\gamma)$ en een rotatie r_3 met $\Phi(r_3) = (\gamma\delta)$.
Het beeld $\Phi(\mathcal{K})$ is dus een ondergroep van $S(\mathcal{D})$ die de permutaties $(\alpha\beta)$, $(\beta\gamma)$ en $(\gamma\delta)$ bevat. We zullen zien dat deze feiten al impliceren dat $\Phi(\mathcal{K}) = S(\mathcal{D})$, dus dat Φ surjectief is. Omdat $\Phi(\mathcal{K})$ een ondergroep is van $S(\mathcal{D})$ en omdat $(\alpha\beta)$ en $(\beta\gamma)$ in $\Phi(\mathcal{K})$ liggen, ligt ook

$$(\alpha\beta)(\beta\gamma) = (\alpha\beta\gamma)$$

in $\Phi(\mathcal{K})$.

Opgave 1.3.28. Gebruik dit idee om te laten zien dat ook $(\alpha\gamma\beta)$, $(\beta\gamma\delta)$ en $(\alpha\beta\gamma\delta)$ in $\Phi(\mathcal{K})$ liggen.

Definitie 1.3.29. De elementen $g_1, \ldots, g_N$ van een groep G *brengen de groep G voort* als de kleinste ondergroep van G die $g_1, \ldots, g_N$ bevat gelijk is aan G zelf. Equivalent: $g_1, \ldots, g_N$ brengen G voort als ieder element g in G te schrijven is als een eindige uitdrukking

$$g = w_1 w_2 \cdots w_M$$

met $w_1 = g_1^{a_1} \cdots g_N^{a_N}$, $w_2 = g_1^{b_2} \cdots g_N^{b_N}$, enzovoorts, met a_1, …, a_N, b_1, …, b_N, … gehele getallen (positief, nul of negatief).

Opgave 1.3.30. Waarom zijn de twee voorwaarden in de bovenstaande definitie equivalent?

Stelling 1.3.31. *De groep $S(\mathcal{D})$ wordt voortgebracht door $(\alpha\beta)$, $(\beta\gamma)$ en $(\gamma\delta)$.*

Bewijs. Algemener wordt de permutatiegroep S_N voortgebracht door (12), (23), …, $(n-1, n)$. We geven hier de bewijsideeën, maar we schrijven het bewijs niet formeel op, omdat dat dit deze eenvoudige ideeën zou laten verdrinken in een zee van notaties. We beginnen met op te merken dat

$$(23)(12)(23) = (13).$$

Net zo geldt

$$(34)(13)(34) = (14).$$

Met dit idee zie je gemakkelijk dat alle 2-cykels (ij) worden voortgebracht door de speciale 2-cykels $(12), (23), \ldots, (n-1, n)$.
Het tweede bewijsidee betreft de observatie

$$(12)(23) = (123).$$

Algemener geldt

$$(ij)(jk) = (ijk)$$

als i, j, k drie verschillende elementen van $\{1, \ldots, N\}$ zijn. Alle 3-cykels worden dus voortgebracht door de 2-cykels, die op hun beurt werden voortgebracht door de speciale 2-cykels $(12), (23), \ldots, (n-1, n)$. Analoog geldt

$$(ij)(jk)(k\ell) = (ijk\ell)$$

als i, j, k, ℓ vier verschillende elementen van $\{1, \ldots, N\}$ zijn. Dus alle 4-cykels worden dus voortgebracht door de 2-cykels, die op hun beurt werden voortgebracht door de speciale 2-cykels $(12), (23), \ldots, (n-1, n)$. Dit patroon zet zich door naar 5-cykels, 6-cykels, enzovoorts. We concluderen dat dus alle cykels worden voortgebracht door de 2-cykels, die op hun beurt werden voortgebracht door de speciale 2-cykels $(12), (23), \ldots, (n-1, n)$.
Nu zijn er elementen in S_N die geen cykel zijn, bijvoorbeeld $(12)(34)$ als $N \geq 4$ of $(124)(35)$ als $N \geq 5$. Maar alle elementen van S_N zijn wel producten (composities) van cykels en omdat al die cykels worden voortgebracht door de speciale 2-cykels $(12), (23), \ldots, (n-1, n)$, geldt zelfs dat de hele groep S_N wordt voortgebracht door deze speciale 2-cykels. □

Stelling 1.3.32. *Het groepshomomorfisme $\Phi\colon \mathcal{K} \to S(\mathcal{D})$ is surjectief (en daarmee een isomorfisme).*

Bewijs. We weten dat $\Phi(\mathcal{K})$ een ondergroep van $S(\mathcal{D})$ is die de speciale 2-cykels $(\alpha\beta)$, $(\beta\gamma)$ en $(\gamma\delta)$ bevat. Maar die 3 elementen brengen al de hele groep $S(\mathcal{D})$ voort, dus $\Phi(\mathcal{K}) = S(\mathcal{D})$. □

1.3.5 De hele groepsactie van S_4 op de kubus

In de tabel hieronder vindt u alle 24 rotaties van de kubus $ABCD.EFGH$. Na een kolom met hun meetkundige type en een kolom met hun orde volgen 8 kolommen met hun werking op de 8 hoekpunten $A, \ldots, H$ van de kubus. Daarna geven we in cykelnotatie de werking op de 4 (ongerichte) diagonalen $\alpha = \{A, G\}$, $\beta = \{B, H\}$, $\gamma = \{C, E\}$ en $\delta = \{D, F\}$. In de meest rechtse kolom geven we de actie op de 6 zijvlakken $p = \{A, B, C, D\}$,

$q = \{E, F, G, H\}$, $r = \{A, D, E, H\}$, $s = \{B, C, G, F\}$, $t = \{A, B, F, E\}$ en $u = \{C, D, H, G\}$.

De eerste 4 regels geven de ondergroep $\{e, (\alpha\beta)(\gamma\delta), (\alpha\gamma)(\beta\delta), (\alpha\delta)(\beta\gamma)\}$ van orde 4 die we met V_4 aanduiden, en de eerste 12 regels geven de ondergroep A_4 van orde 12.

type	orde	A	B	C	D	E	F	G	H	diagonalen	zijvlakken
e	1	A	B	C	D	E	F	G	H	()	()
v	2	C	D	A	B	G	H	E	F	$(\alpha\gamma)(\beta\delta)$	$(rs)(tu)$
		F	E	H	G	B	A	D	C	$(\alpha\delta)(\beta\gamma)$	$(pq)(rs)$
		H	G	F	E	D	C	B	A	$(\alpha\beta)(\gamma\delta)$	$(pq)(tu)$
h	3	A	E	F	B	D	H	G	C	$(\beta\gamma\delta)$	$(ptr)(qus)$
		A	D	H	E	B	C	G	F	$(\beta\delta\gamma)$	$(prt)(qsu)$
		C	B	F	G	D	A	E	H	$(\alpha\gamma\delta)$	$(pst)(qru)$
		F	B	A	E	G	C	D	H	$(\alpha\delta\gamma)$	$(pts)(qur)$
		H	D	C	G	E	A	B	F	$(\alpha\beta\delta)$	$(pus)(qtr)$
		F	G	C	B	E	H	D	A	$(\alpha\delta\beta)$	$(psu)(qrt)$
		C	G	H	D	B	F	E	A	$(\alpha\gamma\beta)$	$(pur)(qts)$
		H	E	A	D	G	F	B	C	$(\alpha\beta\gamma)$	$(pru)(qst)$
r	2	B	A	E	F	C	D	H	G	$(\alpha\beta)$	$(pt)(qu)(rs)$
		E	H	G	F	A	D	C	B	$(\alpha\gamma)$	$(pq)(rt)(su)$
		D	H	E	A	C	G	F	B	$(\alpha\delta)$	$(pr)(qs)(tu)$
		G	C	B	F	H	D	A	E	$(\beta\gamma)$	$(ps)(qr)(tu)$
		G	F	E	H	C	B	A	D	$(\beta\delta)$	$(pq)(ru)(st)$
		G	H	D	C	F	E	A	B	$(\gamma\delta)$	$(pu)(qt)(rs)$
v	4	B	C	D	A	F	G	H	E	$(\alpha\beta\gamma\delta)$	$(rtsu)$
		D	A	B	C	H	E	F	G	$(\alpha\delta\gamma\beta)$	$(rust)$
		B	F	G	C	A	E	H	D	$(\alpha\beta\delta\gamma)$	$(psqr)$
		E	A	D	H	F	B	C	G	$(\alpha\gamma\delta\beta)$	$(prqs)$
		D	C	G	H	A	B	F	E	$(\alpha\delta\beta\gamma)$	$(puqt)$
		E	F	B	A	H	G	C	D	$(\alpha\gamma\beta\delta)$	$(ptqu)$

Opgave 1.3.33. We kunnen de 8 hoekpunten $A, \ldots, H$ opdelen in twee disjuncte *blokken*: $\{A, C, F, H\}$ en $\{B, D, E, G\}$. Laten we zeggen dat de hoekpunten A, C, F, H uit het eerste blok zwart zijn en dat de hoekpunten B, D, E, G uit het tweede blok wit zijn. Als f een willekeurige rotatie is van de kubus $ABCD.EFGH$ en f beeldt A op een zwart hoekpunt af, dan beeldt f *alle* zwarte hoekpunten op zwarte hoekpunten af. Als f het punt A op een wit hoekpunt afbeeldt, dan beeldt f *alle* zwarte hoekpunten op witte hoekpunten af. Overtuig uzelf van de waarheid van deze twee uitspraken door naar de kubus te kijken en door naar de bovenstaande

tabel te kijken.

Opgave 1.3.34. Hoe kunnen we de 8 hoekpunten opdelen in 4 blokken van ieder 2 punten, d.w.z. de 8 hoekpunten kleuren met 4 kleuren, zodat de analoge eigenschap geldt?

Opgave 1.3.35. Wat is de stabilisatorondergroep H_A van het punt A, d.w.z. de groep $H = \{g \in \mathcal{K} \cong S_4 \mid g(A) = A\}$? Bepaal voor beide bloksystemen de stabilisator van het blok dat A bevat. Hoe verhoudt deze zich tot de stabilisatorgroep H_A van punt A?

Opgave 1.3.36. De 6 vlakken p, q, r, s, t, u van de kubus kunnen we in de 3 blokken $\{p, q\}$ ('blauw'), $\{r, s\}$ ('geel') en $\{t, u\}$ ('rood') opdelen, zodat de blokeigenschap geldt. (Als een rotatie één blauw zijvlak op een geel zijvlak afbeeldt, dan beeldt die rotatie ook het andere blauwe zijvlak op een geel zijvlak af, etcetera.) Bepaal de stabilisatorondergroep $H_p = \{\rho \in \mathcal{K} \mid \rho(p) = p\}$ van het zijvlak p en de stabilisatorondergroep $H_{\{p,q\}}$ van het blauwe blok $\{p, q\}$. Hoe groot zijn deze groepen? (Antwoorden: $H_p = \langle(\alpha\beta\gamma\delta)\rangle = \langle(rtsu)\rangle$ heeft orde 4 en $H_{\{p,q\}} = \langle(\alpha\beta\gamma\delta), (\alpha\beta)(\gamma\delta)\rangle = \langle(rtsu), (pq)(rs)\rangle$ heeft orde 8. Helemaal uitgeschreven:

$$\begin{aligned} H_p &= \{e, (\alpha\beta\gamma\delta), (\alpha\gamma)(\beta\delta), (\alpha\delta\gamma\beta)\} \\ &= \{e, (rtsu), (rs)(tu), (rust)\} \end{aligned}$$

en

$$\begin{aligned} H_{\{p,q\}} &= \{e, (\alpha\beta\gamma\delta), (\alpha\gamma)(\beta\delta), (\alpha\delta\gamma\beta), (\alpha\beta)(\gamma\delta), (\beta\delta), (\alpha\delta)(\beta\gamma), (\alpha\gamma)\} \\ &= \{e, (rtsu), (rs)(tu), (rust), \\ &\qquad (pq)(rs), (pq)(rt)(su), (pq)(tu), (pq)(ru)(st)\}. \end{aligned}$$

Opgave 1.3.37. Neem een vierkant en noem de hoekpunten (tegen de klok in) R, T, S en U. De symmetriegroep (rotaties en spiegelingen) van dit vierkant is

$$D_8 := \{e, (RTSU), (RS)(TU), (RUST), (RS), (RT)(SU), (TU), (RU)(ST)\}.$$

(Deze groep wordt de *diëdergroep van orde 8* genoemd.) Er is een voor de hand liggende afbeelding $f\colon D_8 \to H_{\{p,q\}}$ van deze groep D_8 naar de groep $H_{\{p,q\}}$ uit de vorige opgave: $f(e) = e$ en

$$f((RTSU)) := (rtsu) \quad f((RS)(TU)) = (rs)(tu) \quad f((RUST)) = (rust)$$

$$\begin{aligned} f((RS)) &= (pq)(rs) \qquad f((RT)(SU)) = (pq)(rt)(su) \\ f((TU)) &= (pq)(tu) \qquad f((RU)(ST)) = (pq)(ru)(st). \end{aligned}$$

Laat zien dat f een groepsisomorfisme is.

Opgave 1.3.38. Neem voor R, T, S, U de middens van de zijden r, t, s, u in de kubus $ABCD.EFGH$. Door naar deze te kijken zou de vorige opgave nu 'evident' moeten zijn. Lukt dat? (Misschien helpt het als u p interpreteert als de onderkant van het vierkant $RTSU$ en q als de bovenkant van dat vierkant.)

1.3.6 De platonische lichamen

An idea that can be used once is a trick. If it can be used more than once, it becomes a method. G. Pólya.

Behalve de kubus bestaan er nog vier platonische lichamen: de tetraëder, de octaëder, de dodecaëder en de icosaëder. (We bekijken alleen regelmatige lichamen.) De octaëder krijgen we uit een kubus door de middens van de zijvlakken van de kubus te nemen als hoekpunten van de octaëder. Omgekeerd krijgen we de kubus uit de octaëder door de middens van de zijvlakken van de octaëder te nemen als hoekpunten van de kubus. Dit proces heet 'dualiseren'. Als we twee keer dualiseren zijn we terug bij af (op een schaalfactor na, maar die is irrelevant voor ons). De kubus en de octaëder zijn dus duaal aan elkaar.

Opgave 1.3.39. Overtuig uzelf dat de icosaëder en dodecaëder duaal zijn aan elkaar, terwijl de tetraëder duaal is aan zichzelf.

Opgave 1.3.40. Overtuig uzelf dat iedere rotatie van een kubus ook een rotatie is van zijn duale octaëder. Omgekeerd is iedere rotatie van die duale octaëder een rotatie van de kubus. Concludeer dat de kubus en zijn duale octaëder dezelfde rotatiegroep hebben.

Opgave 1.3.41. Is de rotatiegroep van de icosaëder gelijk aan de rotatiegroep van zijn duale dodecaëder?

Definitie 1.3.42. De alternerende groep A_n is de groep van even permutaties in S_n. De orde van A_n is $\frac{1}{2}n!$.

De volgende opgaven zijn eigenlijk onderzoeksprojectjes: pas de ideeën die wij hebben gebruikt om de rotatiegroep van de kubus te begrijpen toe om de rotatiegroep van de tetraëder en van de icosaëder te begrijpen.

Opgave 1.3.43. Onderzoek de rotatiegroep $\mathcal{T}$ van de regelmatige tetraëder $ABCD$. Laat zien dat $\mathcal{T}$ orde 12 heeft. Hoeveel elementen van $\mathcal{T}$ hebben orde 2, 3, 4, ... Laat zien dat $\mathcal{T} \cong A_4$. (Hint: Associeer 4 meetkundige objecten met een tetraëder die door de groep $\mathcal{T}$ worden gepermuteerd. Tel de rotaties van de tetraëder en verifieer dat de 12 rotaties van de tetraëder bijectief corresponderen met de 12 even permutaties van de

vier meetkundige objecten.)

De volgende opgave is de analoge opgave voor de icosaëder. Er zijn niet echt nieuwe ideeën nodig, maar omdat de rotatiegroep van de icosaëder wat groter is (de orde is 60) neemt het werk wat toe. Als we meer wisten over de groep A_5 (zoals diens simpelheid, waarover later meer), dan konden we met wat meer theorie het werk weer inperken.

Opgave 1.3.44. Onderzoek de rotatiegroep $\mathcal{I}$ van de regelmatige icosaëder of (equivalent) van de regelmatige dodecaëder. Laat zien dat $\mathcal{I}$ orde 60 heeft. Hoeveel elementen heeft $\mathcal{I}$ van orde 2, 3, 4, 5, 6, ...? Laat zien dat $\mathcal{I} \cong A_5$. (Hint 1: associeer 5 meetkundige objecten met een icosaëder (of een dodecaëder) die door de groep $\mathcal{I}$ worden gepermuteerd. Tel de rotaties van de icosaëder (of van de dodecaëder) en verifieer dat de 60 rotaties bijectief corresponderen met de 60 even permutaties van de vijf meetkundige objecten. Hint 2: U kunt de 30 ribben van een icosaëder of dodecaëder groeperen in 5 sextetten, die door de rotaties worden gepermuteerd. Als alternatief kunt u de 5 kubussen nemen die ingeschreven zijn in een gegeven dodecaëder. Hint 3: De groep A_5 wordt voortgebracht door $(1, 2, 3)$, $(1, 2, 4)$ en $(1, 2, 5)$, dus het is voldoende om die 3 permutaties van de 5 objecten te realiseren door een rotatie van de icosaëder.

1.4 De classificatie van 'symmetrieatomen'

That which is not measurable is not science. That which is not physics is stamp collecting. E. Rutherford

1.4.1 'Ontbinden' van groepen

Veel eigenschappen van natuurlijke getallen kunnen we beschrijven door ze te ontbinden in priemgetallen. Het blijkt dat je groepen ook kunt 'ontbinden' in 'priemgroepen'. Dit ontbinden van een groep in kleinere 'factorgroepen' en het weer samenvoegen van die kleinere groepen tot een grotere groep is nogal subtiel. Vandaar dat ik in het stukje hieronder nogal eens aanhalingstekens moet gebruiken om de lezer te waarschuwen dat op zo'n plek de nodige groepentheoretische techniek onder het tapijt is geschoven.

De rotatiegroep

$$G_2 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

kun je begrijpen als een soort 'product' van de groepen $\{e, r, r^2, r^3\}$ en $\{e, s\}$.

De rotatiegroep heeft orde 8 en de 'factorgroepen' hebben orde 4 en 2. Als je een groep G 'ontbindt' in 'factorgroepen' G_1 en G_2, heb je altijd $|G| = |G_1| \cdot |G_2|$.
De groep S_4 van permutaties van 4 objecten kun je begrijpen als 'product' van de ondergroep A_4 van even permutaties en de groep $\{e, (1,2)\}$. De groep A_4 van orde 12 zelf kun je weer verder 'opdelen' in de groepen

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$$

van orde 4 en

$$C_3 = \{e, (1,2,3), (1,3,2)\}$$

van orde 3. De groep V_4 kun je zien als product van de groepjes $\{e, (12)(34)\}$ en $\{e, (13)(24)\}$ van orde 2. Essentieel bij deze 'factorisatie' van de groep S_4 is dat in de keten

$$S_4 > A_4 > V_4 > \{e, (12)(34)\} > \{e\}$$

de ondergroepen *normaal* zijn: $\{e, (12)(34)\}$ is normaal in V_4, V_4 is normaal in A_4 en A_4 is normaal in S_4. (Ter herinnering: een ondergroep H van G is normaal in G als H de vereniging van conjungatieklassen van G is.) De 'stapgrootten' $24/12 = 2$, $12/4 = 3$, $4/2 = 2$ en $2/1 = 2$ kunnen niet nog kleiner worden gemaakt, omdat 2, 3, 2 en 2 priemgetallen zijn. We kunnen deze keten dan ook zien als een soort 'priemfactorisatie' van de groep S_4.

1.4.2 Waarom bestaat er geen *abcdef*-formule?

Évariste Galois (1811–1832) ontdekte als tiener dat de *abcd*-formule voor de vergelijking

$$ax^3 + bx^2 + cx + d = 0$$

correpondeert met de keten $S_3 > A_3$ voor de groep S_3, terwijl de *abcde*-formule voor de vergelijking

$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

correspondeert met de keten $S_4 > A_4 > V_4$ voor de groep S_4. Hij begreep ook dat *als* er *abcdef*-formule zou bestaan voor de vergelijking

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0,$$

dat er dan een vergelijkbare keten moest bestaan $S_5 > A_5 > \cdots$. De keten onder A_5 zou de vorm

$$A_5 > N_1 > N_2 > \cdots > \{e\}$$

waarbij we in iedere stap een normale ondergroep nemen en waarbij iedere 'stapgrootte' een priemgetal is.

Vervolgens bewees Galois dat zo'n keten niet bestaat en daarmee bewees hij dus dat er geen *abcdef*-wortelformule bestaat voor de algemene vergelijking van graad 5 (of hoger)!

Stelling 1.4.1 (Galois)**.** *Als $n \geq 5$ dan zijn $\{e\}$ en A_n de enige normale ondergroepen van A_n.*

1.4.3 Symmetrieatomen

Een groep G zoals A_n voor $n \geq 5$ die geen normale ondergroepen N heeft anders dan de twee triviale gevallen $N = \{e\}$ en $N = G$ heet een *simpele groep*. Het woord 'simpel' betekent hier *niet* 'eenvoudig'maar '*enkelvoudig*', in de zin van 'niet verder te ontbinden'. Deze groepen worden daarom ook wel *enkelvoudige groepen* genoemd. Simpele groepen spelen dus in de groepentheorie een rol analoog aan die van de priemgetallen in de getaltheorie.

Mark Ronan gebruikt in zijn boek *Symmetry and the Monster* de mooie naam 'symmetrieatomen' voor simpele groepen. Een eindige groep is dan een soort 'symmetriemolecuul' en zo'n 'symmetriemolecuul' wordt opgebouwd uit 'symmetrieatomen', die 'ondeelbaar' zijn. Galois heeft bewezen dat

$$A_5, A_6, A_7, \ldots$$

allemaal symmetrieatomen zijn.

Opgave 1.4.2. Laat zien dat de groep $\mathbf{Z}/n\mathbf{Z}$ (met $n > 1$) precies dan simpel is als n een priemgetal is.

Het eerste symmetrieatoom dat niet van de vorm $\mathbf{Z}/p\mathbf{Z}$ of van de vorm A_n is, heeft orde $168 = 7 \times 24$. (Dit getal kun je gemakkelijk onthouden: het is precies het aantal uren in een week!) Dit is de symmetriegroep van het Fano-vlak. Het Fano-vlak bestaat uit de 7 punten $A = (1,0,0)$, $B = (0,1,0)$, $C = (0,0,1)$, $D = (0,1,1)$, $E = (1,0,1)$, $F = (1,1,0)$ en $G = (1,1,1)$. De 7 lijnen van het Fano-vlak zijn $\{A,B,F\}$, $\{A,C,E\}$, $\{B,C,D\}$, $\{A,D,G\}$, $\{B,E,G\}$, $\{C,F,G\}$ en $\{D,E,F\}$. Een symmetrie is een permutatie van de 7 punten die lijnen op lijnen afbeeldt. De symmetriegroep van het Fano-vlak is dus een ondergroep van de permuatiegroep S_7. De elementen van deze symmetriegroep zijn matrices

$$g = \begin{pmatrix} g_{1,1} & g_{1,2} & g_{1,3} \\ g_{2,1} & g_{2,2} & g_{2,3} \\ g_{3,1} & g_{3,2} & g_{3,3} \end{pmatrix},$$

waarbij $g_{i,j} \in \{0,1\}$, waarbij we rekenen modulo 2 en waarbij $\det(g) \neq 0$. De groepsbewerking is matrixvermenigvuldiging. Merk op dat er $2^3 - 1 = 7$ mogelijkheden zijn voor de eerste kolom. Gegeven die eerste kolom zijn er $2^3 - 2 = 6$ mogelijkheden voor de tweede kolom. Gegeven de eerste en tweede kolom zijn er $2^3 - 2^2 = 4$ mogelijkheden voor de derde kolom. Zo kom je op de orde $|G| = 7 \cdot 6 \cdot 4 = 7 \times 24 = 168$.

1.4.4 Classificatie van alle symmetrieatomen

Alle symmetrieatomen zijn bekend! Hoogstwaarschijnlijk. In 2004 werd het laatste onderdeel gepubliceerd van de volledige classificatie van alle eindige symmetrieatomen! Het totale bewijs beslaat duizenden bladzijden verdeeld over honderden artikelen en is het werk van ongeveer 100 wiskundigen. De kans bestaat dus dat er her en der foutjes en gaatjes en misschien zelfs fouten en gaten zitten in de bewijzen. Toch vertrouwen de experts erop dat ze alle eindige symmetrieatomen hebben gevonden. Sommige onderdelen van het bewijs zijn met computers geverifieerd.

Het resultaat van dit mammoetwerk is de volledige classificatie van alle eindige symmetrieatomen. In deze zin kunnen we zeggen dat we alle mogelijke eindige symmetrieën kennen, van welk soort objecten dan ook, in welke dimensie dan ook, hoe abstract ook, nu al bekend of nog onbekend! (De eerlijkheid gebiedt me te zeggen dat het samenstellen van symmetrieatomen tot symmetriemoleculen niet zo eenvoudig is als het vermenigvuldigen van priemgetallen.)

Er blijken een paar reeksen van symmetrieatomen te bestaan, zoals de groepen $\mathbf{Z}/p\mathbf{Z}$ en de groepen A_n voor $n \geq 5$ van Galois. Ook de matrixgroep van orde 168 past in een grote familie van symmetrieatomen (zekere matrixgroepen). Naast die families zijn er nog precies 26 (of 27, afhankelijk van je definities) buitenbeentjes die niet in de families passen. Deze symmetrieatomen worden de *sporadische eindige simpele groepen* genoemd.

De kleinste simpele eindige groep is gevonden in 1861 door de Franse wiskundige Émile Mathieu. Deze groep heeft orde $2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7\,920$. Het grootste sporadische symmetrieatoom is in 1980 geconstrueerd door de Duitser Bernd Fischer en de Amerikaan Robert Griess. Deze groep wordt de *monstergroep* of *the friendly giant* genoemd. De orde van deze groep is

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Uitgeschreven is dit

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000$$

zeg maar een 8 met 53 nullen. Dit is groter dan het aantal protonen of neutronen in de aarde!

De kleinste dimensie waarin deze groep zich manifesteert is 196 883. Via het fenomeen van *monstrous moonshine* is er een diep verband tussen het monster, die manifestatie in 196 883 dimensies en de j-functie

$$j(q) = \frac{1}{q} + 744 + 196\,884q + 21\,493\,760q^2 + 864\,299\,970q^3 + \cdots$$

uit de theorie van modulaire vormen en elliptische krommen. Dit is bewezen door de Brit Richard Borcherds, die hiervoor in 1992 de Fieldsmedaille kreeg. Hij gebruikte hierbij ideeën uit de snaartheorie. (Snaartheorie is nogal omstreden in de natuurkunde, maar de theorie heeft heel veel moois te weeg gebracht in de wiskunde!) De j-functie is trouwens al in de 19e eeuw ontdekt, weer een prachtig voorbeeld van de eeuwigheidswaarde van goede wiskunde.

1.5 Symmetrieën van $\mathbf{R}^2$ en $\mathbf{R}^3$

The biggest conceptual change [in physics] over the last 100 years is the way physicists think about the world is symmetry. L.M. Krauss

We bekijken de symmetrieën van het euclidische vlak en van de euclidische ruimte, d.w.z. de afstandsbehoudende afbeeldingen

$$f\colon \mathbf{R}^n \to \mathbf{R}^n$$

voor $n = 2$ en $n = 3$.

Opgave 1.5.1. Laat zien dat afstandsbehoudende afbeeldingen $f\colon \mathbf{R}^n \to \mathbf{R}^n$ (a) bijectief zijn en (b) een groep vormen.

We noemen die groep $\mathcal{E}_n$. De letter '$\mathcal{E}$' staat voor 'euclidisch'.

1.5.1 Symmetrieën van het euclidische vlak

De volgende afbeeldingen behouden afstand in het euclidische vlak:

1. rotaties $R_\theta\colon (x, y) \mapsto (\cos(\theta)x - \sin(\theta)y, \sin(\theta)x + \cos(\theta)y)$ rond de oorsprong voor een vaste hoek θ;
2. translaties $T_{(a,b)}\colon (x, y) \mapsto (x + a, y + b)$ voor vaste $(a, b) \in \mathbf{R}^2$;
3. de lijnspiegeling $S\colon (x, y) \mapsto (x, -y)$ in de lijn $y = 0$.

We kunnen deze afbeeldingen samenstellen. Als we twee rotaties rond de oorsprong combineren, krijgen we opnieuw een rotatie rond de oorsprong. Deze rotaties vormen dus een ondergroep $\mathcal{R}_2$ van de groep $\mathcal{E}_2$ van alle afstandsbehoudende afbeeldingen $\mathbf{R}^2 \to \mathbf{R}^2$. Analoog vormen de translaties een ondergroep $\mathcal{T}_2$ van de groep $\mathcal{E}_2$.

Interessanter wordt het als we rotaties en translaties combineren. Als we eerst roteren over θ en dan transleren over (a, b), dan krijgen we

$$T_{a,b} \circ R_\theta \colon (x, y) \mapsto (a + \cos(\theta)x - \sin(\theta)y, b + \sin(\theta)x + \cos(\theta)y).$$

Laten we deze afbeelding noteren als $F_{a,b;\theta}$.

Opgave 1.5.2. Verifieer de volgende beweringen:

1. $F_{0,0;\theta} = R_\theta$;
2. $F_{a,b;0} = T_{a,b}$;
3. $R_\theta^{-1} = R_{-\theta}$;
4. $T_{a,b}^{-1} = T_{-a,-b}$.

Voor de volgende opgave is het prettig om $F_{a,b;\theta}$ in vectorvorm te schrijven als

$$F_{a,b;\theta}(\mathbf{x}) = \mathbf{t} + R_\theta(\mathbf{x}),$$

where $\mathbf{x} = (x, y)$ en $\mathbf{t} = (a, b)$. (Als je wilt, kun je deze vectoren ook verticaal schrijven en bij R_θ denken aan de 2×2-matrix $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.)

Opgave 1.5.3. Verifieer de volgende beweringen:

1. $F_{c,d;\phi} \circ F_{a,b;\theta} = F_{u,v;\phi+\theta}$, waarbij $(u, v) = (c, d) + R_\phi(a, b)$, dus $(u, v) = (c + \cos(\phi)a - \sin(\phi)b, d + \sin(\phi)a + \cos(\phi)b)$;
2. $F_{a,b;\theta}^{-1} = F_{c,d;-\theta}$ waarbij $(c, d) = -R_{-\phi}(a, b)$, dus $(c, d) = (-\cos(\theta)a - \sin(\theta)b, \sin(\theta)a - \cos(\theta)b)$.

We zien dat

$$\mathcal{E}_2^+ = \{F_{a,b;\theta} \mid a, b, \theta \in \mathbf{R}\}$$

een groep is. Het plusje betekent 'oriëntatiebehoudend'. Translaties en rotaties behouden oriëntatie. Puntspiegelingen in het vlak zijn ook oriëntatiebehoudend. (Puntspiegelingen in het vlak zijn rotaties over 180°.) Lijnspiegelingen in het vlak keren daarentegen de oriëntatie om: de latijnse letter 'R' wordt de cyrillische letter 'Ja'. In dit document doen we geen poging om het begrip 'oriëntatie' precies te definiëren; we vertrouwen hier op onze intuïtie. (U kunt proberen het begrip precies te definiëren, bijvoorbeeld met behulp van determinanten.)

De groep $\mathcal{E}_2^+$ heeft oneindig veel elementen. Er zijn drie continue parameters a, b, θ nodig om een element te beschrijven, dus de groep is 3-

dimensionaal. (Hier vegen we weer het nodige onder het tapijt. Om dit netjes uit te werken, heb je de theorie van continue (Lie)groepen nodig.)

Stelling 1.5.4. *De groep $\mathcal{E}_2^+$ is precies de groep van alle oriëntatie- en afstandbehoudende afbeeldingen $\mathbf{R}^2 \to \mathbf{R}^2$.*

Bewijs. Het is duidelijk dat de elementen van $\mathcal{E}_2^+$ orientatie- en afstandbehoudend zijn. Om te bewijzen dat omgekeerd iedere orientatie- en afstandbehoudende afbeelding $\mathbf{R}^2 \to \mathbf{R}^2$ in $\mathcal{E}_2^+$ zit, moet nog wat werk worden verricht. Zie *The Four Pillars of Geometry* van John Stillwell voor een bewijs. □

Opgave 1.5.5. Bekijk $T_{a,b} \circ R_\theta \circ T_{a,b}^{-1}$. Verifieer dat deze afbeelding een rotatie om (a, b) over de hoek θ is.

Opgave 1.5.6. Is de ondergroep $\mathcal{R}_2$ van rotaties rond $(0, 0)$ een normale ondergroep van $\mathcal{E}_2$?

Opgave 1.5.7. Bekijk $R_\theta \circ T_{a,b} \circ R_\theta^{-1}$. Verifieer dat deze afbeelding een translatie over $R_\theta(a, b)$ is.

Opgave 1.5.8. Is de ondergroep $\mathcal{T}_2$ een normale ondergroep van $\mathcal{E}_2$?

Definieer $G_{a,b;\theta} := F_{a,b;\theta} \circ S = T_{a,b} \circ R_\theta \circ S$, waarbij $S(x, y) = (x, -y)$.

Opgave 1.5.9. Verifieer dat

$$G_{a,b;\theta} \colon (x, y) \mapsto (a + \cos(\theta)x + \sin(\theta)y, b + \sin(\theta)x - \cos(\theta)y)$$

Er zijn precies evenveel $F_{a,b;\theta}$'s als $G_{a,b;\theta}$'s, namelijk ∞^3, precieser: de afbeelding $F \mapsto F \circ S$ is een bijectie is van de verzameling

$$\mathcal{E}_2^+ = \{F_{a,b;\theta} \mid a, b, \theta \in \mathbf{R}\}$$

van orientatiebehoudende, afstandsbewarende afbeeldingen $\mathbf{R}^2 \to \mathbf{R}^2$ naar de verzameling

$$\mathcal{E}_2^- = \{G_{a,b;\theta} \mid a, b, \theta \in \mathbf{R}\}$$

van orientatieomkerende, afstandsbewarende afbeeldingen $\mathbf{R}^2 \to \mathbf{R}^2$. De inverse van deze bijectie is $G \mapsto G \circ S$.

Opgave 1.5.10. Laat zien dat $\mathcal{E}_2^+ \cup \mathcal{E}_2^-$ een groep is met ondergroep $\mathcal{E}_2^+$. Is $\mathcal{E}_2^-$ ook een ondergroep?

Stelling 1.5.11. *De groep $\mathcal{E}_2^+ \cup \mathcal{E}_2^-$ is precies de groep van afstandsbehoudende afbeeldingen $\mathbf{R}^2 \to \mathbf{R}^2$.*

Bewijs. Als $G \colon \mathbf{R}^2 \to \mathbf{R}^2$ een orientatieomkerende afstandsbehoudende afbeelding $\mathbf{R}^2 \to \mathbf{R}^2$ is, dan is $F := G \circ S$ een orientatiebehoudende,

afstandsbehoudende afbeelding $\mathbf{R}^2 \to \mathbf{R}^2$. Volgens de vorige stelling ligt $G \circ S$ dus in $\mathcal{E}_2^+$. Daarom ligt G in $\mathcal{E}_2^-$. □

1.5.2 Symmetrieën van de euclidische ruimte

Analoog aan de vorige paragraaf kunnen we een afstandsbehoudende afbeelding $\mathbf{R}^3 \to \mathbf{R}^3$ schrijven als

$$\text{translatie} \circ \text{rotatie}$$

in het oriëntatiebehoudende geval en als

$$\text{translatie} \circ \text{rotatie} \circ S,$$

met $S(x, y, z) = (x, y, -z)$ in het oriëntatieomkerende geval. In deze paragraaf kijken we alleen naar de rotaties.

Een stelling van Euler

Stelling 1.5.12 (Euler)**.** *Laat $R\colon \mathbf{R}^3 \to \mathbf{R}^3$ een afstand- en oriëntatiebehoudende afbeelding zijn. Neem aan dat er een punt Q is in $\mathbf{R}^3$ met $f(Q) \neq Q$ en een punt O met $R(O) = O$. Dan is*

$$\ell := \{P \in \mathbf{R}^3 \mid R(P) = P\}$$

een rechte lijn door O en R is de rotatie om die lijn over een zekere hoek θ.

Het bewijs is niet moeilijk, maar het gebruikt lineaire algebra, in het bijzonder met de theorie van eigenwaarden. Daarom laten we het hier weg.

Topologie van de groep van rotaties

Om een rotatie R die een vast punt O, zeg $O = (0, 0, 0)$, vasthoudt te beschrijven heb je dus een lijn ℓ door O en een rotatiehoek θ nodig. Neem voor het gemak aan dat de lijn ℓ de z-as is. Dan hebben we de rotatie

$$(x, y, z) \mapsto (\cos(\theta)x - \sin(\theta)y, \sin(\theta)x + \cos(\theta)y, z).$$

We kunnen de informatie 'rotatieas plus rotatiehoek' representeren door de vector $(0, 0, \theta)$: de richting geeft ℓ en de lengte geeft θ. We nemen hierbij θ in het interval $[-\pi, \pi]$. De vectoren $(0, 0, \pi)$ en $(0, 0, -\pi)$ beschrijven nu dezelfde rotatie, maar verder zijn er geen dubbelingen. Uiteraard kunnen we dit met iedere rotatieas doen.

Opgave 1.5.13. Welke rotatie correspondeert met de oorsprong $(0,0,0)$? Welk punt correspondeert met de identiteit $e\colon \mathbf{R}^3 \to \mathbf{R}^3$?

We krijgen nu het volgende topologische recept voor de groep van rotaties van $\mathbf{R}^3$ die $(0,0,0)$ vasthouden:

Stelling 1.5.14. *De groep van rotaties van* $\mathbf{R}^3$ *die* $(0,0,0)$ *vasthouden ontstaat topologisch gezien uit de massieve bol*

$$B = \{(x,y,z) \in \mathbf{R}^3 \mid x^2 + y^2 + z^2 \leq \pi^2\}$$

door het identificeren van antipodale punten (x,y,z) *en* $(-x,-y,-z)$ *op de rand van de bol (dus punten* (x,y,z) *met* $x^2+y^2+z^2=\pi^2$*).*

Als u vertrouwd bent met de projectieve ruimte, dan begrijpt u nu dat de groep van rotaties in $\mathbf{R}^3$ die $(0,0,0)$ vasthouden dus de topologie heeft van de 3-dimensionale reële projectieve ruimte. Dit speelt een rol in de vrijdagavondlezing van David Eelbode.

1.6 Opgaven met of zonder GAP

Never trust a computer you can't throw out of a window. S. Wozniak

De opgaven in dit hoofdstuk kunnen met of zonder GAP worden gemaakt.

1.6.1 De ondergroepen van de groep A_4

De groep A_4 van even permutaties van $\{1,2,3,4\}$ bestaat uit de volgende 12 elementen:

$$e, (12)(34), (13)(24), (14)(23)$$

en

$$(123), (132), (124), (142), (134), (143), (234), (243).$$

De opgave van dit hoofdstuk is:

Opgave 1.6.1.
1. Bepaal alle ondergroepen van A_4.
2. Geef in een diagram (graaf) met al deze ondergroepen de inclusies aan.
3. Welke ondergroepen van A_4 zijn normaal?

U kunt deze opgave beginnen te maken zonder verder te lezen. Als u vast komt te zitten, kunt u naar de hints hieronder kijken. Loopt u dan opnieuw vast, dan kunt u naar de uitgebreide hints kijken. Verder heeft u nog

minstens twee alternatieve aanpakken: werken met de software GAP of het antwoord opzoeken en checken wat u goed had en waar u een idee heeft gemist.

Hints

U kunt de volgende resultaten (bewezen in paragraaf 1.7) gebruiken:

1. De orde van een ondergroep deelt de orde van de groep.
2. Een ondergroep van index 2 is normaal. (De index van een ondergroep H in een eindige groep G is $|G|/|H|$. Zie ook paragraaf 1.8.) Ondergroepen van een hogere index kunnen normaal zijn of niet.
3. Een ondergroep is precies dan normaal als zij de vereniging is van conjungatieklassen.

Uitgebreide hints

Hier zijn twee manieren om ondergroepen van A_4 te maken.

1. We hebben $V_4 = \{e, (12)(13), (13)(24), (14)(23)\}$. (Dit heet de *Vierergruppe* van Felix Klein.) Laat zien dat V_4 een ondergroep is van A_4.
2. Bewijs het volgende: Als $V_4 \leq H \leq A_4$, dus als H een ondergroep is van A_4 die V_4 bevat, dan geldt $H = V_4$ of $H = A_4$.
3. Kies een $i \in \{1, 2, 3, 4\}$ en bekijk alle permutaties $\sigma \in A_4$ die i vasthouden. Voor $i = 4$ krijg je $H = \{e, (1, 2, 3), (1, 3, 2)\}$. Laat zien dat H een ondergroep is van A_4. Dit heet de stabilisatorondergroep van i in A_4.
4. Laat zien dat als $H \leq H' \leq A_4$, dus H' is een ondergroep van A_4 die H bevat, dan $H' = H$ of $H' = A_4$.

GAP

We kunnen de groep A_4 op twee manieren definiëren. We kunnen voortbrengers aangeven:

```
G := Group( (1,2,3), (1,2)*(3,4) );
Size(G);
IdGroup(G);I
```

GAP bevestigt dat $|G| = 12$, dus de twee even permutaties $(1, 2)(3, 4)$ en $(1, 2, 3)$ brengen de hele groep A_4 voort (en niet slechts een kleinere ondergroep). Het commando `IdGroup(G)` geeft als resultaat: `[12,3]`. Dit betekent dat in GAP's lijst van 'kleine groepen' de groep G de derde groep

is van orde 12.

We kunnen ook definiëren:

```
G := AlternatingGroup(4);
Size(G);
IdGroup(G);
```

Opnieuw bevestigt GAP dat $|G| = 12$ en opnieuw is `[12,3]` de 'id' van de groep. Deze groep is dus 'dezelfde' (preciezer: isomorf met) de groep gedefinieerd door de twee voortbrengers $(1, 2, 3)$ en $(1, 2)(3, 4)$.

We kunnen nu GAP vragen om een lijst met alle ondergroepen:

```
lijst := AllSubgroups(G);
Size(lijst);
```

Blijkbaar zijn er 10 ondergroepen. Dus behalve $\{e\}$ en A_4 zelf zijn er nog 8 ondergroepen. We hebben de 4 stabilisatorondergroepen corresponderend met de punten $i = 1, 2, 3, 4$ van $\{1, 2, 3, 4\}$. We hebben de ondergroep V_4. Blijkbaar zijn er nog 3 ondergroepen. Weet u welke? (Hint: Het zijn ondergroepen van V_4.)

```
H := lijst[1];
Size(H);
H := lijst[10];
Size(H);
```

We vinden de 'triviale' ondergroepen: $\{e\}$ en A_4 zelf.

```
H := lijst[9];
Size(H);
```

We vinden een ondergroep H van orde 4. De elementen in deze groep moeten orde 2 of 4 hebben. De groep A_4 bevat geen elementen van orde 4, dus H bestaat uit e en de 3 elementen in A_4 van orde 2. Kortom, $H = V_4$. Dat zien we ook in de GAP-output:

```
Group([ (1,3)(2,4), (1,2)(3,4) ])
```

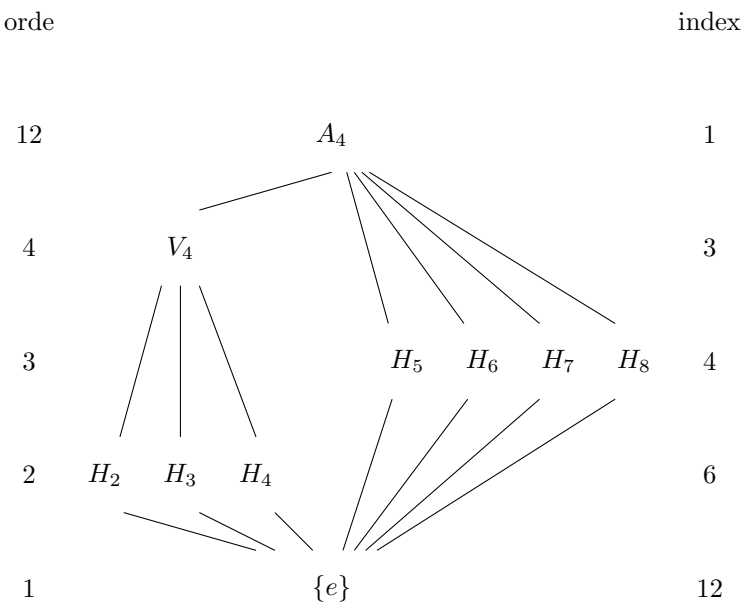
Merk op dat deze output niet alle elementen van H geeft – het element $(1, 4)(2, 3)$ staat er niet in – maar slechts twee *voortbrengers*.

U kunt nu zelf checken dat de groepen `lijst[8]`, `lijst[7]`, `lijst[6]`, `lijst[5]` de stabilisatorondergroepen zijn. Bijvoorbeeld is de laatste gelijk aan $\{e, (2, 3, 4), (2, 4, 3)\}$, de stabilisatorondergroep van $i = 1$.

Tot slot de groepen `lijst[4]`, `lijst[3]` en `lijst[2]`: dit zijn de ondergroepjes $\{e, (1, 4)(2, 3)\}$, $\{e, (1, 3)(2, 4)\}$ en $\{e, (1, 2)(3, 4)\}$.

Alle ondergroepen van A_4

In Figuur 1.2 staan de ondergroepen van A_4 en hun onderlinge relaties weergegeven.



Figuur 1.2: De ondergroepen van A_4

Normaliteit

In iedere groep G zijn de triviale ondergroep $\{e\}$ en de hele groep G normale ondergroepen. Ondergroepen van index 2 zijn normaal, dus H_2, H_3 en H_4 zijn normaal in V_4. (De groep V_4 is commutatief, dus iedere ondergroep van V_4 is sowieso normaal in V_4.) Verder is in het bovenstaande diagram alleen V_4 normaal in A_4.

Om in te zien dat V_4 normaal is in A_4, is het voldoende op te merken dat conjungatie cykeltype behoudt. De ondergroep V_4 bevat behalve e alle 3 permutaties van cykeltype $2+2$, dus alle conjugaties in A_4 (en zelfs in S_4) beelden V_4 op zichzelf af.

Het is gemakkelijk om in te zien dat de 4 stabilisatoren $H_5, \ldots, H_8$ niet normaal zijn in A_4. Conjungatie met $(1,2)(3,4)$ verwisselt bijvoorbeeld de

stabilisatoren van 1 en 2 (en ook die van 3 en 4). Net zo zie je in dat de ondergroepen H_2, H_3, H_4 niet normaal zijn in A_4.

Je kunt ook GAP gebruiken:

```
G := AlternatingGroup(4);
NSG := NormalSubgroups(G);
Size(G);
H := NSG[2];
Size(H);
```

GAP zegt dat er 3 normale ondergroepen zijn. Behalve de triviale normale ondergroepen $\{e\}$ en A_4 hebben we `NSG[2]`. Dit is de groep V_4.

1.6.2 De ondergroepen van de groep D_8

Hiervoor hebben we de groep van rotaties en spiegelingen van een vierkant bekeken. We noemden deze groep toen G_2, maar de officiële naam van deze groep is *de diëdergroep van orde 8*. Soms wordt deze groep genoteerd als D_4, vanwege de connectie met het 4-kant, maar anderen schrijven D_8 om aan te geven dat de groep orde 8 heeft. Wij kiezen in dit document voor de notatie D_8, omdat dat beter past bij de notaties van de software GAP.

In de vorige paragrafen heeft u de ondergroepen van A_4 bepaald, de inclusies en u heeft bepaald welke ondergroepen normaal zijn.

Opgave 1.6.2. Doe nu hetzelfde voor de symmetriegroep D_8 van het vierkant. De code in GAP hiervoor is `DihedralGroup(8)`.

1.6.3 De automorfismengroep van Q_8

Deze lange paragraaf is in wezen één vrij lange en lastige opgave, namelijk het construeren van een isomorfisme tussen de automorfismengroep van Q_8 en de groep S_4. Waarom? Omdat dit weer een andere manier is om interessante groepen te maken. Je kunt de automorfismengroep van een groep G zien als 'de groep van symmetrieën van G'. Uiteraard geeft deze groep belangrijke informatie over de groep G.

De quaterniongroep Q_8 is een groep van orde 8. De elementen hebben traditioneel de volgende namen:

$$Q_8 := \{1, -1, i, -i, j, -j, k, -k\}$$

Het element 1 is het neutrale element van de groep en vermenigvuldiging met -1 doet precies wat je denkt: $(-1)^2 = 1$, $(-1) \cdot i = i \cdot (-1) = -i$, $(-1) \cdot (-i) = (-i) \cdot (-1) = i$, etcetera. De groepsvermenigvuldiging wordt

verder bepaald door

$$i^2 = j^2 = k^2 = -1$$

en

$$ij = k = -ji \qquad jk = i = -kj \qquad ki = j = -ik.$$

Opgave 1.6.3. Laat f een automorfisme van Q_8 zijn, dus $f\colon Q_8 \to Q_8$ is een groepsisomorfisme van Q_8 naar zichzelf. Laat zien dat $f(1) = 1$ en $f(-1) = -1$. (Hint: -1 is het enige element in $Q_8 \setminus \{1\}$ dat commuteert met alle elementen van Q_8.)

Stelling 1.6.4. *De groep* $\mathrm{Aut}(Q_8)$ *van automorfismen van* Q_8 *is isomorf met* S_4*.*

Bewijs. We construeren een isomorfisme

$$\Phi\colon S_4 \to \mathrm{Aut}(Q_8).$$

We weten dat ieder automorfisme f van Q_8 voldoet aan $f(1) = 1$, $f(-1) = -1$ en $f(-g) = -f(g)$ voor alle $g \in Q_8$. het is dus voldoende om $x = f(i)$, $y = f(j)$ en $z = f(k)$ te weten. Dit zijn elementen van Q_8 die voldoen aan

$$xy = z = -yx \qquad yz = x = -zy \qquad zx = y = -xz.$$

We zullen in het vervolg van dit bewijs zo'n automorfisme f noteren als $[x, y, z]$.

Een manier om automorfismen van Q_8 te produceren is door middel van conjungatie. Conjungatie met i is de afbeelding $g \mapsto igi^{-1} = -igi$. Merk op dat conjungatie met $-i$ hetzelfde is als conjungatie met i, want $(-i)g(-i)^{-1} = -igi = igi^{-1}$ voor alle $g \in Q_8$. Deze conjungatieafbeelding heeft $[x, y, z] = [i, -j, -k]$. Analoog: conjungatie met $\pm j$ heeft $[x, y, z] = [-i, j, -k]$ en conjungatie met $\pm k$ heeft $[x, y, z] = [-i, -j, k]$.

Deze drie automorfismen laten we via Φ corresponderen met de permutaties $(1, 2)(3, 4)$, $(1, 3)(2, 4)$ en $(1, 4)(2, 3)$, dus:

$$\begin{aligned} \Phi((1,2)(3,4)) &= [i, -j, -k] \\ \Phi((1,3)(2,4)) &= [-i, j, -k] \\ \Phi((1,4)(2,3)) &= [-i, -j, k]. \end{aligned}$$

We hebben nu Φ gedefinieerd op de ondergroep

$$V_4 = \{e, (12)(34), (13)(24), (14)923)\}$$

van S_4.

We definiëren $\Phi((2,3,4))$ door $[x,y,z] = [j,k,i]$. Dit impliceert

$$\Phi((1,3,2)) = \Phi((2,3,4))\Phi((1,2)(3,4)) = [j,k,i] \circ [i,-j,-k] = [j,-k,-i],$$

omdat $(2,3,4)(1,2)(3,4) = (1,3,2)$. Merk op dat $(1,3)(2,4)(2,3,4) = (1,3,2)$, dus

$$\Phi((1,3,2)) = \Phi((1,3)(2,4))\Phi((2,3,4)) = [-i,j,-k] \circ [j,k,i] = [j,-k,-i].$$

Gelukkig levert dit hetzelfde antwoord op. (Dit is de reden waarom ik $\Phi((2,3,4))$ heb gedefinieerd als $[j,k,i]$. Ik had eerst $\Phi((1,2,3) = [j,k,i]$ geprobeerd, maar dat leidde tot inconsistenties.)
Analoog vind je

$$\Phi((1,2,4)) = [-j,-k,i] \qquad \Phi((1,4,3)) = [-j,k,-i].$$

Door te inverteren, vinden we

$$\begin{aligned}
\Phi((2,4,3)) &= [j,k,i]^{-1} = [k,i,j] \\
\Phi((1,2,3)) &= [j,-k,-i]^{-1} = [-k,i,-j] \\
\Phi((1,4,2)) &= [-j,-k,i]^{-1} = [k,-i,-j] \\
\Phi((1,3,4)) &= [-j,k,-i]^{-1} = [-k,-i,j]
\end{aligned}$$

Nu hebben we Φ gedefinieerd op de ondergroep A_4 van S_4 die bestaat uit de 4 elementen van V_4 en de 8 3-cykels $(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$ en $(4,3,2)$.
Tot slot definiëren we $\Phi((1,2))$ door $[-i,k,j]$. Nu volgt

$$\Phi((2,3)) = \Phi((1,2))\Phi((1,2,3)) = [-i,k,j] \circ [-k,i,-j] = [-j,-i,-k]$$

omdat $(1,2)(1,2,3) = (2,3)$ en

$$\Phi((3,4)) = \Phi((1,2))\Phi((1,2)(3,4)) = [-i,k,j] \circ [i,-j,-k] = [-i,-k,-j]$$

omdat $(1,2)(1,2)(3,4) = (3,4)$. □

Opgave 1.6.5. Verifieer dat dit soort berekeningen leiden tot een groepshomomorfisme $\Phi\colon S_4 \to \mathrm{Aut}(Q_8)$. De volledige beschrijving van Φ staat in Tabel 1.2.

Opgave 1.6.6. Verifieer dat Φ injectief is.

Opgave 1.6.7. Overtuig uzelf dat Φ surjectief is.

g	$\Phi(g)$
e	$[i,j,k]$
$(1,2)(3,4)$	$[i,-j,-k]$
$(1,3)(2,4)$	$[-i,j,-k]$
$(1,4)(2,3)$	$[-i,-j,k]$
$(1,2,3)$	$[-k,i,-j]$
$(1,3,2)$	$[j,-k,-i]$
$(1,2,4)$	$[-j,-k,i]$
$(1,4,2)$	$[k,-i,-j]$
$(1,3,4)$	$[-k,-i,j]$
$(1,4,3)$	$[-j,k,-i]$
$(2,3,4)$	$[j,k,i]$
$(2,4,3)$	$[k,i,j]$

g	$\Phi(g)$
$(1,2)$	$[-i,k,j]$
$(1,3)$	$[k,-j,i]$
$(1,4)$	$[j,i,-k]$
$(2,3)$	$[-j,-i,-k]$
$(2,4)$	$[-k,-j,-i]$
$(3,4)$	$[-i,-k,-j]$
$(1,2,3,4)$	$[k,j,-i]$
$(1,4,3,2)$	$[-k,j,i]$
$(1,2,4,3)$	$[j,-i,k]$
$(1,3,4,2)$	$[-j,i,k]$
$(1,3,2,4)$	$[i,k,-j]$
$(1,4,2,3)$	$[i,-k,j]$

Tabel 1.2: Beschrijving van Φ

Opgave 1.6.8. Neem de kubus met hoekpunten $(\pm 1, \pm 1, \pm 1)$. Identificeer het hoekpunt $(\epsilon_1, \epsilon_2, \epsilon_3)$ met $\epsilon_1 i + \epsilon_2 j + \epsilon_3 k$. Een automorfisme f van Q_8 werkt op de 8 hoekpunten van de kubus door

$$f(\epsilon_1 i + \epsilon_2 j + \epsilon_3 k) := \epsilon_1 f(i) + \epsilon_2 f(j) + \epsilon_3 f(k).$$

Verifieer dat dit een isomorfisme Ψ van de groep $\mathrm{Aut}(Q_8)$ naar de rotatiegroep van de kubus definieert. De actie van de rotatiegroep van de kubus op de 4 diagonalen van de kubus geeft een isomorfisme van de rotatiegroep van de kubus met S_4. Door deze twee isomorfismen te combineren, krijg je een isomorfisme $\Psi\colon \mathrm{Aut}(Q_8) \cong S_4$. (Als je de diagonaal door $(1,1,1) = i+j+k$ nummer 1 geeft, de diagonaal door $(-1,1,1) = -i+j+k$ nummer 2, de diagonaal door $(1,-1,1) = i-j+k$ nummer 3 en de diagonaal door $(1,1,-1) = i+j-k$ nummer 4, dan krijg je op deze manier precies de inverse van het isomorfisme $\Phi\colon S_4 \to \mathrm{Aut}(Q_8)$ van opgave 6.4.)

Opgave 1.6.9. Je kunt ook GAP gebruiken om te verifiëren dat $\mathrm{Aut}(Q_8)$ en S_4 isomorf zijn.

```
S4 := SymmetricGroup(4);
Q8 := QuaternionGroup(8);
A := AutomorphismGroup(Q8);
```

Vervolgens vraag je `IdGroup(A)` en `IdGroup(S4)`. Beide keren geeft GAP hetzelfde antwoord, namelijk $[24, 12]$. Beide groepen zijn dus nummer 12 op GAP's lijstje van (isomorfieklassen van) groepen van orde 24. Er geldt dus $\mathrm{Aut}(Q_8) \cong S_4$.

1.7 Enkele elementaire stellingen uit de groepentheorie

You can never be overdressed or overeducated. Oscar Wilde

Laat G een eindige groep zijn.

Stelling 1.7.1 (Lagrange)**.** *Laat H een ondergroep zijn van G. Dan is $|H|$ een deler van $|G|$.*

Bewijs. Dit volgt uit de theorie van nevenklassen. □

Gevolg 1.7.2. *Voor elk element g in G geldt dat de orde van g een deler is van $|G|$.*

Stelling 1.7.3 (Cauchy)**.** *Als p een priemdeler is van $|G|$, dan bevat G een element g van orde p.*

1.8 Nevenklassen en quotiëntgroepen

We behandelen kort nevenklassen (Engels: *cosets*) en quotiëntgroepen en we bewijzen daarmee de stelling van Lagrange uit het vorige hoofdstukje. Gegeven zijn een groep G en een ondergroep H.

1.8.1 Linkernevenklassen

Definitie 1.8.1. We definiëren de *linkernevenklassen* van H in G als de verzamelingen

$$gH = \{gh \mid h \in H\}.$$

Lemma 1.8.2.
1. *Twee elementen $g_1, g_2 \in G$ liggen precies dan in dezelfde linkernevenklasse van H in G als er een $h \in H$ is met $g_1 = g_2 h$.*
2. *De relatie*

$$g_1 \sim g_2 \qquad \Longleftrightarrow \qquad \exists h \in H : g_1 = g_2 h$$

   is een equivalentierelatie op G en de linkernevenklassen van H in G zijn de equivalentieklassen van deze relatie.
3. *Als $g_1 H$ en $g_2 H$ verschillende nevenklassen van H in G zijn, dan geldt $g_1 H \cap g_2 H = \emptyset$.*
4. *G is de disjuncte vereniging van de nevenklassen van H in G.*

5. *H is de nevenklasse van e.*
6. *De afbeelding $h \mapsto gh$ is een bijectie tussen H en gH. Alle nevenklassen zijn dus even groot.*

Bewijs. Opgave. □

Gevolg 1.8.3. *Als $|G|$ eindig is, dan is $|H|$ een deler van $|G|$.*

Bewijs. Opgave. □

Gevolg 1.8.4. *Als $g \in G$ en $|G|$ is eindig, dan is de orde van g een deler van $|G|$.*

Bewijs. Als k de orde is van g, dan is

$$\langle g \rangle := \{g, g^2, \ldots, g^k = e\}$$

een ondergroep van G van orde k. Dus is k een deler van $|G|$. □

1.8.2 Rechternevenklassen

Analoog aan de linkernevenklassen definiëren we rechternevenklassen van H in G als

$$Hg = \{hg \mid h \in H\}$$

voor $g \in G$. De theorie is volkomen analoog aan die van linkernevenklassen.

1.8.3 De index van een ondergroep

We schrijven G/H voor de verzameling linkernevenklassen van H in G. Als het aantal nevenklassen eindig is, dan wordt dit aantal de *index* van H in G genoemd. Dit getal wordt genoteerd als $[G : H]$. Als $|G|$ eindig is, zeg $|H| = m$ en $|G| = nm$, dan zijn er precies n linkernevenklassen van H in G. In dit geval is de index van H in G dus gelijk aan

$$[G : H] = n = \frac{|G|}{|H|}.$$

1.8.4 Quotiëntgroepen

Definitie 1.8.5. De ondergroep H is *normaal* in G als de linkernevenklassen van H in G samenvallen met de rechternevenklassen van H in G, dus als

$$gH = Hg$$

voor alle $g \in G$.

Lemma 1.8.6. *Iedere ondergroep H van G van index 2 is normaal in G.*

Bewijs. Omdat de index 2 is, zijn er slechts 2 linkernevenklassen en ook slechts 2 rechternevenklassen. De ondergroep H is zowel een linkernevenklasse eH als een rechternevenklasse He. De unieke andere linkernevenklasse is dus het complement $G \setminus H$ van H in G en dit complement is tegelijkertijd ook de unieke andere rechternevenklasse. □

Dit werkt alleen bij index 2. Bijvoorbeeld is de ondergroep $H = \{e, (12)\}$ niet normaal in S_3, hoewel de index van H in S_3 slechts $6/2 = 3$ is.

Laat nu N een normale ondergroep van G zijn. De linkernevenklassen gN vallen nu samen met de rechternevenklassen Ng.

Stelling 1.8.7. *Gegeven twee nevenklassen A en B van N in G is ook het product*

$$AB = \{ab \mid a \in A, b \in B\}$$

een nevenklasse. Dit product definieert een groepsstructuur op de verzameling G/N van nevenklassen van N in G. Deze groep heet de quotiëntgroep *van N in G. Het neutrale element van deze quotiëntgroep is de nevenklasse $N = eN = Ne$. De inverse van de nevenklasse $gN = Ng$ is $g^{-1}N = Ng^{-1}$.*

Bewijs. Stel $A = g_1N = Ng_1$ en $B = g_2N = Ng_2$. Dan geldt

$$AB = \{g_1n_1g_2n_2 \mid n_1, n_2 \in N\} = \{g_1g_2n_1n_2 \mid n_1, n_2 \in N\} = g_1g_2N.$$

In de tweede stap hebben we de normaliteit van N in G gebruikt. De rest van het bewijs laten we als opgave voor de lezer. □

Opgave 1.8.8. Bewijs dat A_4 een normale ondergroep is van S_4 van index 2 en bewijs dat de quotiëntgroep S_4/A_4 isomorf is met $\mathbf{Z}/2\mathbf{Z}$.

Opgave 1.8.9. Bewijs dat $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ een normale ondergroep is van S_4 van index 3 en bewijs dat de quotiëntgroep S_4/V_4 isomorf is met $\mathbf{Z}/3\mathbf{Z}$.

Opgave 1.8.10. Bewijs dat $Z = \{e, r^2\}$ een normale ondergroep is van de symmetriegroep

$$D_8 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

van het vierkant. (Deze groep hebben we eerder ook wel G_2 genoemd omdat dit de tweede groep was die we bestudeerd hebben.) Laat zien dat Z index 4 heeft in D_8 en bewijs dat de quotiëntgroep D_4/Z isomorf is met $V_4 \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

1.9 Hoe verder in de groepentheorie?

Learning never exhausts the mind. Leonardo Da Vinci

Dit was een eerste kennismaking met groepentheorie. De nadruk lag op het begrijpen van enkele kleine groepen, zoals rotatiegroepen van regelmatige lichamen (tetraëders, kubussen, octaëders, dodecaëders, icosaëders) en op de volgende elementaire concepten:

- orde van een groep;
- orde van een element;
- ondergroep;
- normale ondergroep;
- voortbrengers;
- symmetriegroepen begrijpen als ondergroepen van bepaalde permutatiegroepen.

Om verder te komen in de groepentheorie kunt u de *eerste isomorfiestelling* bestuderen (het beeld van een groepshomomorfisme $f\colon G_1 \to G_2$ is isomorf met het quotiënt van G_1 naar de kern van f), de structuur van eindige abelse groepen, directe producten, semi-directe producten, de stellingen van Sylow, etcetera.

Hier zijn twee bronnen voor uw vervolgstudie:

1. J.S. Milne, *Group Theory*, `https://milne.org/math/CourseNotes/gt.html`.
2. J.J. Rotman, *An Introduction to the Theory of Groups*, Graduate Texts in Mathematics 148, Springer Verlag.

Het eerste boek is gratis toegankelijk (maar ik kreeg een waarschuwing van mijn browser...). De volgende twee boeken zijn populair-wetenschappelijk en vertellen over de classificatie van eindige simpele groepen (de 'symmetrieatomen' van Mark Ronan) en over 'monstrous moonshine':

1. Mark Ronan, *Symmetry and the Monster*, Oxford University Press (2006).
2. Marcus du Sautoy, *Finding Moonshine*, Harper Perennial (2008).

We hebben al geroken aan het belangrijke concept van de *werking van een groep op een verzameling*. Een groep G kan werken op een verzameling $X = \{1, \ldots, n\}$. Dit correspondeert met een groepshomomorfisme $G \to S_n$. We hebben dit gezien voor de rotatiegroep van de kubus: die werkte op de verzameling X van de 4 diagonalen van de kubus. Het belangrijkste elementaire feit over groepswerkingen is vermoedelijk: *de lengte van een baan is gelijk aan de index van de stabilisatorondergroep*. Dus als $x \in X$ en

$$Y := Gx = \{gx \mid g \in G\} \subseteq X$$

is de *baan* van x onder G (Engels: *orbit*) in X, dan geldt

$$|Y| = |G|/|G_x|,$$

waarbij $G_x := \{g \in G \mid g(x) = x\}$ de *stabilisatorondergroep* van x in G is. Een grove intuïtie hierbij is: als $|G_x|$ groot is, dan zijn er veel elementen in G die niets doen met x, dus de baan Gx van x in X is klein. Preciezer: als $|G_x| = m$ en $|G| = mn$, dan valt de groep G uiteen in n disjuncte delen[6] $A_1, \ldots, A_n$ van ieder m elementen zodat alle elementen in een vaste A_j hetzelfde doen met x, terwijl elementen van G in verschillende delen A_j, A_k x op verschillende elementen van X afbeeldt.

Een belangrijk speciaal geval van groepswerking is groepswerking door middel van lineaire afbeeldingen op een vectorruimte. Dit worden (lineaire) representaties van de groep genoemd. De theorie van representaties is een prachtig en krachtig hulpmiddel om groepen te begrijpen. Tabellen die de representatietheorie beschrijven van de simpele groepen vormen dan ook het hart van het eerdergenoemde monumentale naslagwerk *ATLAS of Finite Simple Groups*.

[6] Deze delen zijn de eerdergenoemde linkernevenklassen van G_x in G.

2 Waarom complex niet per se moeilijk is een introductie tot de groep SU(2)

David Eelbode

In dit deel van de bundel gaan we uit van de volgende voorkennis:

- De formele definitie van een groep $(G, *)$. In het bijzonder kan de lezer dus nagaan of alle groepsaxioma's voldaan zijn, en het eenheidselement in een specifieke groep vinden.
- Het concept van een groepsmorfisme $\rho : G_1 \to G_2$. Daarbij is het uiteraard vooral belangrijk om na te gaan dat $\rho(gh) = \rho(g)\rho(h)$, met $g, h \in G_1$.
- De basisdefinities voor matrices[1], zoals de elementaire bewerkingen, en de definitie voor de determinant. In het bijzonder is cruciaal om te weten dat $\det(AB) = \det(A)\det(B)$. Ook het concept van de *trace* (het spoor) van een matrix zal gebruikt worden in wat volgt (de som van alle elementen op de diagonaal).
- Basisconcepten voor complexe getallen, zoals de modulus en de polaire voorstelling (met dus $\zeta = |\zeta|e^{i\theta}$ voor een $\zeta \in \mathbb{C}$).

Deze bundel bevat ook een aantal oefeningen: deze kunnen helpen om zelf wat aan de slag te gaan met het materiaal in deze bundel, en zo meer te ontdekken over matrixgroepen. Ze zijn echter nooit nodig om verder te kunnen lezen.

2.1 Fantastic groups & where to find them

Voor we onze aandacht richten op de groep SU(2) is het misschien handig om heel even stil te staan bij de vraag waarom matrices überhaupt opduiken in een workshop over groepen. Daar is een makkelijke en directe verklaring voor te geven, alsook een meer fundamentele.

Laten we beginnen met de meest eenvoudige reden: omdat men de (vierkante) matrices kan zien als 'veralgemeningen van getallen' ligt het voor de

[1] We gebruiken de notatie $\mathbb{R}^{m\times n}$ en $\mathbb{C}^{m\times n}$ voor matrices in deze bundel.

hand om daar naar voorbeelden van groepen te zoeken, iets wat uiteraard belangrijk is in de educatieve context van een les over groepen. Op die manier kan je namelijk als leerkracht makkelijk (interessante) voorbeelden of oefeningen verzinnen over groepen. Wanneer het gaat over groepen ziet men vaak in eerste instantie de volgende voorbeelden opduiken:

- Eindige groepen gebaseerd op de symmetrieën van vlakke figuren (zoals de groep S_3 of de zogenaamde diëdergroepen D_n).
- Oneindige groepen gebaseerd op de gekende getallenverzamelingen. Dat kunnen dan zowel additieve groepen zijn (waarbij de bewerking de optelling is), als multiplicatieve[2] groepen (voor de vermenigvuldiging). Denk maar aan de groepen $(\mathbb{Z}, +)$ of $(\mathbb{Q}_0, \times)$, al zijn hier uiteraard meer voorbeelden te verzinnen.
- Ook de combinatie van bovenstaande voorbeelden bestaat: *eindige* groepen, waar je toch met getallen zit te werken[3]. Zo is $(\{+1, -1\}, \times)$ een klein groepje, en kan je voor elke $n \in \mathbb{N}_0$ gaan kijken naar de groep
$$C_n := (\{\xi \in \mathbb{C} : \xi^n = 1\}, \times) \ ,$$
waarbij we hier meteen ook de geijkte notatie meegeven (C_n staat voor de 'cyclische groep' van orde n). De goede verstaander ziet hopelijk meteen dat ons kleine groepje dan niets anders is dan C_2.
- Indien modulo-rekenen reeds gepasseerd is in de lessen, dan kan men ook gaan kijken naar eindige 'getallengroepen' binnen de wereld van het modulo-rekenen. Zowel additief, alsook multiplicatief (tenzij je allergisch bent aan priemgetallen, dan beter niet).
- Wie vertrouwd is met vectorruimten kan meteen een stapje verder gaan, en opmerken dat $(V, +)$ steeds een (additieve) groep zal definiëren. Dat opent de deur naar vrij abstracte voorbeelden.

Omdat men matrices van eenzelfde formaat steeds bij elkaar kan optellen, en zelfs vermenigvuldigen indien dat formaat van een *vierkante* familie is, ligt het voor de hand dat men de voorbeelden van de tweede soort in de lijst hierboven makkelijk kan gaan uitbreiden. Dit past ook in de filosofie dat men de klassieke getallen kan opvatten als matrices van orde (1×1), iets wat we uiteraard zelden doen[4]. Zo is het een makkelijke oefening om aan te tonen dat pakweg $(\mathbb{R}^{m\times n}, +)$ en $(\mathbb{C}^{m\times n}, +)$ groepen zijn, zeker voor

[2] In deze bundel wordt de notatie $\mathbb{K}_0 = \mathbb{K} \setminus \{0\}$ gebruikt voor een getallenverzameling waaruit we de nul weglaten. Merk op dat dit soms ook wordt genoteerd als $\mathbb{K}^\times$.

[3] Of toch op het eerste zich, want de kunst bestaat er uiteraard in om die groepen dan toch 'meetkundig' te gaan interpreteren.

[4] En gelukkig maar, het zou een aanslag zijn op ons milieu moesten we getallen telkens opnieuw noteren met haakjes rond: logisch correct, ecologisch iets minder.

wie weet dat dit deze verzamelingen ook de structuur van een vectorruimte hebben.

Matrices geven ook aanleiding tot een resem multiplicatieve groepen, alleen moet men hier rekening houden met één cruciaal gegeven: *deze keer is het niet voldoende om enkel de nulmatrix uit te sluiten.* Een vierkante matrix is namelijk enkel (multiplicatief) inverteerbaar als de determinant niet nul is, en dat brengt ons meteen bij 2 van de meest elementaire matrixgroepen[5]:

$$\boxed{\begin{aligned} \mathrm{GL}(m,\mathbb{R}) &:= \{M \in \mathbb{R}^{m\times m} : \det(M) \neq 0\} \\ \mathrm{GL}(m,\mathbb{C}) &:= \{M \in \mathbb{C}^{m\times m} : \det(M) \neq 0\} \end{aligned}}$$

Merk op dat de bewerking hier niet expliciet meer vermeld werd (zie ook voetnoot 4). Bovenstaande groepen zijn dus de veralgemeningen van $(\mathbb{R}_0, \times)$ en $(\mathbb{C}_0, \times)$ naar 'hogere dimensie'.

Oefening 2.1: *de groep* $(\mathbb{R}_0^+, \times)$ *is een deelgroep van* $(\mathbb{R}_0, \times)$. *Kan je deze groep veralgemenen naar hogere dimensie (door een matrixgroep in de te voeren)?*

Oefening 2.2: *kan je de determinant interpreteren als een groepsmorfisme tussen twee geschikte groepen?*

Je kan gerust stellen dat alle 'interessante' matrixgroepen deelgroepen zullen zijn van bovenstaande groepen, die men in de vakliteratuur de *General Linear groups* noemt (over $\mathbb{R}$ of $\mathbb{C}$). In het bijzonder zullen we straks ook zien dat $\mathrm{SO}(3,\mathbb{R}) < \mathrm{GL}(3,\mathbb{R})$ en $\mathrm{SU}(2) < \mathrm{GL}(2,\mathbb{C})$, waarbij in deze bundel de notatie $H < G$ wordt gebruikt voor een deelgroep H in G.

Oefening 2.3: *kan je een* $a \neq 0$ *vinden met als eigenschap dat alle matrices* M *in* $\mathrm{GL}(m,\mathbb{R})$ *waarvoor geldt dat* $\det(M) = a$ *een deelgroep vormen? Indien ja, kan je zien welke deelgroep van de getallenverzameling je dan precies veralgemeend hebt naar de wereld van de matrices?*

Oefening 2.4: *toon aan dat de verzameling van alle symmetrische matrices in* $\mathbb{R}^{m\times m}$ *of* $\mathbb{C}^{m\times m}$ *een groep is voor de optelling (een matrix is symmetrisch als* $M^T = M$, *met* M^T *de getransponeerde van een matrix). Is het ook een groep voor de vermenigvuldiging (als we niet-inverteerbare*

[5] In de wiskunde gebruikt men de term 'matrixgroep' enkel in multiplicatieve context: dit zijn dus alle inverteerbare matrices over een veld (of lichaam), waarbij de bewerking de vermenigvuldiging is.

matrices weglaten)?

Je zou bijna vergeten dat we op de eerste pagina ook hadden gesproken over een meer fundamentele reden waarom matrices zo vaak opduiken in de wereld van de groepen. Dit heeft alles te maken met het feit dat we matrices meestal opvatten als *lineaire transformaties*, waarmee we dan vectoren kunnen omzetten in andere vectoren. Dat doen we typisch in coördinaten, door $X \mapsto Y = MX$ te beschouwen als onze transformatie (met X en Y dan kolommatrices). Stel nu dat onze vectoren *een bijzondere eigenschap* vertonen — we geven meteen een makkelijk voorbeeld van zo'n eigenschap — dan is het uiteraard interessant om te weten welke transformaties (lees: matrices) die eigenschap zullen *bewaren*. Dergelijke (matrix)groepen zijn dus symmetriegroepen, waarbij je het woord 'symmetrie' dan wel iets ruimer (lees: abstracter) moet interpreteren dan wat je gewoon bent als je denkt aan het concept 'symmetrie'. Meestal denken we dan spontaan aan sneeuwvlokken[6], of aan het gezicht van knappe actrices en acteurs, maar hier moet je de transformatie zien als een symmetrie 'omdat het iets bewaart' (de eigenschap in kwestie).

Laten we niet langer rond de abstracte pot draaien, en een voorbeeld geven om bovenstaand principe te illustreren. We zullen daarbij werken met vectoren in $\mathbb{R}^3$, die we voorstellen met een kolommetje $(x, y, z)^T$, uitgedrukt ten opzichte van een orthonormale basis[7]. Elk punt in de ruimte kunnen we nu identificeren met zo'n kolommetje, dat dan uiteraard de coördinaten van dat punt voorstelt. Elke matrix M in $\mathrm{GL}(3, \mathbb{R})$ kunnen we nu zien als een transformatie die 'inwerkt op de punten' door $(x, y, z)^T$ naar $M(x, y, z)^T$ te sturen. Maar wat als we nu ook eisen dat de afstand van een punt tot de oorsprong bewaard blijft onder de transformatie? Uiteraard verliezen we dan bepaalde matrices, want zo zal pakweg de matrix

$$M = \begin{pmatrix} 42 & 0 & 0 \\ 0 & 42 & 0 \\ 0 & 0 & 42 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{R})$$

de afstand tot de oorsprong *niet* bewaren. Door enkel op zoek te gaan naar matrices die de afstand tot de oorsprong *wel* bewaren, gaan we dus op zoek naar transformaties (van punten in de ruimte) die een eigenschap invariant

[6] Wie nu spontaan aan de Lagrangiaan van het standaardmodel in de deeltjesfysica moet denken is een uitzondering.

[7] Voor de kenners: we werken dus in een Euclidische ruimte, zijnde de vectorruimte $(\mathbb{R}^3, +, \cdot)$ waarop we het klassieke inproduct hebben gedefinieerd.

laten[8]. Op deze manier komen we tot de zogenaamde orthogonale groep:

$$\boxed{\mathrm{O}(3,\mathbb{R}) := \{M \in \mathrm{GL}(3,\mathbb{R}) : MM^T = M^T M = \mathrm{Id}_3\}}$$

met Id_3 de notatie voor de eenheidsmatrix. Omdat $\det(M) = \det(M^T)$ vinden we ook dat $\det(M)^2 = 1$ als $M \in \mathrm{O}(3,\mathbb{R})$, en dat brengt ons op natuurlijke wijze tot een belangrijke deelgroep:

$$\boxed{\mathrm{SO}(3,\mathbb{R}) := \{M \in \mathrm{O}(3,\mathbb{R}) : \det(M) = +1\}}$$

Dit is de zogenaamde *speciale orthogonale groep* (of rotatiegroep) in 3 dimensies, die je bijvoorbeeld kan gebruiken om te begrijpen wat je doet als je een *Rubik's cube* gaat bestuderen.

Oefening 2.5: *kan je een element M vinden dat wel in $\mathrm{O}(3,\mathbb{R})$ zit, maar niet in de deelgroep $\mathrm{SO}(3,\mathbb{R})$? Kan je ook meetkundig interpreteren wat de elementen zijn die niet in deze deelgroep zitten?*

Oefening 2.6: *vormt de verzameling matrices $M \in \mathrm{O}(3)$ met $\det(M)$ gelijk aan -1 ook een deelgroep?*

Oefening 2.7: *als je rekening houdt met het feit dat het kwadraat van de afstand van een punt in de ruimte tot de oorsprong kan geschreven worden als*

$$x^2 + y^2 + z^2 = (x, y, z)(x, y, z)^T \ ,$$

kan je dan inzien vanwaar de conditie $M^T M = \mathrm{Id}_3$ vandaan komt?

Oefening 2.8: *toon aan[9] dat als er voor twee (vierkante) matrices A en B geldt dat $AB = \mathrm{Id}_3$, dat dan ook $BA = \mathrm{Id}_3$. Bewijs daarvoor eerst dat B^{-1} bestaat (hint: gebruik de determinant), en gebruik dan dat we uit het gegeven alvast kunnen halen dat $BAB = B$.*

Bij wijze van samenvatting, en mits een licht gevoel voor dramatiek, kunnen we besluiten dat alle groepen in de wiskunde symmetriegroepen zijn, die in één of andere context één of andere relevante eigenschap zullen bewaren. Omdat deze groepen bovendien ook constant opduiken in de fysica, en al zeker in de mysterieuze wereld van de quantummechanica, kan men stellen dat fysica de studie is van symmetrie. Of zoals de Nobelprijswinner Philip Anderson het ooit zei:

[8] Merk op dat $M(0,0,0)^T = (0,0,0)^T$ voor alle matrices M, dus hier hebben we ook dat de oorsprong blijft liggen onder de inwerking van een transformatie.

[9] Deze opgave verklaart waarom we in feite ook gewoon kunnen zeggen dat de voorwaarde $M^T M = \mathrm{Id}_3$ voldoende is om $\mathrm{O}(3)$ te definiëren.

...it is only slightly overstating the case
to say that physics is the study of symmetry.

2.2 Complex draaien: rotaties versimpelen

Waarom rotaties nu precies zo belangrijk zijn in de natuur is nog steeds een mysterie — zeker de vraag waarom de ons gekende elementaire deeltjes een 'spin' hebben is nog steeds een bron van vraagtekens — maar het goede nieuws is wel dat we rotaties makkelijk wiskundig kunnen beschrijven. In dit deel gaan we daar dieper op in, en wel door gebruik te maken van complexe getallen. Hoewel die laatste (soms) schrik inboezemen is de connectie met rotaties wel makkelijk te verklaren: zo kunnen we punten in het vlak (vectoren in $\mathbb{R}^2$) roteren over een hoek θ in positieve draaizin (i.e. tegenwijzerzin) door te transformeren met

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ ,$$

maar wie dat punt opvat als het complexe[10] getal $\zeta = x + iy$ ziet hopelijk in dat diezelfde rotatie makkelijk te schrijven valt als $\zeta \mapsto e^{i\theta}\zeta$. We zagen eerder wat de definitie is voor $\mathrm{SO}(2,\mathbb{R})$, waar dus het type matrix leeft zoals hierboven (met de goniometrische getallen), maar wat we nu bijleren is dat we evengoed zouden kunnen werken met de (op dit moment nieuwe) groep

$$\boxed{\mathrm{U}(1) := \{\xi \in \mathbb{C} : |\xi| = 1\}}$$

Merk op dat dit een deelgroep is van $(\mathbb{C}_0, \times)$, waarbij we dus enkel de complexe getallen beschouwen met modulus gelijk aan 1 (anders gezegd: de getallen op een afstand 1 van de oorsprong in het complexe vlak). Omdat $x^2+y^2 = |\zeta|^2$, met daarbij $\zeta = x+iy$, zou het ook meteen duidelijk moeten zijn dat $|\zeta|^2$ hier bewaard blijft als eigenschap. Inderdaad, als $|\xi| = 1$, dan zien we dat

$$|\xi\zeta|^2 = |\xi|^2|\zeta|^2 = |\zeta|^2 \ .$$

De groep U(1) is dus inderdaad een symmetriegroep, in de betekenis van de inleiding, die bekend staat als *de cirkelgroep* (soms moet je het, in tegenstelling tot je sleutels waarvan je weer eens vergeten bent waar je die gelegd hebt, echt niet ver zoeken). Merk op dat deze cirkelgroep U(1) en

[10] Omdat we straks punten in de ruimte nodig hebben, die we coördinaten (x, y, z) zullen geven, zullen we nooit de letter z gebruiken voor complexe getallen in deze bundel. Voor getallen in $\mathbb{C}$ nemen we kleine Griekse letters, zoals ζ of ξ.

de rotatiegroep SO(2) *isomorfe groepen* zijn.

Oefening 2.9: *ga na dat de afbeelding*

$$\varphi : \mathrm{U}(1) \to \mathrm{SO}(2,\mathbb{R}) : e^{i\theta} \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

een groepsmorfisme is. Verklaar ook waarom het een isomorfisme is, door na te gaan dat het verband tussen ξ en de bijhorende matrix $\varphi(\xi)$ een bijectief verband is.

We zouden ons nu kunnen afvragen of we deze efficiënte manier om naar rotaties te kijken kunnen veralgemenen van 2 naar meer dimensies. Dit kan uiteraard — onderschat nooit de wiskunde — maar we zullen ons in deze bundel beperken[11] tot de stap van 2 naar 3. Jammer genoeg zal deze stap meer voeten in de aarde hebben dan de gemiddelde groenteboer. Om te beginnen moeten we een manier zoeken om de relatie $x^2 + y^2 = |\zeta|^2$ uit te breiden, waarbij we dus $x^2 + y^2 + z^2$ willen herschrijven. Met één complex getal zullen we hier nooit genoeg hebben, omdat we links van de gewenste gelijkheid met 3 reële parameters zitten, maar met 2 complexe getallen hebben we dan weer teveel[12]. Dus ja, wat nu?

Er zijn nu 2 manieren om verder te gaan:

- Ofwel denk je zoals de wiskundige Sir William Rowan Hamilton, de Ierse wiskundige die bekend staat als de vader van de quaternionen. Dat zijn de 'getallen' die gezien worden als de veralgemening[13] van de complexe getallen naar hogere dimensie. Ook hij worstelde destijds met de vraag van hierboven — dus ja, wat nu — en zijn geniale inzicht was dat je van 2 dimensies naar 4 moest gaan om 'de juiste' aanpak te vinden.
- Ofwel merk je op dat we kunnen starten van 2 complexe getallen, laten we ze ζ_1 en ζ_2 noemen, en verzinnen we dan wel een manier om één van de parameters in die getallen *kwijt* te spelen. Dat moeten we uiteraard doen, omdat $|\zeta_1|^2 + |\zeta_2|^2$ een som is van 4 reële parameters (in het kwadraat), en dat is er dus eentje te veel. Merk overigens op dat die manier uiteraard equivalent zal zijn met wat Hamilton destijds deed, alleen zullen we het niet per se expliciet zo benoemen.

[11] Wie er echt niet genoeg van kan krijgen kan terecht in de wereld van de spingroepen.

[12] Mensen met een achtergrond in de jeugdbeweging denken nu ongetwijfeld aan de klassieker '2 is te weinig, 3 is teveel'.

[13] We kozen hier voor aanhalingstekens omdat je kan filosoferen over de vraag of quaternionen wel getallen zijn. Een zeer boeiende vraag natuurlijk, al was het maar omdat veel mensen ook vraagtekens zouden plaatsen bij imaginaire getallen als 'getallen'.

Hoewel er zeker iets te zeggen is voor het gebruik van quaternionen, al was het maar omdat dit een pad is dat snel veralgemeend kan worden naar dimensies hoger dan 3 (of 4, het is te zien hoe je het bekijkt), zullen we in deze bundel kiezen voor de tweede aanpak. Laten we dus om te beginnen volgende notaties vastleggen:

$$\zeta_1 = a_1 + ib_1 \qquad \text{en} \qquad \zeta_2 = a_2 + ib_2 \ ,$$

met dan uiteraard a_j en $b_j \in \mathbb{R}$. Verder zullen we zien hoe deze letters in verband staan met de coördinaten (x, y, z) van een punt in de ruimte $\mathbb{R}^3$. Omdat we intussen de kracht van matrices kennen, zullen we nu proberen om alles zodanig te formuleren dat die vanzelf naar boven komen. Om te beginnen merken we dan op dat

$$(\zeta_1^c, \zeta_2^c)(\zeta_1, \zeta_2)^T = |\zeta_1|^2 + |\zeta_2|^2 = a_1^2 + b_1^2 + a_2^2 + b_2^2 \in \mathbb{R} \ ,$$

waarbij we de notatie $\zeta^c = x - iy$ gebruiken voor de complex toegevoegde[14] van een complex getal $\zeta = x + iy$. Als we dan willen dat $|\zeta_1|^2 + |\zeta_2|^2$ niet verandert, dan kunnen we dus met een gerust hart transformaties van de vorm $(\zeta_1, \zeta_2)^T \to M(\zeta_1, \zeta_2)^T$ beschouwen, met M een matrix in $\mathbb{C}^{2\times 2}$, op voorwaarde dat die matrix voldoet aan $M^\dagger M = \mathrm{Id}_2$. Hierbij staat de zogenaamde *dagger* (of Hermitisch toegevoegde) voor de combinatie van transponeren *en* complex toevoegen. Anders gezegd:

$$\begin{pmatrix} \zeta_1 & \zeta_2 \\ \zeta_3 & \zeta_4 \end{pmatrix}^\dagger = \begin{pmatrix} \zeta_1^c & \zeta_3^c \\ \zeta_2^c & \zeta_4^c \end{pmatrix} \ .$$

Omdat het cruciaal is dat je inziet waar die voorwaarde vandaan komt doen we het even expliciet: als de (complexe) kolomvector $(\zeta_1, \zeta_2)^T \in \mathbb{C}^2$ transformeert tot $M(\zeta_1, \zeta_2)^T$, dan transformeert het getal $|\zeta_1|^2 + |\zeta_2|^2$ als volgt:

$$(\zeta_1^c, \zeta_2^c)(\zeta_1, \zeta_2)^T \mapsto (\zeta_1^c, \zeta_2^c) M^\dagger M (\zeta_1, \zeta_2)^T \ ,$$

zodat we zien dat het getal inderdaad niet verandert als $M^\dagger M = \mathrm{Id}_2$.

Oefening 2.10: *toon aan dat de verzameling van alle matrices $M \in \mathbb{C}^{2\times 2}$ die aan de voorwaarde $M^\dagger M = M M^\dagger = \mathrm{Id}_2$ voldoen inderdaad een groep vormt.*

Omdat groepen als kinderen zijn — je geeft ze best een naam als je ze enigszins onder controle wil kunnen houden — voeren we voor bovenstaande groep ook een eigen symbool in:

[14] Een andere vaak gebruikte notatie is $\overline{\zeta}$ (vertikale streep boven het getal).

$$\boxed{\mathrm{U}(2) := \{M \in \mathbb{C}^{2\times 2} : M^\dagger M = M M^\dagger = \mathrm{Id}_2\}}$$

Merk op dat $M^\dagger M = \mathrm{Id}_2 \Rightarrow |\det(M)|^2 = 1$, en dat betekent dus dat we een voor de hand liggende deelgroep kunnen maken door enkel die matrices in U(2) te selecteren waarvan de determinant *exact* gelijk is aan 1 (dus niet zomaar $\det(M) = e^{i\theta}$, een determinant met modulus 1). De goede verstaander heeft hopelijk door dat dit lijkt op wat we deden met de orthogonale matrices, waar we in de groep O(2) konden kiezen voor die matrices waarvoor $\det(M) = 1$. Die analogie ligt zodanig hard voor de hand dat we op eenzelfde manier tot een bijhorende notatie komen:

$$\boxed{\mathrm{SU}(2) := \{M \in \mathrm{U}(2) : \det(M) = 1\}}$$

Oefening 2.11: *om tot de meest algemene gedaante van een matrix M in $SU(2)$ te komen*[15] *kan je vertrekken van een willekeurige matrix*

$$M = \begin{pmatrix} \zeta_1 & \zeta_2 \\ \zeta_3 & \zeta_4 \end{pmatrix} \in \mathbb{C}^{2\times 2}$$

en dan eisen dat $M^\dagger M = M M^\dagger = \mathrm{Id}_2$ en $\det(M) = 1$. Doe dit expliciet, en toon daarmee aan dat elke matrix in $SU(2)$ zich herleidt tot een matrix van de vorm

$$M = \begin{pmatrix} \zeta_1 & \zeta_2 \\ -\zeta_2^c & \zeta_1^c \end{pmatrix}$$

met de bijkomende voorwaarde dat $|\zeta_1|^2 + |\zeta_2|^2 = 1$.

Op dit moment hebben we nu de wiskundige objecten te pakken die we kunnen zien als de veralgemening van de 'rotaties' $\xi = e^{i\theta}$ die we konden gebruiken in het vlak. Dat zijn dus de matrices in SU(2) die we net ingevoerd hebben. Alleen moeten we nu nog verklaren op welke manier die matrices ons kunnen helpen om een vector in $\mathbb{R}^3$ te roteren. Soms loont het de moeite om iets te doen wat niet werkt, omdat dit ons kan helpen om in te zien waarom we dieper moeten ploeteren in de wiskundige moerassen. Het geeft bovendien wat intuïtief inzicht in de kracht van invariantie, en hoe dit vanzelf opduikt in de wereld van de groepen en haar toepassingen. Je zou namelijk als volgt kunnen redeneren:

- We weten dat een complexe kolom $(\zeta_1, \zeta_2)^T$ naar een nieuwe complexe kolom gaat, via de transformatie

$$(\zeta_1, \zeta_2)^T \mapsto M(\zeta_1, \zeta_2)^T \ ,$$

[15] Deze oefening vergt een beetje goochelen met vergelijkingen complexe getallen. Wie daar geen zin in heeft kan deze opgave gerust negeren.

en dat deze transformatie zelfs de waarde $|\zeta_1|^2 + |\zeta_2|^2 \in \mathbb{R}$ zal bewaren. We kiezen hier dan uiteraard voor een transformatie M in SU(2).

- Als we 2 complexe getallen ter beschikking hebben, dan uiteraard ook 4 reële getallen. Kunnen we dan niet gewoon *kiezen*[16] voor pakweg $\zeta_1 \in \mathbb{C}$ (dat zijn al 2 reële parameters) en dan $\zeta_2 \in \mathbb{R}$ (da's dan onze resterende reële parameter)? Dus we verzinnen gewoon een makkelijke manier om 1 van de 4 reële parameters in (ζ_1, ζ_2) weg te werken. Het probleem is dat dit nooit zal werken, om de simpele reden dat onze transformatie die eigenschap niet bewaart. Kijk maar naar onderstaand product:

$$\frac{1}{2}\begin{pmatrix} i & 1 \\ -1 & -i \end{pmatrix}\begin{pmatrix} p+iq \\ r \end{pmatrix} = \frac{1}{2}\begin{pmatrix} (r-q)+ip \\ -p-i(q+r) \end{pmatrix} .$$

  Wat we hier kunnen zien is dat een kolommetje met $\zeta_2 \in \mathbb{R}$ hier *niet* wordt afgebeeld op een nieuw kolommetje $(\zeta_1', \zeta_2')^T$ waarbij ook $\zeta_2' \in \mathbb{R}$. Wat dit ons leert is dat we dus *geen* goeie manier gevonden hebben om M in SU(2) te laten inwerken, omdat onze zelf verzonnen identificatie tussen $\mathbb{R}^3$ en $(\zeta_1, \zeta_2)^T$ die voldoen aan een bijkomende voorwaarde niet werkt.

De moeilijkheid bestaat er dus in om op de juiste manier twee complexe getallen $(\zeta_1, \zeta_2)^T \in \mathbb{C}^2$ te associëren aan vectoren in $\mathbb{R}^3$, zodanig dat de inwerking van $N \in \mathrm{SU}(2)$ op die complexe getallen nog op dezelfde werkwijze kan geassocieerd worden aan een vector in $\mathbb{R}^3$. We willen dus het volgende pad kunnen doorlopen:

$$\boxed{(x,y,z) \xrightarrow{\kappa} (\zeta_1,\zeta_2)^T \xrightarrow{N} (\zeta_1',\zeta_2')^T \xrightarrow{\rho} (x',y',z')}$$

waarbij we κ kozen voor dat 'kopietje' en ρ voor de 'restrictie' (een *retrieval of information*, zo kan je het ook noemen).

2.3 Drie is vier min één (voor gevorderden)

Verrassend genoeg zit het antwoord in de groep SU(2) zelf! Als we namelijk even terugkeren naar de algemene gedaante voor een matrix in die groep, dan zien we dat dit van de volgende vorm is (zie de laatste oefening

[16] Merk op dat er talloze andere keuzes zijn, zoals $\zeta_1 \in i\mathbb{R}$ zuiver imaginair en $\zeta_2 \in \mathbb{C}$. De essentie is dat we telkens een manier vastleggen om één van de reële parameters kwijt te spelen.

hierboven):

$$M = \begin{pmatrix} a_1 + ib_1 & a_2 + ib_2 \\ ib_2 - a_2 & a_1 - ib_1 \end{pmatrix} \in \mathrm{SU}(2) \ ,$$

op voorwaarde dat $a_1^2 + b_1^2 + a_2^2 + b_2^2 = 1$. We zijn het niet gewoon om na te denken over sferen in dimensie 4, maar wat hierboven staat is dat we een matrix in SU(2) kunnen identificeren met een punt $p(a_1, b_1, a_2, b_2)$ op de eenheidssfeer $S^3 \subset \mathbb{R}^4$. Net zoals de eenheidssfeer $S^2 \subset \mathbb{R}^3$ kan gezien worden als een (oneindige) verzameling breedtecirkels — van pool (als punt dus een ontaarde cirkel) naar evenaar (met maximale straal) en weer terug naar pool — kunnen we S^3 ook zien als een oneindige verzameling *breedtesferen*. Van pool (als punt een ontaarde sfeer) naar 'evenaar' (deze keer dus de sfeer S^2 met maximale straal) en weer terug naar pool. Die 'evenaar' speelt hier een cruciale rol, dus laten we die er even uitpikken. We zullen dat doen op een bijzondere manier, door eerst op te merken dat de parameter a_1 een speciale rol speelt. Dat lijkt op het eerste zicht niet zo, je zou denken dat de relatie $a_1^2 + b_1^2 + a_2^2 + b_2^2 = 1$ alle 4 reële parameters op gelijke voet behandelt, maar dat is slechts schijn. Je kan namelijk makkelijk zien dat de *trace* (het spoor) van de matrix M gelijk is aan

$$\mathrm{tr}(M) = \mathrm{tr} \begin{pmatrix} a_1 + ib_1 & a_2 + ib_2 \\ ib_2 - a_2 & a_1 - ib_1 \end{pmatrix} = 2a_1 \ .$$

Omdat $a_1 \in [-1, +1]$, ga voor jezelf na waarom dit zeker waar is, zouden we dus kunnen zeggen dat elke *breedtesfeer* vastegelegd wordt door een a_1 te kiezen. In het bijzonder kunnen we dus $a_1 = 0$ stellen, wat dan overeen komt met de 'evenaar'. Dit kan je intuïtief inzien, omdat $a_1 = 0$ halfweg tussen $a_1 = \pm 1$ zit zoals ook de 'evenaar' halfweg tussen de polen zit, of gewoon strak wiskundig: als $a_1 = 0$ dan voldoen de resterende parameters aan de voorwaarde $b_1^2 + a_2^2 + b_2^2 = 1$, wat inderdaad de conditie is om op een eenheidssfeer S^2 in $\mathbb{R}^3$ te liggen. We zijn er dan bijna, omdat we *elk* punt $(x, y, z) \neq (0, 0, 0)$ in de ruimte $\mathbb{R}^3$ (zonder de oorsprong) kunnen schrijven als

$$(x, y, z) = R(b_1, a_2, b_2) \in \mathbb{R}^+ \times S^2 \ .$$

Inderdaad, neem een punt (x, y, z) en verbind het met de oorsprong: daar waar de halfrechte die beide punten verbindt (vanuit de oorsprong naar oneindig) de sfeer S^2 snijdt vind je een punt $(b_1, a_2, b_2) \in S^2$. Het getal R heb je nog nodig om langs die halfrechte te bewegen tot je in het punt (x, y, z) zit (in technische termen: een dilatatie). Hopelijk is het ook duidelijk dat het uitsluiten van de oorsprong hier niet erg is: we weten dat dit punt sowieso zal blijven liggen (denk aan rotaties in het vlak), we komen

hier later nog wel op terug. Als we er even de notaties van voorheen bijhalen, dan is het misschien duidelijk dat we nu de afbeelding κ gevonden hebben:

$$(x,y,z) = R(b_1,a_2,b_2) \xrightarrow{\kappa} R\begin{pmatrix} ib_1 & a_2+ib_2 \\ ib_2-a_2 & -ib_1 \end{pmatrix} \in \mathbb{R}^+ \times \mathrm{SU}(2)\ .$$

De goede verstaander heeft misschien zelfs gezien dat we hier stiekem gedaan hebben wat eigenlijk een slecht idee leek: we hebben (ζ_1,ζ_2) zodanig gekozen dat $\zeta_1 \in i\mathbb{R}$, wat inderdaad één van de totaal arbitraire manieren is om een reële parameter kwijt te spelen. *Waarom is dit plots een goed idee dan?* Wel, het heeft allemaal te maken met het feit dat we *niet* zomaar kozen voor de afbeelding

$$(x,y,z) = R(b_1,a_2,b_2) \xrightarrow{\kappa} (\zeta_1,\zeta_2) = R(ib_1,a_2+ib_2)\ ,$$

wat nochtans min of meer op hetzelfde neerkomt[17]. Het enige wat we anders deden is dat we (x,y,z) *niet* zomaar hebben afgebeeld op een element van $\mathbb{C}^2$ (een kolommetje), maar op een *matrix*. Het kan dan uiteraard niet anders dat matrices een eigenschap moeten hebben die hier *cruciaal* van pas komt, want waar zou anders dat verschil vandaan komen? Wel, door met matrices te werken zijn we inderdaad iets op euh, *het spoor*, want daar ligt de sleutel tot succes. Als we namelijk in herinnering brengen dat de *trace* van een matrix voldoet aan de (cyclische) voorwaarde

$$\mathrm{tr}(ABC) = \mathrm{tr}(BCA) = \mathrm{tr}(CAB)\ ,$$

dan brengt ons dit vanzelf bij de 'juiste' manier waarop we nu zullen moeten transformeren. Inderdaad, als we een willekeurige N in $\mathrm{SU}(2)$ nemen, dan is het zo dat

$$\mathrm{tr}\begin{pmatrix} ib_1 & a_2+ib_2 \\ ib_2-a_2 & -ib_1 \end{pmatrix} = \mathrm{tr}\left(N\begin{pmatrix} ib_1 & a_2+ib_2 \\ ib_2-a_2 & -ib_1 \end{pmatrix}N^{-1}\right) = 0\ .$$

Indrukwekkende formule, dus laten we even rustig ademhalen en samenvatten wat we nu geleerd hebben:

- We kunnen punten in $\mathbb{R}^3 \setminus \{(0,0,0)\}$ op unieke wijze voorstellen als een 'geschaalde spoorloze matrix' in $\mathrm{SU}(2)$. Dus de meest precieze definitie voor onze afbeelding κ ziet er als volgt uit:

$$\boxed{\kappa : \mathbb{R}^3 \setminus \{(0,0,0)\} \to \mathbb{R}_0^+ \times \{M \in \mathrm{SU}(2) : \mathrm{tr}(M) = 0\}}$$

[17] We bedoelen daarmee het volgende: die matrix bevat 'dezelfde informatie', eens je weet wat (ζ_1,ζ_2) is kan je M maken, en andersom!

De oorsprong zelf kunnen we gewoon afbeelden op de nulmatrix[18], dan zijn we daar ook vanaf. Dan hebben we een unieke matrix voor *elk* punt gevonden.

- Bovendien kunnen we κ ook 'inverteren', iets wat we in het vorige hoofdstuk ρ genoemd hebben. Als je een matrix A krijgt, dan is $R = \det(A)$ en dan kunnen we de resterende getallen (b_1, a_2, b_2) gewoon aflezen uit onze matrix nadat we R hebben weggedeeld. Anders gezegd (ga na dat je dit inderdaad kan bevestigen):

$$\boxed{(x, y, z) = \left(-ia_{11}, \frac{a_{12} + a_{12}^c}{2}, \frac{a_{12} - a_{12}^c}{2i}\right)}$$

  waarbij a_{ij} de elementjes in A voorstelt.
- Als we een matrix $N \in \mathrm{SU}(2)$ laten inwerken op de matrix $\kappa(x, y, z)$ via de 'toevoeging'[19] (standaard terminologie voor sandwichen tussen een element en het inverse van dat element), dan weten we zeker dat het resultaat iets zal zijn dat terug een vector in $\mathbb{R}^3$ oplevert, *met eenzelfde lengte*. Inderdaad, er geldt dat $N\kappa(x, y, z)N^{-1}$ terug een getal is (opnieuw diezelfde R) maal een matrix in $\mathrm{SU}(2)$ waarvan de *trace* nul is.

Rest ons nog natuurlijk de (veganistische versie voor een) hamvraag: waarom kunnen we deze inwerking van $N \in \mathrm{SU}(2)$ op de 'vectoren' $\kappa(x, y, z)$ zien als *rotaties*? Dat is een belangrijke vraag, omdat we (al dan niet) gewoon zijn om rotaties die inwerken op vectoren in $\mathbb{R}^3$ te zien als matrices in $\mathrm{SO}(3)$. Onze matrices N bevatten niet alleen complexe getallen, ze hebben dan ook nog eens het verkeerde formaat. Opnieuw zijn er 2 manieren om in te zien waarom we de transformatie N echt mogen identificeren met een rotatie: een eenvoudige, en een meer fundamentele. Laten we deze keer met dat laatste beginnen: de inwerking van N is lineair, omdat

$$N\big(R_1M_1 + R_2M_2\big)N^{-1} = N\big(R_1M_1\big)N^{-1} + N\big(R_2M_2\big)N^{-1} \ ,$$

en we merkten eerder al op dat de inwerking van N de lengte van een vector (lees: de afstand tot de oorsprong) invariant laat. Anders gezegd, als we het pad

$$(x, y, z) \in \mathbb{R}^3 \xrightarrow{\kappa} RM \xrightarrow{N} N(RM)N^{-1} \xrightarrow{\rho} (x', y', z') \in \mathbb{R}^3$$

doorlopen, dan zal $x^2 + y^2 + z^2 = (x')^2 + (y')^2 + (z')^2$. *But if it looks and quacks like a duck, then it probably is a duck*: een lineaire transformatie op vectoren die de afstand tot de oorsprong bewaart *is* gewoon een

[18] De gekende Wet van Behoud van Nulligheid.
[19] In hoofdstuk 1 'conjugatie' genoemd

rotatie. Dat zouden we uiteraard ook kunnen testen, door *berekeningen* uit te voeren. Dat zullen we hier niet in volle algemeenheid doen[20], maar we kunnen natuurlijk wel eens een voorbeeld bekijken. Om te beginnen zullen we $(x, y, z) \in S^2$ kiezen, of dus $R = 1$, dat heeft geen enkele impact op de redenering. Voor N zullen we een makkelijke matrix kiezen, zoals bijvoorbeeld een diagonaalmatrix:

$$N_1 = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \in \mathrm{SU}(2) \ .$$

Een eenvoudige berekening leert ons dan dat

$$\begin{aligned} N_1 \begin{pmatrix} ix & y+iz \\ iz-y & -ix \end{pmatrix} N_1^{-1} &= \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \begin{pmatrix} ix & y+iz \\ iz-y & -ix \end{pmatrix} \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} \\ &= \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \begin{pmatrix} ixe^{-i\theta} & e^{i\theta}(y+iz) \\ e^{-i\theta}(iz-y) & -ixe^{i\theta} \end{pmatrix} \\ &= \begin{pmatrix} ix & e^{2i\theta}(y+iz) \\ e^{-2i\theta}(iz-y) & -ix \end{pmatrix} \ . \end{aligned}$$

Zoals we kunnen zien krijgen we nu opnieuw een matrix met *trace* gelijk aan nul (dat moest uiteraard), maar we kunnen nu ook makkelijk zien waar onze vector (x, y, z) beland is na de inwerking van N door de inverse operatie ρ los te laten op de laatste matrix. Dan vinden we dus:

$$(x, y, z) \mapsto \big(x, y\cos 2\theta - z\sin 2\theta, y\sin 2\theta + z\cos 2\theta\big) \ .$$

Anders gezegd: de inwerking van onze specifieke N_1 op $\kappa(x, y, z)$ komt overeen met een rotatie rond de X-as (want $x' = x$) over een hoek 2θ. Dat is op zijn minst gezegd verrassend, omdat de matrix N het getal $e^{i\theta}$ bevat, iets dat we eerder associëren met een rotatie over een hoek θ. Omdat die hoek in de exponent staat zouden we ergens kunnen stellen dat N als het ware de (vierkants)wortel uit een rotatie voorstelt. Dat intuïtieve beeld kunnen we ook formeel onderbouwen, dat is voer voor de laatste sectie.

Oefening 2.12: *Hierboven hebben we een bijzondere diagonaalmatrix N beschouwd, maar daarmee kunnen we uiteraard niet alle rotaties in $\mathbb{R}^3$ beschrijven. Werk ook eens de situatie uit voor volgend geval:*

$$N_2 = \begin{pmatrix} 0 & e^{i\theta} \\ -e^{-i\theta} & 0 \end{pmatrix} \ .$$

Herken je de bijhorende rotatie?

[20] Bovendien kunnen ze omzeild worden, in die zin dat je in zekere zin met een kort argument kan verklaren waarom 1 berekening zal volstaan, maar daar gaan we niet dieper op in.

2.4 De kracht van wortels

Laten we om te beginnen eerst even proberen om 'de klassieke wortelfunctie' te bekijken door de bril van groepen. We voeren daarvoor twee (gekende) groepen in: $G_1 = (\mathbb{R}_0, \times)$ en $G_2 = (\mathbb{R}_0^+, \times)$. Daarnaast stellen we

$$\sigma : G_1 \to G_2 : x \mapsto \sigma(x) := x^2 \ .$$

Het is makkelijk in te zien dat dit een groepsmorfisme is, omdat we uiteraard hebben dat

$$\sigma(ab) = (ab)^2 = a^2b^2 = \sigma(a)\sigma(b) \ .$$

Wat dit morfisme zo speciaal maakt, is dat de groep G_1 als het ware 'twee kopietjes' van de groep G_2 bevat[21]. Als je de groep G_1 visueel voorstelt als de reële rechte waaruit de oorsprong is weggeprikt, dan zou je kunnen zeggen dat σ als het ware het 'dichtklappen' is van die rechte, waarbij je de linkerhelft (de negatieve getallen) over de rechterhelft legt (de positieve getallen), gevolgd door 'een kwadratisch uitrekken'. Wat daarbij vooral bijzonder is, is dat je $x = -1$ eerst op $x = +1$ klapt, en dat dit punt dan als het ware blijft liggen (omdat, *here's a knowledge bomb for you*, $(\pm 1)^2 = 1$). Dit is bijzonder, omdat het in essentie zegt dat de getallen $x = \pm 1$ worden afgebeeld op het eenheidselement in G_2. Bovendien is $(\{-1, +1\}, \times) < G_1$ ook een deelgroep[22]. Het zou ons nu net iets te ver brengen om ook het theoretische concept van 'normale deelgroepen' en 'quotiëntgroepen' in te voeren, maar we kunnen wel enkele nuttige dingen opmerken die enkel steunen op het concept van groepsmorfismen. Zo kunnen we volgende zogenaamde *exact sequence* beschouwen:

$$\boxed{(\{1\}, \times) \longrightarrow (\{-1, +1\}, \times) \longrightarrow (\mathbb{R}_0, \times) \longrightarrow (\mathbb{R}_0^+, \times) \longrightarrow (\{1\}, \times)}$$

waarbij elke pijl komt met een eigen morfisme (uitstekende kans om je Griekse alfabet te oefenen). Als we nu *de kern van een morfisme* (tussen 2 groepen) definiëren als de verzameling van alle elementen in de eerste groep die worden afgebeeld op het eenheidselement van de tweede groep, dan kan je iets heel bijzonder opmerken in bovenstaande configuratie. Daarvoor halen we er een 'atoom' aan informatie uit:

$$\boxed{G \xrightarrow{\phi} H \xrightarrow{\psi} K}$$

[21] Niet letterlijk natuurlijk, omdat G_1 ook negatieve getallen bevat.
[22] Bonuspunten voor wie spontaan aan C_2 denkt nu.

Voor elke keuze van (G, H, K) hierboven — en hopelijk zie je meteen in dat er zo 3 keuzes te maken zijn — is het zo dat $\phi(G)$ door ψ wordt afgebeeld op het eenheidselement in K. Je kan dat inderdaad testen voor de 'atomen'

$$\begin{aligned}
(\{1\}, \times) &\xrightarrow{\iota} (\{-1, +1\}, \times) \xrightarrow{\iota} (\mathbb{R}_0, \times) \\
(\{-1, +1\}, \times) &\xrightarrow{\iota} (\mathbb{R}_0, \times) \xrightarrow{\sigma} (\mathbb{R}_0^+, \times) \\
(\mathbb{R}_0, \times) &\xrightarrow{\rho} (\mathbb{R}_0^+, \times) \xrightarrow{\alpha} (\{1\}, \times) \ ,
\end{aligned}$$

waarbij we 3 Griekse letters hebben gekozen: de iota ι staat voor 'inbedding', een technisch woord om gewoon te zeggen dat je elke element 'naar zichzelf' stuurt, de σ van eerder (het kwadraat, of *square*) en de α die staat voor 'alles naar 1 sturen' (dat laatste morfisme voelt wat vreemd, maar werkt wel, omdat je gewoon alles naar het eenheidselement 1 stuurt). Hoog tijd om deze abstracte boterham even door te spoelen met een concrete toepassing, en daarvoor keren we uiteraard terug naar de hoofdrolspelers van onze workshop. Want de essentie van bovenstaand verhaal is dat er zoiets bestaat als de *exact sequence*

$$\boxed{(\{1\}, \times) \longrightarrow (\{-1, +1\}, \times) \longrightarrow (\mathrm{SU}(2), \times) \longrightarrow (\mathrm{SO}(3), \times) \longrightarrow (\{1\}, \times)}$$

Het bestaan van deze configuratie, en het feit dat die er (pun non-intended) exact hetzelfde uitziet als die voor de klassieke wortelfunctie, is de reden waarom men soms wel eens de boerenwijsheid *'de groep SU(2) bevat de wortels van de rotatiegroep SO(3)'* in de mond neemt. De essentie van die *sequence* zit uiteraard in het atoom

$$\boxed{(\{-1, +1\}, \times) \longrightarrow (\mathrm{SU}(2), \times) \longrightarrow (\mathrm{SO}(3), \times)}$$

Laten we de twee pijlen in detail beschrijven:

- De eerste stuurt simpelweg ± 1 (als getallen) naar de matrices $\pm \mathrm{Id}_2$ in SU(2). Het belangrijkste hier is dat je inziet dat beide matrices inderdaad in SU(2) zitten (merk op dat $\det(-\mathrm{Id}_2) = 1$).
- De tweede pijl stuurt *plus en min* een matrix $N \in \mathrm{SU}(2)$ naar *dezelfde* rotatie in SO(3), waarbij je natuurlijk het vorige hoofdstuk nodig hebt om te weten welke rotatie dat precies is. Zo hebben we bijvoorbeeld dat

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos 2\theta & -\sin 2\theta \\ 0 & \sin 2\theta & \cos 2\theta \end{pmatrix}$$

Absoluut *cruciaal* hier is dat N en $-N$ *hetzelfde* beeld hebben (denk aan vierkantswortels), wat je makkelijk kan inzien door op te merken dat

$$N \begin{pmatrix} ix & y+iz \\ iz-y & -ix \end{pmatrix} N^{-1} = (-N) \begin{pmatrix} ix & y+iz \\ iz-y & -ix \end{pmatrix} (-N)^{-1} \ .$$

Omdat de matrix N 'aan beide kanten staat' (weliswaar éénmaal met een inverse) zien we inderdaad dat het eventuele minteken ook twee keer voorkomt en dus geen impact heeft!

Bij deze is alvast één cruciale eigenschap van de groep SU(2) toegelicht. Wie zich afvraagt of dit verhaal ook geldt in hogere dimensie stelt een goeie vraag, maar is iets vergeten: onderschat werkelijk *nooit* de wiskunde. Dat is namelijk exact wat de fameuze *spingroepen* zijn, 'wortels' uit $\mathrm{SO}(m)$ voor $m \geq 4$.

2.5 Het mysterie van de spinor

Eén van de meest fascinerende wiskundige objecten is de spinor. Niet mijn woorden, het was Sir Michael Atiyah[23] die ooit liet optekenen:

No one fully understands spinors. Their algebra is formally understood but
their general significance is mysterious. In some sense they describe the 'square root' of geometry and, just as understanding the square root of -1 *took centuries, the same might be true of spinors...*

Er valt zeer veel te vertellen over spinoren en hun meetkundige interpretatie — wie er een boompje over wil opzetten op een receptie kan pakweg de auteur van deze bundel eens aanspreken — maar daar hebben we tijd noch ruimte voor. Al kunnen we wel op zijn minst proberen om de zinsnede *'their algebra is formally understood'* toe te lichten. Het basisidee is op zich niet zo moeilijk, als je de volgende bedenkingen maakt:

- Matrices N in SU(2) kan je opvatten als rotaties *op vectoren*, al moet je dan wel het (steile) pad bewandelen dat je van een klassieke vector $(x, y, z) \in \mathbb{R}^3$ naar een 'geschikte voorstelling' brengt. Dat laatste hebben we gedaan via twee complexe getallen $(\zeta_1, \zeta_2)^T \in \mathbb{C}^2$, *maar* dat vergde wel het absoluut niet zo triviale inzicht dat we die complexe getallen in een matrix moesten gieten. Eens we dat gerealiseerd hadden vonden we wel min of meer 'vanzelf' (wie houdt

[23] Fields Medal winnaar in 1966, een referentie waar je al eens mee kan thuiskomen.

er nu niet van een welgemikt eufemisme?) dat de inwerking van N dan liep via de toevoeging $N[\cdot]N^{-1}$.

- Los van alle inhoudelijke details werkt bovenstaand mechanisme, omdat we binnen de verzameling $\mathbb{C}^{2\times 2}$ zitten te werken. Vierkant maal vierkant, complex maal complex. Dat werkt perfect, geen verdere klachten hier. Maar waarom zouden we het überhaupt zo ver zoeken? Als iemand jou een element van SU(2) geeft[24], dan krijg je in essentie een element in $\mathbb{C}^{2\times 2}$. Als dit nu moet inwerken op 'een vector', dan denk ik spontaan aan de meest natuurlijke vectorruimte waarop die matrix kan inwerken, en dat is uiteraard gewoon $\mathbb{C}^2$ zelf, niet? Wel, dat is de algebra van de spinoren. Klaar.

Je zou namelijk kunnen zeggen dat een spinor een element $(\eta_1, \eta_2)^T$ is van de ruimte $\mathbb{C}^2$, en dan is het hopelijk meteen duidelijk dat (linkse) vermenigvuldiging met N in SU(2) inderdaad een spinor omzet in een spinor. Op het gevaar van misplaatste arrogantie af: *that's it.* Algebraïsch valt er in feite niet veel meer over te vertellen. Behalve dan misschien de verklaring waarom er ook een andere boerenwijsheid is die zegt dat *spinoren moeten roteren over een hoek van* 4π *voor ze terug zijn bij hun beginpositie.* Het idee daarachter is gelukkig niet zo moeilijk meer, omdat we al het voorbereidende werk gedaan hebben. Als we namelijk N_1 kiezen voor $\theta = \pi$, of dus een matrix $N = -\mathrm{Id}_2$, dan weten we dat de impact op een 'klassieke vector' in $\mathbb{R}^3$ zal zijn dat, wel ja, dat er geen impact is. We weten immers reeds dat een matrix N overeenkomt met een rotatie over *de dubbele hoek*, en een rotatie over 2π is gewoon de identieke transformatie (wat de as van de rotatie ook moge zijn). Maar een spinor gaat wel degelijk de impact voelen: er geldt namelijk dat

$$\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} \to N \begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} = \begin{pmatrix}-\eta_1\\ -\eta_2\end{pmatrix} \ ,$$

waarbij de mintekens erop wijzen dat die spinor eigenlijk gepuntspiegeld werd t.o.v. de oorsprong. Anders gezegd: als we (uiteraard) *eenzelfde* matrix N in SU(2) gebruiken om in te werken op een spinor in $\mathbb{C}^2$ dan wel op een vector (x, y, z) in $\mathbb{R}^3$ (na inwerken van κ et cetera), dan zal die spinor 'roteren' over de helft van de hoek waarover de vector roteert. Let op het selectieve gebruik van aanhalingstekens hier: dat onderstreept in feite het eerder *meetkundige* mysterie van spinoren. Bij rotaties denken mensen namelijk spontaan aan een draaimolen, of een tol, of de wieken van een drone of zo. Met een beetje geluk heb je zelfs de as van die rotatie en een hoek in je gedachten. Maar bij het 'roteren' van een spinor kunnen

[24]Hopelijk niet voor je verjaardag, want een leuk cadeau zou ik het toch niet noemen.

we ons niet zoveel voorstellen, en de reden daarvoor is een zekere vorm van 'vooringenomenheid'. We zijn zodanig gewoon — als mens, wezens die in 3 dimensies opgroeien en leven — om over rotaties na te denken van 'gewone vectoren' (want het kan ook in het vlak uiteraard, het hoeft niet in de ruimte te zijn) dat we ons bij spinoren niets kunnen voorstellen.

Tot slot nog even iets over katten. Je zou namelijk moeten(?) weten dat $\mathbb{C}^2$ een vectorruimte is van dimensie 2 (over $\mathbb{C}$, dat wil zeggen als je lineaire combinaties met complexe getallen mag maken), met pakweg

$$\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} = \eta_1 \begin{pmatrix}1\\ 0\end{pmatrix} + \eta_2 \begin{pmatrix}0\\ 1\end{pmatrix} \ .$$

De speciale kolommetjes rechts herkent iedereen vermoedelijk als de elementen van 'een (canonische) basis', en als we onze intussen favoriete matrix N_1 erbij halen dan zien we dat

$$N_1 \begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}e^{i\theta}\\ 0\end{pmatrix} \qquad \text{en} \qquad N_1 \begin{pmatrix}0\\ 1\end{pmatrix} = \begin{pmatrix}0\\ e^{-i\theta}\end{pmatrix} \ .$$

Los van de vraag waarom de matrix N_1 blijkbaar zo belangrijk is (absolute kenners bereiden alvast een antwoord voor met Cartan algebra's en zo), valt hier op dat onze basiselementen verschillend reageren op de 'rotatie' N_1. Dat verschil zit trouwens niet in de *grootte* van de hoek, maar in de *oriëntatie* van de hoek. Daar waar de eerste basisvector in tegenwijzerzin 'roteert', zal de andere in wijzerzin 'roteren'. En dan is het gewoon een kwestie van geschikte metaforen kiezen: positief of negatief, zwart of wit, *up or down*, dood of levend. Jawel, de onfortuinlijke kat van Schrödinger, het beest dat werd gekozen als beeld voor de spinor

$$\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} = \eta_1 \begin{pmatrix}1\\ 0\end{pmatrix} + \eta_2 \begin{pmatrix}0\\ 1\end{pmatrix} \ .$$

Links staat onze kat, rechts staat een lineaire combinatie van dood en levend. Merk op dat η_1 en η_2 *complexe* getallen zijn, dus het is moeilijk om dit te lezen als 'zoveel procent dood' versus 'zoveel procent levend'. Tenzij je afspreekt dat je vectoren $(\eta_1, \eta_2)^T \in \mathbb{C}^2$ kiest waarvoor *de modulus* van de getallen voldoet aan $|\eta_1|^2 + |\eta_2|^2 = 1$. Dan kunnen we op zijn minst zeggen dat we eigenlijk met waarschijnlijkheden te maken hebben. En zo zitten we recht in het hart van de quantumfysica.

3 De paradox van Banach-Tarski

Stefaan Vaes en Anna Vanden Berghe

Inleiding

Precies 100 jaar geleden publiceerden Stefan Banach en Alfred Tarski het artikel

> **Sur la décomposition des ensembles de points en parties respectivement congruentes.**
>
> Par
>
> St. Banach (Lwów) et A. Tarski (Varsovie).

in het zesde volume van het Poolse tijdschrift *Fundamenta Mathematicae*. Dat tijdschrift bestaat honderd jaar later trouwens nog steeds en publiceert in de zomer van 2024 volume 265.

Het artikel [BT24] start meteen met de volgende bondige formulering van de hoofdresultaten.

> *Dans un espace euclidien à $n \geqslant 3$ dimensions deux ensembles arbitraires, bornés et contenant des points intérieurs (p. ex. deux sphères à rayons différents), sont équivalents par décomposition finie.*
>
> *Un théorème analogue subsiste pour les ensembles situés sur la surface d'une sphère; mais le théorème correspondant concernant l'espace euclidien à 1 ou 2 dimensions est faux.*

Een speciaal geval van het eerste luik van deze stelling gaat als volgt. Het is een van de meest fascinerende resultaten uit de wiskunde, vandaag gekend onder de naam "paradox van Banach-Tarski".

Stelling A ([BT24, Théorème 24]). *In de driedimensionale ruimte kan je een massieve bol met een straal van 1 meter in eindig veel stukken verdelen, deze stukken roteren en verschuiven en zo* twee *massieve bollen met* elk *een straal van 1 meter bekomen.*

Hoewel dit effectief een stelling is, met een volledig rigoureus bewijs, staat

dit toch gekend als een paradox. De uitspraak is immers volledig in tegenspraak met onze intuïtie.

Merk daarenboven op dat de formulering van Banach en Tarski nog algemener is. Zij nemen *willekeurige* deelverzamelingen U en V van de driedimensionale ruimte met de volgende eigenschappen.

- U en V zijn niet te groot: ze hebben een eindige diameter.
- U en V zijn niet te klein: U en V omvatten allebei minstens een klein bolletje.

Vervolgens bewijzen ze dat je U in eindig veel stukken kan verdelen, deze stukken kan roteren en verschuiven, om zo V te bekomen.

Wij zullen in deze lessen alleen het speciale geval van Stelling A behandelen. Dit is het geval waarbij U een massieve bol met een straal van 1 meter is en V de unie van twee massieve bollen met elk een straal van 1 meter is. De volledig algemene Stelling van Banach-Tarski behandelen we in de uitbreiding in paragraaf 3.3.5.

Het mysterie is echter nog groter. Het tweede luik van de stelling die Banach en Tarski bewezen in [BT24] zegt dat een analoge uitspraak in het tweedimensionale vlak niet waar is!

Stelling B ([BT24, Théorème 16])**.** *In het tweedimensionale vlak is het* niet mogelijk *om een schijf met een straal van 1 meter in eindig veel stukken te verdelen, deze stukken te roteren en te verschuiven en zo twee schijven met elk een straal van 1 meter te bekomen.*

In deze reeks van vier werkcolleges zullen we een bewijs schetsen van Stelling A en Stelling B, gebruikmakend van groepentheorie en de inleiding hierop die eerder door Jeroen Spandaw gegeven werd. De eerste drie lessen gaan over de eigenlijke paradox, Stelling A, en de laatste les gaat over Stelling B. De paragrafen van deze cursustekst die gelabeld zijn als "uitbreiding" zullen we niet in de les behandelen.

Tijdens de werkcolleges zullen jullie regelmatig zelf de details van de redeneringen en berekeningen aanvullen, startend van de schema's in deze cursustekst.

Wie na deze lessenreeks meer wil weten over de paradox van Banach-Tarski en over heel wat bijkomende ontwikkelingen in groepentheorie verwijzen we naar het uitstekende boek [TW16]. Voor een meer populairwetenschappelijke en entertainende bespreking van de paradox van Banach-Tarski raden we het boek [Wap05] aan. Deze lessenreeks en cursustekst is in belangrijke mate gebaseerd op hoofdstukken 3 en 12 van [TW16] en op het honoursproject van de tweede auteur, onder begeleiding van de eerste auteur, aan de Faculteit Wetenschappen van de KU Leuven.


Figuur 3.1: Stefan Banach op de bank rechts in gesprek met Otton Nikodym, Kraków. Alfred Tarski waakt als tweede van rechts over de Universiteitsbibliotheek van Warschau.

Wat voorbereiding of voorkennis

We zullen in deze lessenreeks gebruikmaken van de volgende concepten. Enige vertrouwdheid hiermee is nuttig om de lessenreeks zo vlot mogelijk te volgen.

(i) Rotaties van de driedimensionale en tweedimensionale ruimte spelen een belangrijke rol in deze lessenreeks. Elke rotatie van $\mathbb{R}^3$ met rotatieas door de oorsprong is ook een lineaire transformatie $\rho : \mathbb{R}^3 \to \mathbb{R}^3$ en kan dus voorgesteld worden aan de hand van een 3×3 matrix A:

$$\rho : \mathbb{R}^3 \to \mathbb{R}^3 : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto A \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} .$$

We zullen gebruikmaken van dit verband tussen 3×3 matrices en rotaties van $\mathbb{R}^3$, en ook van het verband tussen 2×2 matrices en lineaire transformaties van $\mathbb{R}^2$.

Zo is bijvoorbeeld

$$\rho = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

de rotatie over een hoek θ met de z-as als rotatieas. In een dergelijke matrixvoorstelling komt het samenstellen en inverteren van rotaties overeen met het vermenigvuldigen en inverteren van de bijhorende matrix.

(ii) We maken voortdurend gebruik van operaties met verzamelingen. Als $A \subset \mathbb{R}^3$ en $B \subset \mathbb{R}^3$ verzamelingen van punten zijn, bekijken we de unie $A \cup B$, de doorsnede $A \cap B$ en het verschil $A \setminus B$. Je kan er hier meer over lezen[1].

(iii) We zullen ook gebruikmaken van het verschil tussen aftelbare en overaftelbare verzamelingen. Je kan er hier[2] en hier[3] meer over lezen. We zullen alleen gebruikmaken van het volgende feit: als C de eenheidscirkel in het vlak is en $x_1, x_2, \ldots$ een rij punten in C is, dan bestaat er nog altijd een punt $x \in C$ dat verschillend is van alle x_n. Met andere woorden: je kan nooit alle punten van de cirkel C opsommen in een rij. De reden hiervoor is dat C overaftelbaar is, terwijl de rij $x_1, x_2, \ldots$ aftelbaar is.

(iv) We maken ten slotte gebruik van modulair rekenen en in ons geval specifiek van rekenen modulo 5. Je kan er hier meer over lezen[4]. Dit betekent concreet dat we zullen rekenen (optellen en vermenigvuldigen) met de getallen 0, 1, 2, 3 en 4 "op veelvouden van 5 na". Zo zal $3 + 4 = 2$ omdat 7 hetzelfde is als 2 op een veelvoud van 5 na. Op dezelfde manier is $3 \times 3 = 4$ omdat 9 hetzelfde is als 4 op een veelvoud van 5 na.

Terminologie

Nogal wat wiskundige terminologie heeft een Vlaamse en een Nederlandse variant. We volgen in deze cursustekst de Vlaamse terminologie. We gebruiken dus het woord *deelgroep* voor *ondergroep* en het woord *actie* (of *groepsactie*) voor *werking* (of *groepswerking*).

[1] nl.wikipedia.org/wiki/Verzameling_(wiskunde)#Operaties
[2] nl.wikipedia.org/wiki/Aftelbare_verzameling
[3] nl.wikipedia.org/wiki/Overaftelbare_verzameling
[4] nl.wikipedia.org/wiki/Modulair_rekenen

Les 1 De stelling die we een paradox noemen

Waarom staat Stelling A gekend als een paradox?

Een eerste redenering om "aan te tonen" dat de Stelling van Banach-Tarski fout is, gaat als volgt. Die eerste massieve bol met een straal van 1 meter heeft een volume van $4\pi/3$ m^3. Zowel bij het opdelen in stukken als bij het verschuiven en roteren van deze stukken blijft het volume bewaard. Maar die twee massieve bollen met elk een straal van 1 meter hebben het dubbele volume van $8\pi/3$ m^3. Dat is een tegenspraak en dus is de stelling fout.

Deze redenering maakt echter een verborgen aanname. Je gaat ervan uit dat het mogelijk is om aan eender welke deelverzameling A van de driedimensionale ruimte $\mathbb{R}^3$ een volume $\text{vol}(A)$ toe te kennen zodanig dat de volgende eigenschappen gelden.

(i) Voor alle $A \subset \mathbb{R}^3$ is $\text{vol}(A)$ een element van $[0, +\infty]$. Merk op dat het logisch is om toe te laten dat sommige deelverzamelingen $A \subset \mathbb{R}^3$ een oneindig volume hebben, bijvoorbeeld de hele ruimte $\mathbb{R}^3$.

(ii) Als $A, B \subset \mathbb{R}^3$ disjunct zijn, dan is $\text{vol}(A \cup B) = \text{vol}(A) + \text{vol}(B)$.

(iii) Als $\theta : \mathbb{R}^3 \to \mathbb{R}^3$ een rotatie of translatie is, dan is $\text{vol}(\theta(A)) = \text{vol}(A)$ voor alle $A \subset \mathbb{R}^3$.

(iv) Als $A \subset \mathbb{R}^3$ een massieve bol met straal 1 is, dan is $\text{vol}(A) = 4\pi/3$.

Een gevolg van Stelling A is dat een dergelijke volumefunctie gewoonweg niet bestaat. Het is onmogelijk om aan alle deelverzamelingen $A \subset \mathbb{R}^3$ een volume $\text{vol}(A)$ toe te kennen zonder een van de bovenstaande eigenschappen te schenden. De reden hiervoor is dat er simpelweg te veel deelverzamelingen van $\mathbb{R}^3$ zijn en te veel rotaties en translaties waaronder het volume invariant zou moeten zijn.

In de vierde les zullen we zien dat er wel een oppervlaktefunctie bestaat voor willekeurige deelverzamelingen $A \subset \mathbb{R}^2$ die aan gelijkaardige voorwaarden voldoet. Hieruit volgt dan meteen dat de paradox van Banach-Tarski niet geldt in het tweedimensionale vlak.

Een tweede redenering om "aan te tonen" dat de Stelling van Banach-Tarski fout is, is wat praktischer van aard. Als deze stelling waar is, waarom doe je dit dan niet met gouden bollen om vervolgens rijk te worden?

Deze redenering maakt een andere verborgen aanname. Je gaat ervan uit dat je willekeurige deelverzamelingen A van de driedimensionale ruimte $\mathbb{R}^3$

ook effectief kan construeren of, nog concreter, kan laten uitsnijden door een lasersnijmachine. Ook dat is niet het geval. De stukken waarin je de bol in de Stelling van Banach-Tarski gaat opdelen zijn in die mate bizar dat je ze niet expliciet kan construeren of produceren. De Stelling van Banach-Tarski is dan ook bij uitstek een *bestaansstelling*: we zullen bewijzen dat een dergelijke opdeling in stukken *bestaat*, terwijl het tegelijkertijd onmogelijk is om deze stukken expliciet te construeren of definiëren.

3.1.1 Equivalente deelverzamelingen van $\mathbb{R}^3$

In [Spa24, paragraaf 1.5] maakten jullie kennis met de Euclidische groep $\mathcal{E}_n$ van afstandsbewarende transformaties (of *isometrieën*) van de Euclidische ruimte $\mathbb{R}^n$. Verderop zullen we alleen gebruikmaken van $\mathcal{E}_2$ en $\mathcal{E}_3$, de groepen van isometrieën van het vlak $\mathbb{R}^2$ en de driedimensionale ruimte $\mathbb{R}^3$.

Elke isometrie van $\mathbb{R}^n$ kan je ofwel schrijven als een samenstelling van een translatie en een rotatie – dat zijn de isometrieën die de oriëntatie bewaren – of als een samenstelling van een translatie, een rotatie en een spiegeling – en dat zijn de isometrieën die de oriëntatie omkeren. De deelgroep van oriëntatiebewarende isometrieën noteren we als $\mathcal{E}_n^+$. Je kan aan deze groep dus gewoon denken als de groep die bestaat uit alle rotaties en translaties, en hun samenstellingen.

Een isometrie α van $\mathbb{R}^n$ is per definitie een bijectie $\alpha : \mathbb{R}^n \to \mathbb{R}^n : x \mapsto \alpha(x)$ die de afstand bewaart. De groepsoperatie in $\mathcal{E}_n$ is gedefinieerd als de samenstelling van deze transformaties: $\alpha\beta = \alpha \circ \beta$.

De groep $\mathcal{E}_n$ is dus gedefinieerd aan de hand van haar actie op $\mathbb{R}^n$. We kunnen $\alpha(x)$ dan bekijken als de actie van $\alpha \in \mathcal{E}_n$ op het punt $x \in \mathbb{R}^n$. Deze actie schrijven we soms ook als $\alpha \cdot x$. Dan geldt

$$\alpha \cdot (\beta \cdot x) = (\alpha\beta) \cdot x \quad \text{voor alle } \alpha, \beta \in \mathcal{E}_n \text{ en } x \in \mathbb{R}^n.$$

Het linkerlid moet je lezen als: we passen eerst β toe op x en vervolgens passen we α toe op $\beta \cdot x$. In het rechterlid staat $\alpha\beta$, wat het product van α en β in de groep $\mathcal{E}_n$ is.

Op die manier is de actie van $\mathcal{E}_n$ op $\mathbb{R}^n$ een voorbeeld van het algemene concept van een actie van een groep G op een verzameling X, zoals aan bod kwam in [Spa24, paragraaf 1.3]. De precieze definitie gaat als volgt.

Definitie 3.1.1. Een actie van een groep G op een verzameling X is een afbeelding

$$G \times X \to X : (g, x) \mapsto g \cdot x$$

die voldoet aan de volgende eigenschappen.

(i) $e \cdot x = x$ voor alle $x \in X$, waarbij $e \in G$ het neutraal element is.

(ii) $g \cdot (h \cdot x) = (gh) \cdot x$ voor alle $g, h \in G$ en $x \in X$.

Je kan dan zelf nagaan dat voor elke $g \in G$, de transformatie $x \mapsto g^{-1} \cdot x$ de inverse is van de transformatie $x \mapsto g \cdot x$. Kortom: voor elke $g \in G$ is $x \mapsto g \cdot x$ een bijectie van X naar X en dus een permutatie van X.

Om het bewijs van Stelling A op een meer systematische manier aan te pakken, voeren we de volgende terminologie in. We voeren de terminologie in voor willekeurige groepsacties, maar zullen ze alleen maar gebruiken voor de concrete acties van de isometriegroepen $\mathcal{E}_2$ en $\mathcal{E}_3$ op $\mathbb{R}^2$ en $\mathbb{R}^3$.

Stel dat een groep G werkt op een verzameling X. We zeggen dat deelverzamelingen A en B van X equivalent zijn (onder de actie van G op X) als je A in stukken kan verdelen, deze stukken kan bewegen via de actie van G, om zo B te bekomen. Wanneer G de groep $\mathcal{E}_3^+$ voortgebracht door translaties en rotaties met haar actie op $\mathbb{R}^3$ is, is dat precies wat we doen in de Stelling van Banach-Tarski.

Strakker wiskundig geformuleerd gaat de definitie van equivalentie als volgt.

Definitie 3.1.2. Veronderstel dat een groep G werkt op een verzameling X. We noemen deelverzamelingen $A \subset X$ en $B \subset X$ *equivalent* (onder de actie van G op X) als het volgende voldaan is.

(i) We kunnen A en B in eenzelfde eindig aantal stukken verdelen: $A = A_1 \cup \cdots \cup A_n$ en $B = B_1 \cup \cdots \cup B_n$ waarbij $n \in \mathbb{N}$ en waarbij zowel de verzamelingen A_i als de verzamelingen B_j disjunct zijn.

(ii) Er bestaan elementen $g_1, \ldots, g_n \in G$ zodanig dat $B_i = g_i \cdot A_i$ voor alle $i = 1, \ldots, n$.

We noteren $A \sim B$ wanneer A en B op deze manier equivalent zijn.

Overtuig jezelf ervan dat we Stelling A dus als volgt kunnen herformuleren.

Stelling 3.1.3. *Beschouw de actie van $\mathcal{E}_3^+$ op $\mathbb{R}^3$. Zij $A \subset \mathbb{R}^3$ een massieve bol met een straal van 1 meter. Zij $B \subset \mathbb{R}^3$ de unie van twee disjuncte massieve bollen met een straal van 1 meter.*
Dan zijn A en B equivalent in de betekenis van Definitie 3.1.2.

Het nut van het concept equivalentie in Definitie 3.1.2 zit in het volgende resultaat dat jullie aan de hand van de opgegeven stappen zelf kunnen bewijzen. Om aan te tonen dat twee verzamelingen A en B equivalent zijn, kunnen we dankzij dit resultaat in stappen te werk gaan en bijvoorbeeld eerst bewijzen dat A equivalent is met C, dat C equivalent is met D en dat ten slotte D equivalent is met B.

Propositie 3.1.4. *Veronderstel dat een groep G werkt op een verzameling X en dat A, B en C deelverzamelingen van X zijn. Als $A \sim C$ en $C \sim B$, dan is $A \sim B$.*

Bewijs. Je werkt eerst het gegeven uit dat zegt dat $A \sim C$ en dat $C \sim B$.

- Je bekomt onderverdelingen $A = A_1 \cup \cdots \cup A_n$ en $C = C_1 \cup \cdots \cup C_n$, en elementen $g_i \in G$ met $C_i = g_i \cdot A_i$ voor alle i.
- Je bekomt onderverdelingen $C = C'_1 \cup \cdots \cup C'_k$ en $B = B_1 \cup \cdots \cup B_k$, en elementen $h_j \in G$ met $B_j = h_j \cdot C'_j$ voor alle j.

In eerste instantie hebben deze onderverdelingen geen verband met elkaar.

Je maakt nu een *fijnere* onderverdeling van C in de stukken $C_i \cap C'_j$ voor $1 \leq i \leq n$ en $1 \leq j \leq k$. Dat is dus een onderverdeling van C in nk stukken.

Ga nu op zoek naar overeenkomstige verfijningen van de onderverdeling van A en de onderverdeling van B die je met de groepselementen $h_j g_i \in G$ in elkaar kunt transformeren. □

Het volgende resultaat is makkelijker te bewijzen.

Propositie 3.1.5. *Veronderstel dat een groep G werkt op een verzameling X en dat A, B, C en D deelverzamelingen van X zijn.*

Veronderstel dat A en B disjunct zijn. Veronderstel dat ook C en D disjunct zijn.

Als $A \sim C$ en $B \sim D$, dan is $A \cup B$ equivalent met $C \cup D$.

Bewijs. Het volstaat om de onderverdelingen van A en C, en van C en D, samen te bekijken als onderverdelingen van $A \cup B$ en $C \cup D$. Ga dit na als oefening. □

3.1.2 Een variant van het Hotel van Hilbert

Het Hotel van Hilbert[5] is een merkwaardig hotel: zelfs wanneer het helemaal volzet is en een nieuwe gast zich aandient, kan de hoteluitbater een vrije kamer vinden. Het Hotel van Hilbert heeft immers oneindig veel kamers, genummerd met 1, 2, 3, ... Wanneer al deze kamers volgeboekt zijn en een nieuwe gast zich aandient, vraagt de hoteluitbater aan elke gast om door te schuiven naar de volgende kamer. Voor elke $n \in \mathbb{N}$ verhuist de gast in kamer n naar kamer $n + 1$. En zo is kamer 1 vrij voor de nieuwe gast!

[5] nl.wikipedia.org/wiki/Hilberts_hotel

Bijna hetzelfde argument kan gebruikt worden om de volgende eigenschap te bewijzen. Deze eigenschap zegt dat een bol, of een bol waaruit we één punt hebben weggelaten, equivalent zijn.

Propositie 3.1.6. *Beschouw de actie van $\mathcal{E}_3^+$ op $\mathbb{R}^3$. Zij $A \subset \mathbb{R}^3$ een massieve bol (met strikt positieve straal) en zij $x_0 \in A$.*
Dan zijn deze bol A en de bol zonder het punt x_0, namelijk $A \setminus \{x_0\}$, equivalent.

Bewijs. Aan de hand van de volgende stappen kan je zelf een bewijs geven. Noteer met $c_0 \in A$ het middelpunt van de bol A. Veronderstel eerst dat $x_0 \neq c_0$.

(i) Kies een rotatie $r \in \mathcal{E}_3^+$ waarvan de rotatieas door c_0 gaat en niet door x_0, en waarvan de rotatiehoek θ de eigenschap heeft dat $\theta/(2\pi)$ een irrationaal getal is. Dat betekent dus dat geen enkel veelvoud $n\theta$ met $n \in \mathbb{Z}$ gelijk is aan een veelvoud van 2π. Dit zorgt ervoor dat alle $r^n \cdot x_0$, $n \in \mathbb{Z}$, verschillend zijn. Merk ook op dat $r \cdot A = A$.

(ii) Verdeel A in de volgende twee delen: $A_1 = \{x_0, r \cdot x_0, r^2 \cdot x_0, r^3 \cdot x_0, \ldots\}$ en $A_2 = A \setminus A_1$.

(iii) Pas op A_1 rotatie r toe en pas op A_2 de identieke transformatie toe. Ga na dat je een onderverdeling bekomt van $A \setminus \{x_0\}$.

Veronderstel vervolgens dat x_0 wel het middelpunt van A is. Dan kan je in A een kleinere bol $B \subset A$ kiezen zodat $x_0 \in B$, maar x_0 niet het middelpunt van B is. Wegens de vorige stap is B equivalent met $B \setminus \{x_0\}$. Verder is $A \setminus B$ equivalent met zichzelf. Wegens Propositie 3.1.5 is dan A equivalent met $A \setminus \{x_0\}$. □

In het bewijs van Stelling A (= Stelling 3.1.3) zullen we ook de groep SO_3 gebruiken van rotaties met een rotatieas door de oorsprong. Dat is een deelgroep van $\mathcal{E}_3^+$. Deze groep werkt op een natuurlijke manier op de eenheidssfeer $S \subset \mathbb{R}^3$ (= de buitenschil van de eenheidsbol).

Propositie 3.1.7. *Beschouw de actie van SO_3 op de eenheidssfeer $S \subset \mathbb{R}^3$. Veronderstel dat $B \subset \mathbb{R}^3$ een aftelbare deelverzameling is.*
Dan zijn S en $S \setminus B$ equivalent.

Bewijs. Het bewijs is erg gelijkaardig aan het bewijs van Propositie 3.1.6. Je kan in de volgende stappen zelf de details aanvullen.

(i) Omdat de eenheidssfeer S overaftelbaar is terwijl B aftelbaar is, kunnen we een rechte L kiezen die door de oorsprong gaat en die geen

enkel punt van B bevat.

(ii) We gaan nu de gepaste rotatie $r \in \mathrm{SO}_3$ kiezen met als rotatieas L. Omdat B aftelbaar is, kunnen we de punten van B opsommen: $B = \{b_0, b_1, b_2, \ldots\}$. Gegeven i en j, zou het kunnen gebeuren dat er een rotatie $r_{i,j}$ bestaat met rotatieas L die b_i afbeeldt op b_j. Omdat b_i en b_j niet op L liggen, is een dergelijke rotatie uniek, als ze bestaat. Dit levert een aftelbare familie van "verboden rotaties" $r_{i,j}$. Omdat er overaftelbaar veel rotaties met rotatieas L zijn, namelijk een voor elke hoek in $[0, 2\pi)$, kunnen we een rotatie r kiezen met als rotatieas L zodanig dat geen enkele rotatie r^n, $n \in \mathbb{Z} \setminus \{0\}$ verboden is.

Hieruit volgt dat $r^n \cdot b_i \neq b_j$ voor alle $n \in \mathbb{Z} \setminus \{0\}$ en alle i, j. Ga na dat dit betekent dat de deelverzamelingen $r^n \cdot B$, $n \in \mathbb{Z}$, allemaal disjunct zijn.

(iii) Verdeel S in de volgende twee delen:

$$S_1 = B \cup (r \cdot B) \cup (r^2 \cdot B) \cup (r^3 \cdot B) \cup \cdots \qquad \text{en} \qquad S_2 = S \setminus S_1 \,.$$

(iv) Pas op S_1 de rotatie r toe en pas op S_2 de identieke transformatie toe. Ga na dat je zo een onderverdeling bekomt van $S \setminus B$. □

Les 2 De vrije groep $\mathbb{F}_2$ en twee vrije rotaties

In paragraaf Les 4 zullen we een conceptuele reden zien waarom de paradox van Banach-Tarski wel geldt in de driedimensionale ruimte en niet geldt in tweedimensionale ruimte. Erg ruwweg komt het erop neer dat de symmetriegroep $\mathcal{E}_3$ van de driedimensionale ruimte veel rijker en complexer is dan de symmetriegroep $\mathcal{E}_2$ van de tweedimensionale ruimte. Er zijn dus op een specifieke manier "veel meer" manieren om stukken van een bol te verschuiven en te roteren dan voor een schijf in de tweedimensionale ruimte. Om dit concreter te maken, hebben we het concept van een relatie tussen elementen van een groep nodig.

3.2.1 Vrije elementen in een groep

Bekijk eerst de groep $\mathcal{T}$ van verschuivingen van $\mathbb{R}^3$. Elke verschuiving $t \in \mathcal{T}$ wordt bepaald door een vector $a \in \mathbb{R}^3$ en is gegeven door $t(x) = x + a$ voor alle $x \in \mathbb{R}^3$. Op die manier is de groep $\mathcal{T}$ isomorf met de groep $(\mathbb{R}^3, +)$. In het bijzonder is $\mathcal{T}$ een *commutatieve groep*: voor alle verschuivingen $t_1, t_2 \in \mathcal{T}$ geldt dat $t_1 t_2 = t_2 t_1$.

In het algemeen zeggen we dat twee elementen a en b van een groep G *commuteren* als

$$ab = ba\ . \tag{3.1}$$

De gelijkheid (3.1) is een voorbeeld van een relatie (of verband) tussen de groepselementen $a, b \in G$.

In [Spa24] hebben we al gezien dat niet alle groepen commutatief zijn. Zo is bijvoorbeeld de groep $\mathcal{S}_3$ van permutaties van $\{1, 2, 3\}$ niet commutatief.

Het belangrijkste ingrediënt in het bewijs van de Stelling van Banach-Tarski is dat er rotaties α en β bestaan, met rotatieas door de oorsprong, waartussen *helemaal geen relaties gelden*. We noemen zulke rotaties α en β *vrij* en dat begrip definiëren we als volgt nauwkeuriger.

We willen dus definiëren wat het betekent dat er tussen twee elementen a en b van een groep G helemaal geen relaties gelden. We kunnen dit niet letterlijk als definitie gebruiken. Voor elk element a in een groep G geldt immers dat $aa^{-1} = e$ zodat, bijvoorbeeld, de relatie

$$baa^{-1}ba = bba \tag{3.2}$$

geldt voor alle elementen a en b in alle groepen G. Kortom, alle elementen in alle groepen voldoen aan bepaalde "evidente relaties" die allemaal voortkomen uit de gelijkheden $aa^{-1} = a^{-1}a = bb^{-1} = b^{-1}b = e$. We moeten dus meer genuanceerd zijn en nauwkeurig uitdrukken wat het betekent dat er tussen twee elementen a en b van een groep G "alleen maar deze evidente relaties gelden".

Merk op dat je de relatie (3.1) kan herschrijven als de equivalente relatie $aba^{-1}b^{-1} = e$. Op dezelfde manier kan je elke relatie herschrijven als een relatie van de vorm $w = e$, waarbij w een "woord" is met als "letters" a, a^{-1}, b, b^{-1}. Zo kan je de evidente relatie (3.2) herschrijven als

$$baa^{-1}baa^{-1}b^{-1}b^{-1} = e\ . \tag{3.3}$$

Definitie 3.2.1. (i) Veronderstel dat a en b twee symbolen zijn. Elk eindig rijtje van de symbolen a, a^{-1}, b en b^{-1} noemen we een *woord in a en b*. Zo zijn $abba^{-1}$ en $a^{-1}a^{-1}b$ woorden in a en b. Bij conventie laten we ook het *lege woord*[6] toe, dat we voorstellen als e.

(ii) We noemen een woord w in de symbolen a en b *gereduceerd* als de symbolen a en a^{-1} niet naast elkaar voorkomen en ook de symbolen b en b^{-1} niet naast elkaar voorkomen. Zo is $a^{-1}ba$ een gereduceerd woord, maar $ba^{-1}ab$ niet.

[6] Daar hebben zelfs de meest minimalistische dichters nog niet aan gedacht.

(iii) Wanneer a en b elementen van een groep G zijn, dan stelt elk woord w in de symbolen a en b ook een element van G voor. We zeggen dat a en b *vrij* zijn wanneer elk niet-leeg gereduceerd woord in de symbolen a en b in de groep G verschillend is van het neutraal element van G.

We kunnen de definitie van vrijheid ook als volgt formuleren: twee elementen a en b van een groep G zijn vrij als elk product van de elementen a, a^{-1}, b en b^{-1} waarin a, a^{-1} niet naast elkaar voorkomen en b, b^{-1} niet naast elkaar voorkomen, een element van G oplevert dat verschillend is van het neutraal element. Zo moet bijvoorbeeld $aba^{-1}b^{-1} \neq e$, zodat de groep al zeker niet commutatief is. Anderzijds geldt wel (3.3), want deze relatie geldt voor alle elementen in alle groepen.

A priori is het helemaal niet evident dat er een groep G met twee vrije elementen a en b bestaat. Zo meteen zullen we echter zien dat de groep SO_3 van rotaties van $\mathbb{R}^3$ met rotatieas door de oorsprong twee heel concrete vrije elementen bevat.

3.2.2 Twee vrije rotaties

Je zal nu zelf in een aantal stappen de volgende stelling bewijzen. Dit bewijs komt uit [Tao04, Appendix].

Stelling 3.2.2 ([Tao04, Appendix])**.** *De rotaties α en β met respectieve matrixvoorstelling*

$$A = \begin{pmatrix} 3/5 & 4/5 & 0 \\ -4/5 & 3/5 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \textit{en} \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3/5 & 4/5 \\ 0 & -4/5 & 3/5 \end{pmatrix} \quad \textit{zijn vrij.}$$

Als transformaties van de ruimte $\mathbb{R}^3$, worden deze rotaties α en β dan als volgt gegeven. In deze berekening identificeren we punten van $\mathbb{R}^3$, die we voorstellen als drietallen $(x, y, z) \in \mathbb{R}^3$, met kolomvectoren. Dus geldt voor alle $(x, y, z) \in \mathbb{R}^3$ dat

$$\alpha(x,y,z) = A \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{3}{5}x + \frac{4}{5}y \\ -\frac{4}{5}x + \frac{3}{5}y \\ z \end{pmatrix} = \big(\frac{3}{5}x + \frac{4}{5}y, -\frac{4}{5}x + \frac{3}{5}y, z\big) \quad \text{en}$$

$$\beta(x,y,z) = B \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ \frac{3}{5}y + \frac{4}{5}z \\ -\frac{4}{5}y + \frac{3}{5}z \end{pmatrix} = \big(x, \frac{3}{5}y + \frac{4}{5}z, -\frac{4}{5}y + \frac{3}{5}z\big) \quad .$$

Merk op dat α een rotatie is met de z-as als rotatieas, in wijzerzin over

een hoek $\theta \approx 53°$, terwijl β een rotatie is met de x-as als rotatieas, over dezelfde hoek.

Bewijs van Stelling 3.2.2. (i) Neem een niet-leeg gereduceerd woord w in de symbolen α en β. Deze w is dus een opeenvolging van de letters α, α^{-1}, β en β^{-1} waarin de letters α, α^{-1} en β, β^{-1} nooit naast elkaar voorkomen. Dit woord w stelt een rotatie voor waarvan de matrixvoorstelling W gegeven wordt door het overeenkomstige product van de matrices A, A^{-1}, B en B^{-1}. Als bijvoorbeeld $w = \alpha\alpha\beta^{-1}\alpha^{-1}\beta$, dan is $W = AAB^{-1}A^{-1}B$.

We moeten bewijzen dat W niet gelijk is aan de 3×3 eenheidsmatrix I_3.

(ii) Noteer met n het aantal letters in het woord w. Vervang in de uitdrukking voor W overal de matrix A door $5A$, de matrix A^{-1} door $5A^{-1}$, de matrix B door $5B$ en de matrix B^{-1} door $5B^{-1}$. We moeten dus bewijzen dat het nieuwe product van matrices dat we zo bekomen niet gelijk is aan $5^n I_3$ (de matrix met 5^n op de diagonaal en 0 elders).

De reden waarom we deze ingreep doen, is omdat de nieuwe matrices $5A$, $5A^{-1}$, $5B$ en $5B^{-1}$ een eenvoudigere vorm hebben:

$$5A = \begin{pmatrix} 3 & 4 & 0 \\ -4 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}, \qquad 5A^{-1} = \begin{pmatrix} 3 & -4 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix},$$

$$5B = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 3 & 4 \\ 0 & -4 & 3 \end{pmatrix}, \qquad 5B^{-1} = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 3 & -4 \\ 0 & 4 & 3 \end{pmatrix}.$$

We moeten dus bewijzen dat een willekeurig product van deze matrices $5A$, $5A^{-1}$, $5B$ en $5B^{-1}$, waarin $5A, 5A^{-1}$ en $5B, 5B^{-1}$ nooit naast elkaar voorkomen, verschillend is van $5^n I_3$.

(iii) Nu halen we de toverstok van [Tao04, Appendix] boven. We gaan modulair rekenen, modulo 5. We zullen dus werken met het getallenveld $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ van gehele getallen modulo 5. We kunnen getallen modulo 5 optellen en vermenigvuldigen. We kunnen ook delen door getallen verschillend van 0. Kortom, we kunnen in $\mathbb{Z}/5\mathbb{Z}$ op precies dezelfde manier rekenen als met reële getallen.

De matrices $5A$, $5A^{-1}$, $5B$ en $5B^{-1}$ hebben allemaal gehele coëfficienten. We kunnen ze dus bekijken als matrices met coëfficiënten in

$\mathbb{Z}/5\mathbb{Z}$. Om verwarring te vermijden, noteren we met A_1, A_2, B_1 en B_2 deze matrices, maar dan beschouwd als matrices met coëfficiënten in $\mathbb{Z}/5\mathbb{Z}$.

Merk op dat de matrix $5^n I_3$ als matrix met coëfficiënten in $\mathbb{Z}/5\mathbb{Z}$ gelijk is aan de nulmatrix.

Het is dus *voldoende te bewijzen* dat een willekeurig product van de matrices A_1, A_2, B_1 en B_2, waarin A_1, A_2 en B_1, B_2 nooit naast elkaar voorkomen, verschillend is van de nulmatrix, als matrices met coëfficiënten in $\mathbb{Z}/5\mathbb{Z}$.

(iv) We kunnen de matrices A_1, A_2, B_1 en B_2 ook beschouwen als lineaire transformaties van $(\mathbb{Z}/5\mathbb{Z})^3$, op dezelfde manier als $5A$, $5A^{-1}$, $5B$ en $5B^{-1}$ lineaire transformaties van $\mathbb{R}^3$ definiëren. Omdat $5 = 0$ in $\mathbb{Z}/5\mathbb{Z}$, worden de formules nog eenvoudiger:

$$\begin{aligned} A_1(x,y,z) &= (3x+4y, -4x+3y, 0) \\ A_2(x,y,z) &= (3x-4y, 4x+3y, 0) \\ B_1(x,y,z) &= (0, 3y+4z, -4y+3z) \\ B_2(x,y,z) &= (0, 3y-4z, 4y+3z) \end{aligned}$$

voor alle $x, y, z \in \mathbb{Z}/5\mathbb{Z}$.

Herschrijf deze uitdrukkingen als volgt, waarbij we in de rechterleden gebruikmaken van veelvouden van vectoren. Bijvoorbeeld: $2 \cdot (3,1,2) = (6,2,4) = (1,2,4)$ modulo 5.

$$\begin{aligned} A_1(x,y,z) &= (x+3y) \cdot (3,1,0) \\ A_2(x,y,z) &= (x+2y) \cdot (3,4,0) \\ B_1(x,y,z) &= (y+3z) \cdot (0,3,1) \\ B_2(x,y,z) &= (y+2z) \cdot (0,3,4) \end{aligned} \tag{3.4}$$

voor alle $x, y, z \in \mathbb{Z}/5\mathbb{Z}$.

(v) Neem een willekeurig product W van de matrices A_1, A_2, B_1 en B_2, waarin A_1, A_2 en B_1, B_2 nooit naast elkaar voorkomen. We bewijzen *per inductie* op de lengte van W dat W niet gelijk is aan de nulmatrix modulo 5.

Wanneer W lengte 1 heeft, is W gelijk aan één van de matrices A_1, A_2, B_1, B_2. Geen van deze matrices is gelijk aan de nulmatrix modulo 5.

Veronderstel dat het resultaat geldt voor dergelijke producten van lengte $n \geq 1$ en veronderstel dat W lengte $n+1$ heeft. We bewijzen

dat W niet gelijk is aan de nulmatrix modulo 5. Veronderstel dat het eerste symbool in de uitdrukking W het symbool A_1 is. Het argument is analoog wanneer het eerste symbool A_2, B_1 of B_2 is. Dan kunnen we W schrijven als $W = A_1V$ waarbij V een product van lengte n is, waarin A_1, A_2 en B_1, B_2 nooit naast elkaar voorkomen en waarbij het eerste symbool van V verschillend is van A_2.

Wegens de inductiehypothese is V niet gelijk aan de nulmatrix modulo 5. Neem dus $x, y, z \in \mathbb{Z}/5\mathbb{Z}$ zodat $V(x, y, z) \neq (0, 0, 0)$. Omdat het eerste symbool in de uitdrukking V gelijk is aan A_1, B_1 of B_2 volgt uit de formules in (3.4) dat de vector $V(x, y, z)$ een veelvoud is van $(3, 1, 0)$, $(0, 3, 1)$ of $(0, 3, 4)$. Omdat $V(x, y, z) \neq (0, 0, 0)$, is $V(x, y, z)$ een niet-nul veelvoud van een van deze vectoren.

Reken nu uit dat $A_1(3, 1, 0) \neq (0, 0, 0)$, dat $A_1(0, 3, 1) \neq (0, 0, 0)$ en dat $A_1(0, 3, 4) \neq (0, 0, 0)$. Besluit dat ook $W(x, y, z) \neq (0, 0, 0)$, zodat W niet gelijk is aan de nulmatrix modulo 5. □

3.2.3 Uitbreiding: het pingponglemma van Felix Klein

Het volgende resultaat geeft een heel nuttige voldoende voorwaarde om in concrete situaties aan te tonen dat twee elementen a en b in een groep G vrij zijn. Het resultaat gaat terug tot werk van Felix Klein in de 19de eeuw.

Lemma 3.2.3 (Het pingponglemma van Klein)**.** *Veronderstel dat G een groep is die werkt op een verzameling X. Veronderstel dat $X_1, X_2 \subset X$ niet-lege disjuncte deelverzamelingen van X zijn.*
Als $a, b \in G$ voldoen aan $a^n \cdot X_1 \subset X_2$ en $b^n \cdot X_2 \subset X_1$ voor alle $n \in \mathbb{Z} \setminus \{0\}$, dan zijn de elementen a en b van G vrij.

Om de naam van Lemma 3.2.3 te begrijpen, moet je X_1 en X_2 beschouwen als de twee kanten van een pingpongtafel. De slagen a^n, $n \in \mathbb{Z} \setminus \{0\}$, van de ene speler gaan van kant X_1 naar kant X_2. De slagen b^n, $n \in \mathbb{Z} \setminus \{0\}$, van de andere speler gaan van kant X_2 naar kant X_1.

Bewijs. Merk eerst op dat je elk niet-leeg gereduceerd woord w in de symbolen a en b kan schrijven als een product van elementen die alternerend van de vorm a^n en b^k zijn met $n, k \in \mathbb{Z} \setminus \{0\}$. Voorbeelden zijn:

$$a^{n_1}b^{k_1}a^{n_2} \quad \text{en} \quad b^{k_1}a^{n_1}b^{k_2}a^{n_2} \quad \text{met } n_i, k_j \in \mathbb{Z} \setminus \{0\}.$$

Neem zo'n niet-leeg gereduceerd woord.

(i) Als w begint en eindigt met een macht van a, dan zal $w \cdot X_1 \subset X_2$. Dus is $w \neq e$ in G.

(ii) Als w begint en eindigt met een macht van b, dan zal $w \cdot X_2 \subset X_1$. Dus is $w \neq e$ in G.

(iii) Als w begint met een positieve macht van a en eindigt met een macht van b, dan is het woord awa^{-1} nog steeds gereduceerd. Wegens geval (i) is $awa^{-1} \neq e$ in G. Dus is $w \neq e$ in G.

(iv) Alle andere gevallen kan je analoog aanpakken. □

Het volgende is een klassiek voorbeeld waar Lemma 3.2.3 van toepassing is.

Propositie 3.2.4. *In de groep van inverteerbare* 2×2 *matrices zijn*

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \textit{en} \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad \textit{vrij.}$$

Bewijs. De groep G van inverteerbare 2×2 matrices werkt op de verzameling $X = \mathbb{R}^2$ op de volgende natuurlijke manier, als lineaire transformaties:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} .$$

Reken na dat voor alle $n \in \mathbb{Z}$ geldt dat

$$A^n \cdot (x, y) = (x + 2ny, y) \quad \text{en} \quad B^n \cdot (x, y) = (x, 2nx + y) .$$

Definieer dan

$$X_1 = \big\{(x, y) \in \mathbb{R}^2 \;\big|\; |x| < |y|\big\} \quad \text{en} \quad X_2 = \big\{(x, y) \in \mathbb{R}^2 \;\big|\; |x| > |y|\big\} .$$

Ga na dat $A^n \cdot X_1 \subset X_2$ en $B^n \cdot X_2 \subset X_1$ voor alle $n \in \mathbb{Z} \setminus \{0\}$.
Uit Lemma 3.2.3 volgt nu dat A en B vrij zijn. □

Les 3 Bewijs van de Stelling van Banach-Tarski

In deze les bewijzen we Stelling A (= Stelling 3.1.3). In het eerste deel van het bewijs laten we zien hoe vrije elementen in een groep G gebruikt kunnen worden om een paradoxale onderverdeling te maken van G. Vervolgens laten we zien hoe we een dergelijke paradoxale onderverdeling in sommige situaties kunnen gebruiken om ook paradoxale onderverdelingen te bekomen van verzamelingen X waarop G werkt.

3.3.1 Een paradoxale onderverdeling van een vrije groep

Definitie 3.3.1. Veronderstel dat G een groep is en dat $S \subset G$. We zeggen dat S de groep G *voortbrengt* als elk element van G geschreven kan worden als een product van elementen van de vorm a en a^{-1} met $a \in S$.

Zo kan je bijvoorbeeld nagaan dat de symmetrische groep $\mathcal{S}_n$ van alle permutaties van $\{1, 2, \ldots, n\}$ voortgebracht wordt door de transposities $(1, 2)$, $(2, 3)$, …, $(n-1, n)$.

Wanneer een groep G voortgebracht wordt door twee elementen a en b, kan je per definitie elk element van G schrijven als een product van de elementen a, a^{-1}, b en b^{-1}. Dit betekent dus dat je voor elk element $g \in G$ een woord w in de symbolen a en b kan vinden zodat de gelijkheid $g = w$ geldt in G. Over het algemeen zijn er veel woorden w die hetzelfde element $g \in G$ voorstellen. Wanneer echter a en b vrij zijn, dan kan je elk element van G op *unieke* wijze voorstellen door een *gereduceerd* woord in de symbolen a en b.

Propositie 3.3.2. *Veronderstel dat de groep G voortgebracht wordt door twee vrije elementen a en b. Dan kan je elk element van G op unieke wijze voorstellen als een gereduceerd woord in de symbolen a en b.*

Het belangrijkste punt in het bewijs van Propositie 3.3.2 is om aan te tonen dat twee verschillende gereduceerde woorden w en v in de symbolen a en b ook verschillende elementen van G voorstellen. Wanneer v het lege woord is, dan is dit simpelweg de definitie van vrijheid: voor elk niet-leeg gereduceerd woord w geldt dat $w \neq e$ in de groep G. Hieruit kan je Propositie 3.3.2 afleiden. Het bewijs is niet moeilijk, maar enigszins omslachtig. We stellen het dus uit tot paragraaf 3.3.3.

De bron van de paradoxale onderverdeling van een bol in de Stelling van Banach-Tarski zit in het volgende resultaat.

Propositie 3.3.3. *Veronderstel dat de groep G voortgebracht wordt door twee vrije elementen a en b. Dan kan je G onderverdelen in 4 disjuncte delen $G = G_1 \cup G_2 \cup G_3 \cup G_4$ en elementen g_1, g_2, g_3 en g_4 in G vinden zodanig dat*

(i) $G = g_1 G_1 \cup g_2 G_2$ en de verzamelingen $g_1 G_1$ en $g_2 G_2$ zijn disjunct.

(ii) $G = g_3 G_3 \cup g_4 G_4$ en de verzamelingen $g_3 G_3$ en $g_4 G_4$ zijn disjunct.

Je kan dus in zekere zin *één exemplaar* van de groep G onderverdelen in de vier stukken G_1, G_2, G_3 en G_4, vervolgens de stukken G_1, G_2 "verschuiven" en hiermee helemaal G maken, en vervolgens ook de stukken G_3, G_4 "verschuiven" en hiermee helemaal G maken. Zo bekom je *twee*

exemplaren van de groep G.
In een latere stap zullen we deze onderverdeling van G overdragen naar verzamelingen waarop G een actie uitvoert.

Bewijs van Propositie 3.3.3. Omwille van Propositie 3.3.2 maken we in het bewijs geen onderscheid tussen gereduceerde woorden in de symbolen a, b en de bijhorende elementen van G die ze op unieke wijze voorstellen.
We noteren met W_a de verzameling van gereduceerde woorden waarvan de eerste letter gelijk is aan a. Analoog definiëren we $W_{a^{-1}}$, W_b en $W_{b^{-1}}$.

(i) Ga na dat G de unie is van de disjuncte deelverzamelingen $\{e\}$, W_a, $W_{a^{-1}}$, W_b en $W_{b^{-1}}$.

(ii) Definieer

$$G_1 = W_a\ , \qquad G_2 = W_{a^{-1}}\ ,$$
$$G_3 = W_b \setminus \{b, b^2, b^3, \ldots\}\ , \qquad G_4 = W_{b^{-1}} \cup \{e, b, b^2, b^3, \ldots\}\ .$$

Definieer $g_1 = a^{-1}$, $g_2 = e$, $g_3 = b^{-1}$ en $g_4 = e$.
Ga zelf na dat de conclusies van Propositie 3.3.3 gelden. □

3.3.2 Bewijs van de Stelling van Banach-Tarski

In Propositie 3.3.3 zagen we hoe een groep die voortgebracht wordt door twee vrije elementen een paradoxale onderverdeling heeft: je kan met één exemplaar van G via onderverdeling en verschuiving twee exemplaren van G maken.
In het volgende resultaat laten we zien dat je dan automatisch een dergelijke paradoxale onderverdeling kan maken voor verzamelingen waarop G *vrij* werkt. Een actie van een groep G op een verzameling X noemen we vrij als elk element $g \neq e$ van G elk element van X effectief "beweegt". Dit betekent dat $g \cdot x \neq x$ voor alle $g \neq e$ en voor alle $x \in X$.
Herinner uit Definitie 3.1.2 het concept van *equivalente verzamelingen*, van zodra een groepsactie van G op X gegeven is.

Propositie 3.3.4. *Veronderstel dat een groep G werkt op een verzameling X. Veronderstel dat deze actie* vrij *is. Dit wil zeggen dat $g \cdot x \neq x$ voor alle $g \neq e$ en voor alle $x \in X$.*
Veronderstel dat G voortgebracht wordt door twee vrije elementen a en b. Dan kan je X onderverdelen in 2 disjuncte delen $X = L \cup R$ zodanig dat zowel L als R equivalent zijn met heel X.

Bewijs. Beschouw de *banen* van de actie van G op X. Deze banen vormen een partitie of onderverdeling van de verzameling X. Kies nu in elke baan van de actie precies één element van X. Dat levert een deelverzameling $X_0 \subset X$ op met de eigenschap dat elke baan van de actie van G op X precies één element van X_0 bevat. Dat je een dergelijke verzameling X_0 kan kiezen, is een gevolg van het keuzeaxioma in de verzamelingenleer. Meestal is er geen constructieve manier om een dergelijke keuze expliciet te maken.

Ga na dat de afbeelding $\Phi : G \times X_0 \to X : (g, x) \mapsto g \cdot x$ een bijectie is. Hiervoor gebruik je dat de actie van G op X vrij is en dat X_0 precies één element van elke baan bevat.

Neem de onderverdeling $G = G_1 \cup G_2 \cup G_3 \cup G_4$ en de elementen g_1, g_2, g_3, g_4 in G zoals in Propositie 3.3.3. Definieer $X_i = \Phi(G_i \times X_0)$ voor $i = 1, 2, 3, 4$.

Ga de volgende beweringen na.

(i) X is de unie van de disjuncte verzamelingen X_1, X_2, X_3 en X_4.

(ii) $X = g_1 \cdot X_1 \cup g_2 \cdot X_2$ en de verzamelingen $g_1 \cdot X_1$ en $g_2 \cdot X_2$ zijn disjunct.

(iii) $X = g_3 \cdot X_3 \cup g_4 \cdot X_4$ en de verzamelingen $g_3 \cdot X_3$ en $g_4 \cdot X_4$ zijn disjunct.

Definieer $L = X_1 \cup X_2$ en $R = X_3 \cup X_4$. Ga na dat de conclusie van de propositie geldt. □

Met behulp van Propositie 3.3.4 kunnen we het volgende resultaat bewijzen dat ons al een hele stap dichter bij het bewijs van de Stelling van Banach-Tarski brengt. In dit resultaat maken we een paradoxale onderverdeling van de eenheidssfeer $S \subset \mathbb{R}^3$. Dit resultaat werd al in 1914 ontdekt door Hausdorff, [Hau14, pagina 430].

Zoals in paragraaf Les 1 noteren we met SO_3 de groep van rotaties van $\mathbb{R}^3$ met rotatieas door de oorsprong.

Stelling 3.3.5 (Paradox van Hausdorff, [Hau14, pagina 430])**.** *Beschouw de actie van* SO_3 *op de eenheidssfeer* $S \subset \mathbb{R}^3$*. Er bestaat een aftelbare deelverzameling* $B \subset S$ *en een onderverdeling van* $S \setminus B$ *in twee disjuncte delen* $S \setminus B = L \cup R$ *zodanig dat zowel* L *als* R *equivalent zijn met heel* $S \setminus B$*.*

Bewijs. Wegens Stelling 3.2.2 kunnen we twee vrije rotaties $\alpha, \beta \in \mathrm{SO}_3$ kiezen. Definieer $G \subset \mathrm{SO}_3$ als de deelgroep voortgebracht door deze twee vrije rotaties α en β.

Elke niet-triviale rotatie in SO_3 houdt precies twee punten van S vast, namelijk de snijpunten van de rotatieas met de eenheidssfeer. Definieer $B \subset S$ als de verzameling van punten die vastgehouden worden door minstens één van de rotaties in G. Omdat G aftelbaar is, is B aftelbaar.

Als deelgroep van SO_3 werkt de groep G op de eenheidssfeer S. Ga na dat $g \cdot B = B$ voor alle $g \in G$. We kunnen de actie van G op S dus beperken tot een actie van G op $S \setminus B$. Per definitie is deze actie van G op $S \setminus B$ vrij. De conclusie volgt nu uit Propositie 3.3.4. □

En dan is het eindelijk tijd voor vuurwerk.

Bewijs van Stelling A = Stelling 3.1.3. We noteren[7] met $\mathcal{P} \subset \mathbb{R}^3$ de massieve eenheidsbol met middelpunt in de oorsprong. We noteren ook $\mathcal{P}_0 = \mathcal{P} \setminus \{0\}$, wat de eenheidsbol is waaruit de oorsprong is weggenomen.

Beschouw de eenheidssfeer $S \subset \mathbb{R}^3$ en de actie van SO_3 op S. Met behulp van Stelling 3.3.5 vinden we een aftelbare deelverzameling $B \subset S$ en een onderverdeling van $S \setminus B$ in twee disjuncte delen $S \setminus B = L_1 \cup R_1$ zodanig dat zowel L_1 als R_1 equivalent zijn met heel $S \setminus B$.

Omwille van Propositie 3.1.7 is S equivalent met $S \setminus B$. Net zoals in Propositie 3.1.4 kunnen we deze equivalentie gebruiken om de onderverdeling van $S \setminus B$ in de stukken L_1 en R_1 uit de vorige paragraaf om te zetten in een onderverdeling van S zelf. We vinden dus een onderverdeling van S in twee disjuncte delen $S = L_2 \cup R_2$ zodanig dat zowel L_2 als R_2 equivalent zijn met heel S. Deze onderverdeling willen we nu overdragen naar de hele bol $\mathcal{P}$.

Voor elke deelverzameling $T \subset S$ van de eenheidssfeer bekijken we de deelverzameling $\overline{T} \subset \mathcal{P}_0$ die we kunnen beschouwen als de "kegel" met basis T en top in de oorsprong 0. Formeel is

$$\overline{T} = \left\{ tx \;\middle|\; t \in (0,1] \,,\; x \in T \right\} .$$

In nog andere woorden kan je $\overline{T}$ bouwen door alle lijnstukken van de oorsprong 0 naar punten van T samen te zetten.

Ga na dat voor elke rotatie α met rotatieas door de oorsprong geldt dat $\alpha(\overline{T}) = \overline{\alpha(T)}$ voor alle deelverzamelingen $T \subset S$.

Beschouw de actie van SO_3 op $\mathcal{P}_0$. Door $L_3 = \overline{L_2}$ en $R_3 = \overline{R_2}$ te definiëren, bekomen we de onderverdeling van $\mathcal{P}_0$ in twee disjuncte delen $\mathcal{P}_0 = L_3 \cup R_3$ zodanig dat zowel L_3 als R_3 equivalent zijn met heel $\mathcal{P}_0$.

[7] Wiskundigen hebben regelmatig letters te weinig. In de vakantieperiode is het omwille van het Italiaanse *palla* en Spaanse *pelota* toegelaten om de eenheidsbol met een $\mathcal{P}$ te noteren.

Veronderstel nu dat $\mathcal{Q} \cup \mathcal{R} \subset \mathbb{R}^3$ de unie is van twee disjuncte massieve bollen met elk een straal van 1 meter. Noteer met $\mathcal{Q}_0 \subset \mathcal{Q}$ en $\mathcal{R}_0 \subset \mathcal{R}$ dezelfde bollen waaruit het middelpunt verwijderd werd. Beschouw de actie van $\mathcal{E}_3^+$ op $\mathbb{R}^3$. Door in de vorige paragraaf ook verschuivingen te gebruiken, bekomen we dat $\mathcal{P}_0$ equivalent is met $\mathcal{Q}_0 \cup \mathcal{R}_0$ onder de actie van $\mathcal{E}_3^+$ op $\mathbb{R}^3$.

Wegens Propositie 3.1.6 gelden ook de volgende equivalenties onder de actie van $\mathcal{E}_3^+$ op $\mathbb{R}^3$: $\mathcal{P} \sim \mathcal{P}_0$, $\mathcal{Q} \sim \mathcal{Q}_0$ en $\mathcal{R} \sim \mathcal{R}_0$. Wegens Proposities 3.1.4 en 3.1.5, is dan ook $\mathcal{P}$ equivalent met $\mathcal{Q} \cup \mathcal{R}$. Hiermee is de Stelling van Banach-Tarski bewezen. □

3.3.3 Uitbreiding: bewijs van Propositie 3.3.2

Bewijs van Propositie 3.3.2. Neem $g \in G$. Per definitie kan je g schrijven als een product van de elementen a, a^{-1}, b en b^{-1}. Je vindt dus dat $g = w$ in G, waarbij w een woord is in de symbolen a en b. Door in dit woord stap voor stap de deelwoorden aa^{-1}, en $a^{-1}a$, en bb^{-1} en $b^{-1}b$ te schrappen, bekom je op een gegeven moment een gereduceerd woord w'. Omdat in de groep G elk van de uitdrukkingen aa^{-1}, en $a^{-1}a$, en bb^{-1} en $b^{-1}b$ gelijk is aan het neutraal element, geldt nog steeds dat $g = w'$ in G. We hebben dus bewezen dat we elk element op *een* manier kunnen voorstellen door een gereduceerd woord in de symbolen a en b. Hiervoor hebben we de vrijheid van a en b nog niet gebruikt.

Veronderstel dat w en v twee verschillende gereduceerde woorden in de symbolen a en b zijn. We moeten bewijzen dat w en v verschillende elementen van G voorstellen. We moeten dus bewijzen dat $w \neq v$ in G. We bewijzen deze uitspraak per inductie op de lengte van het woord w.

Als w het lege woord is, dan is v een niet-leeg gereduceerd woord en volgt uit de definitie van vrijheid dat $e \neq v$ in G.

Stel dat $w_0 \neq v_0$ in G telkens wanneer w_0 en v_0 verschillende gereduceerde woorden zijn waarbij w_0 lengte $n \geq 0$ heeft. Neem verschillende gereduceerde woorden w en v waarbij w lengte $n+1$ heeft. We moeten bewijzen dat $w \neq v$ in G.

Als de laatste letter van w verschillend is van de laatste letter van v, dan is wv^{-1} een niet-leeg gereduceerd woord. Uit de definitie van vrijheid volgt dat $wv^{-1} \neq e$ in G. Dus is $w \neq v$ in G.

Als de laatste letter van w gelijk is aan de laatste letter van v, dan is $w = w_0c$ en $v = v_0c$, waarbij c een van de letters a, a^{-1}, b of b^{-1} is. Omdat w en v verschillende gereduceerde woorden zijn, zijn ook w_0 en v_0 verschillende gereduceerde woorden. Uit de inductiehypothese volgt dat $w_0 \neq v_0$ in G. Maar dan is ook $w_0c \neq v_0c$ in G, zodat $w \neq v$ in G. □

3.3.4 Uitbreiding: de vrije groep $\mathbb{F}_2$

We maakten verschillende keren gebruik van een groep G voortgebracht door twee vrije elementen a en b. In Stelling 3.2.2 vonden we twee concrete vrije rotaties $\alpha, \beta \in \mathrm{SO}_3$. De groep hierdoor voortgebracht, is dan een groep die voortgebracht wordt door twee vrije elementen. Hetzelfde geldt voor de groep van inverteerbare matrices voortgebracht door de matrices A en B uit Propositie 3.2.4.

Uit het volgende resultaat leiden we in Gevolg 3.3.7 af dat alle groepen voortgebracht door twee vrije elementen a en b isomorf zijn. We noemen deze groep *de vrije groep* $\mathbb{F}_2$. Meer algemeen kan je ook de vrije groep $\mathbb{F}_n$ definiëren als de unieke (op isomorfisme na) groep voortgebracht door n vrije elementen.

Propositie 3.3.6. *Veronderstel dat de groep G voortgebracht is door twee vrije elementen a en b. Dan geldt de volgende* universele eigenschap*: voor alle groepen H en elementen $c, d \in H$ bestaat er een uniek groepshomomorfisme $\varphi : G \to H$ dat voldoet aan $\varphi(a) = c$ en $\varphi(b) = d$.*

Bewijs. Omdat a en b de groep G voortbrengen, is φ noodzakelijk uniek. Om het bestaan van φ aan te tonen, definiëren we alvast $\varphi(a) = c$, $\varphi(b) = d$, $\varphi(a^{-1}) = c^{-1}$ en $\varphi(b^{-1}) = d^{-1}$.

Omwille van Propositie 3.3.2 kunnen we elk element $g \in G$ op unieke wijze voorstellen door een gereduceerd woord w in de symbolen a en b. We definiëren dan $\varphi(g)$ door φ toe te passen op elk van de letters van w. Bijvoorbeeld,

$$\varphi(aab^{-1}a^{-1}b) = \varphi(a)\varphi(a)\varphi(b^{-1})\varphi(a^{-1})\varphi(b) = ccd^{-1}c^{-1}d\ .$$

We definiëren ook $\varphi(e) = e$.

Je kan nu zelf de volgende stappen aanvullen.

(i) Bewijs dat $\varphi(gh) = \varphi(g)\varphi(h)$ voor alle $g \in \{a, a^{-1}, b, b^{-1}\}$ en alle $h \in G$. Dit doe je door h voor te stellen als een gereduceerd woord en dan een gevalsonderscheid te maken in functie van de eerste letter van h.

(ii) Bewijs vervolgens dat $\varphi(gh) = \varphi(g)\varphi(h)$ door g voor te stellen als een gereduceerd woord en herhaaldelijk (i) toe te passen. □

Gevolg 3.3.7. *Veronderstel dat de groep G voortgebracht is door twee vrije elementen a en b, en dat de groep H voortgebracht is door twee vrije elementen c en d. Dan is er een uniek groepsisomorfisme $\varphi : G \to H$ dat voldoet aan $\varphi(a) = c$ en $\varphi(b) = d$.*

Bewijs. Wegens Propositie 3.3.6 bestaat er een uniek groepshomomorfisme $\varphi : G \to H$ dat voldoet aan $\varphi(a) = c$ en $\varphi(b) = d$. Om dezelfde reden bestaat er een uniek groepshomomorfisme $\psi : H \to G$ dat voldoet aan $\psi(c) = a$ en $\psi(d) = b$. Dan is $\psi \circ \varphi$ een groepshomomorfisme van G naar G dat a afbeeldt op a en b afbeeldt op b. Omdat a en b de groep G voortbrengen, zal $\psi \circ \varphi = \mathrm{id}$. Om dezelfde reden is $\varphi \circ \psi = \mathrm{id}$. Dus is φ een isomorfisme. □

Opmerking 3.3.8. Wij hebben tot hier gewacht om de vrije groep $\mathbb{F}_2$ te definiëren. In de meeste literatuur zal je eerst een definitie van $\mathbb{F}_2$ vinden als abstracte groep en dan pas een constructie van twee vrije rotaties. Wij hebben ervoor gekozen om eerder direct te werken met de concrete vrije rotaties uit Stelling 3.2.2. De definitie van $\mathbb{F}_2$ en unieke karakterisering van $\mathbb{F}_2$ krijg je er dan "gratis bij" zoals hierboven.

Om $\mathbb{F}_2$ als abstracte groep te definiëren, kan je als volgt te werk gaan. Je definieert de verzameling $\mathbb{F}_2$ als de verzameling van alle gereduceerde woorden in de symbolen a en b. Vervolgens moeten we de groepsoperatie definiëren. Als w en v gereduceerde woorden zijn, bekijken we eerst het woord wv dat je bekomt door w en v achter elkaar te schrijven. Dit woord is over het algemeen niet gereduceerd. Maar je kan dit woord vereenvoudigen tot een gereduceerd woord en je kan (omslachtig) aantonen dat deze reductie uniek is. We kunnen dan de groepsoperatie in $\mathbb{F}_2$ definiëren als

$$w \cdot v = \text{reductie}(wv) \ .$$

Met opnieuw een omslachtig bewijs kan je dan aantonen dat deze groepsoperatie associatief is. Het neutraal element is het lege woord e. De inverse van een gereduceerd woord w is het evidente gereduceerd woord w^{-1}.

3.3.5 Uitbreiding: de paradox van Banach-Tarski in volle algemeenheid

Zoals je kon lezen in het citaat op pagina 65 bewezen Banach en Tarski in [BT24] een sterker resultaat dan Stelling A. Ze bewezen dat het voor bijna eender welke deelverzamelingen A en B van $\mathbb{R}^3$ mogelijk is om A in stukken te verdelen, deze stukken te roteren en te verschuiven, en zo B te bekomen.

In het bijzonder kan je op die manier van een erwt A de hele zon B maken, wat de oorsprong is voor de titel van het boek [Wap05].

Het is niet mogelijk om op die manier van een totaal willekeurige deelverzameling $A \subset \mathbb{R}^3$ een totaal willekeurige deelverzameling $B \subset \mathbb{R}^3$ te

maken. Zo kan je bijvoorbeeld meteen inzien dat wanneer A eindig is, B ook eindig moet zijn en evenveel elementen als A moet hebben.

Om de Stelling van Banach-Tarski in haar volle algemeenheid te formuleren, hebben we de volgende terminologie nodig.

- We zeggen dat een deelverzameling $A \subset \mathbb{R}^3$ *begrensd* is als er een bol P (eventueel heel groot, maar met eindige straal) bestaat zodat $A \subset P$.
- We zeggen dat een deelverzameling $A \subset \mathbb{R}^3$ een *niet-leeg inwendige* heeft als er een bol Q (eventueel heel klein, maar met strikt positieve straal) bestaat zodat $Q \subset A$.

Ga zelf na dat wanneer $A \subset \mathbb{R}^3$ een begrensde deelverzameling is en $B \subset \mathbb{R}^3$ een onbegrensde deelverzameling, het *onmogelijk* is om A in stukken te verdelen en via rotatie en verschuiving van deze stukken B te bekomen.

Stelling 3.3.9 ([BT24, Théorème 24])**.** *Veronderstel dat A en B deelverzamelingen van $\mathbb{R}^3$ zijn die beide begrensd zijn en beide een niet-leeg inwendige hebben.*

Dan kunnen we A in eindig veel stukken verdelen, deze stukken roteren en verschuiven en zo B bekomen.

In Definitie 3.1.2 voerden we het concept van equivalente deelverzamelingen $A \sim B$ in, gegeven een groepsactie van een groep G op een verzameling X. Om Stelling 3.3.9 te bewijzen, hebben we de volgende veralgemening nodig.

Definitie 3.3.10. Veronderstel dat een groep G werkt op een verzameling X. We zeggen dat een deelverzameling $A \subset X$ *subequivalent* is met een deelverzameling $B \subset X$ (onder de actie van G op X) als A equivalent is met een deelverzameling van B.

We gebruiken de notatie $A \prec B$ om aan te geven dat A subequivalent is met B.

Ga als oefening de volgende beweringen na: als $A \prec B$ en $B \prec C$, dan $A \prec C$; als $A \subset B$, dan ook $A \prec B$.

Een belangrijke stap om Stelling 3.3.9 te bewijzen, is de Stelling van Banach-Schröder-Bernstein die zegt dat wanneer $A \prec B$ en $B \prec A$, dan $A \sim B$.

Dat klinkt onschuldiger dan het werkelijk is. Als je A in stukken kan knippen en met deze stukken een deel van B kan maken (d.w.z. $A \prec B$) en als je omgekeerd B in stukken kan knippen en met deze stukken een deel van A kan maken (d.w.z. $B \prec A$), dan is het niet a priori evident om A op een andere manier in stukken te knippen en hiermee B te maken (d.w.z.

$A \sim B$). Toch is dit mogelijk en wel dankzij de volgende stelling.

Stelling 3.3.11 (Banach-Schröder-Bernstein, [Ban24, Théorème 1])**.** *Veronderstel dat A en B verzamelingen zijn en dat $\varphi : A \to B$ en $\psi : B \to A$ injectieve afbeeldingen zijn.*
Dan bestaat er een deelverzameling $A_0 \subset \psi(B)$ zodanig dat de afbeelding

$$\theta : A \to B : \theta(a) = \begin{cases} \psi^{-1}(a) & \text{als } a \in A_0, \\ \varphi(a) & \text{als } a \in A \setminus A_0, \end{cases}$$

een bijectie is.

Bewijs. Definieer $C_0 = A \setminus \psi(B)$. Definieer vervolgens per inductie $C_{n+1} = \psi(\varphi(C_n))$ voor alle $n \geq 0$. Stel

$$C = \bigcup_{n=0}^{\infty} C_n \quad \text{en} \quad A_0 = A \setminus C \, .$$

We bewijzen dat A_0 voldoet aan de conclusie van de stelling.
Omdat $C_0 = A \setminus \psi(B)$, geldt dat

$$A_0 = A \setminus C = (A \setminus C_0) \setminus \Big(\bigcup_{n=1}^{\infty} C_n \Big) = \psi(B) \setminus \Big(\bigcup_{n=1}^{\infty} C_n \Big) \, .$$

Hieruit halen we dat $A_0 \subset \psi(B)$. Omdat per definitie $C_n \subset \psi(B)$ voor alle $n \geq 1$, halen we hieruit ook dat

$$\begin{aligned} \psi^{-1}(A_0) &= B \setminus \Big(\bigcup_{n=1}^{\infty} \psi^{-1}(C_n) \Big) = B \setminus \Big(\bigcup_{n=1}^{\infty} \varphi(C_{n-1}) \Big) \\ &= B \setminus \Big(\bigcup_{n=0}^{\infty} \varphi(C_n) \Big) = B \setminus \varphi(C) \, . \end{aligned}$$

Dit betekent dat ψ^{-1} een bijectie oplevert tussen A_0 en $B \setminus \varphi(C)$. Per definitie is $A \setminus A_0 = C$ zodat φ een bijectie oplevert tussen $A \setminus A_0$ en $\varphi(C)$. Deze twee bijecties samen leveren dan de bijectie θ tussen A en B. □

Gevolg 3.3.12. *Veronderstel dat een groep G werkt op een verzameling X en dat A en B deelverzamelingen van X zijn. Als $A \prec B$ en $B \prec A$, dan is $A \sim B$.*

Bewijs. We zeggen dat een afbeelding $\varphi : U \to V$ van een deelverzameling $U \subset X$ naar een deelverzameling $V \subset X$ een *G-injectie* is als φ injectief is en als we φ kunnen schrijven door een combinatie van eindig veel

transformaties gegeven door de actie van G op X. Nauwkeuriger gezegd betekent dit dat er eindig veel disjuncte deelverzamelingen $U_1, \ldots, U_n \subset U$ bestaan en groepselementen $g_1, \ldots, g_n \in G$ zodanig dat $U = U_1 \cup \cdots \cup U_n$ en $\varphi(u) = g_i \cdot u$ voor alle $u \in U_i$ en $i = 1, \ldots, n$. Wanneer φ daarenboven bijectief is, noemen we φ een *G-bijectie*.

Ga na dat $U \prec V$ als en slechts als er een G-injectie $\varphi : U \to V$ bestaat. Ga na dat $U \sim V$ als en slechts als er een G-bijectie $\varphi : U \to V$ bestaat. Omdat $A \prec B$ en $B \prec A$, kunnen we dus G-injecties $\varphi : A \to B$ en $\psi : B \to A$ nemen.

Stelling 3.3.11 geeft ons een deelverzameling $A_0 \subset \psi(B)$ zodanig dat de afbeelding

$$\theta : A \to B : \theta(a) = \begin{cases} \psi^{-1}(a) & \text{als } a \in A_0, \\ \varphi(a) & \text{als } a \in A \setminus A_0, \end{cases}$$

een bijectie is.

Omdat de afbeeldingen $\psi^{-1} : A_0 \to B$ en $\varphi : A \setminus A_0 \to B$ allebei G-injecties zijn, is θ een G-bijectie. Dus is $A \sim B$. □

We zijn nu klaar om de Stelling van Banach-Tarski in haar volle algemeenheid te bewijzen.

Bewijs van Stelling 3.3.9. Beschouw de actie van $\mathcal{E}_3^+$ op $\mathbb{R}^3$. We moeten bewijzen dat $A \sim B$ t.o.v. deze actie. Omwille van Gevolg 3.3.12 en omdat de veronderstellingen die we maken dezelfde zijn voor A als voor B, is het voldoende te bewijzen dat $B \prec A$.

Omdat A een niet-leeg inwendige heeft, kunnen we een kleine bol $Q \subset A$ kiezen met een strikt positieve straal. Omdat B begrensd is, kunnen we B bedekken met eindig veel bollen $B \subset P_1 \cup \cdots \cup P_n$ die alle dezelfde straal als Q hebben. Deze bollen P_i kunnen elkaar overlappen.

We kiezen ook disjuncte bollen $Q_1, \ldots, Q_n$ die alle dezelfde straal als Q hebben en disjunct zijn van Q. Voor elke i, is P_i een bol met dezelfde straal als Q_i. Er is dus een verschuiving die P_i afbeeldt op Q_i. Door deze verschuivingen te combineren, vinden we dat

$$P_1 \cup \cdots \cup P_n \prec Q_1 \cup \cdots \cup Q_n \quad \text{en dus} \quad B \prec Q_1 \cup \cdots \cup Q_n \,.$$

Omwille van Stelling 3.1.3, is $Q_1 \cup Q_2 \sim Q$. Dus is

$$Q_1 \cup Q_2 \cup Q_3 \cup \cdots \cup Q_n \sim Q \cup Q_3 \cup \cdots \cup Q_n \,.$$

Als we deze redenering enkele keren herhalen, vinden we dat $Q_1 \cup \cdots \cup Q_n \sim Q$. Omdat $B \prec Q_1 \cup \cdots \cup Q_n$ en $Q \subset A$, volgt dus dat $B \prec A$. □

Les 4 In het tweedimensionale vlak is alles anders

In hun oorspronkelijke artikel [BT24] bewijzen Banach en Tarski ook Stelling B die zegt dat er geen paradox van Banach-Tarski bestaat in dimensie 2. In deze laatste les schetsen we het bewijs van Stelling B.

We volgen hierbij de meer conceptuele aanpak die John von Neumann in 1929 ontdekte en publiceerde in [vNeu29]. De reden waarom er alleen een paradox van Banach-Tarski bestaat in dimensie 3 en hoger is omdat de groep $\mathcal{E}_3$ van isometrieën van $\mathbb{R}^3$ substantieel rijker en complexer is dan de groep $\mathcal{E}_2$ van isometrieën van $\mathbb{R}^2$. Zoals we zagen in Stelling 3.2.2 is het mogelijk om in $\mathcal{E}_3$ twee elementen te vinden die vrij zijn, wat wil zeggen dat er tussen deze groepselementen geen enkele relatie geldt. Dergelijke vrije elementen *bestaan niet* in $\mathcal{E}_2$.

In [vNeu29] definieerde von Neumann het concept van een *amenable*[8] *groep*. Hij toonde aan dat een groep die twee vrije elementen bevat niet amenable is. Anderzijds toonde hij aan dat $\mathcal{E}_2$ wel amenable is. Daarenboven toonde hij aan dat amenability van $\mathcal{E}_2$ gebruikt kan worden om het volgende resultaat te bewijzen.

Stelling 3.4.1. *Er bestaat een* oppervlaktefunctie *die aan elke deelverzameling $U \subset \mathbb{R}^2$ een oppervlakte* $\mathrm{opp}(U)$ *toekent en voldoet aan de volgende eigenschappen.*

(i) Voor alle $U \subset \mathbb{R}^2$ is $\mathrm{opp}(U) \in [0, +\infty]$.

(ii) Voor alle disjuncte deelverzamelingen $U, V \subset \mathbb{R}^2$ geldt dat $\mathrm{opp}(U \cup V)$ *gelijk is aan* $\mathrm{opp}(U) + \mathrm{opp}(V)$.

(iii) Voor alle $U \subset \mathbb{R}^2$ en alle $\alpha \in \mathcal{E}_2$ geldt dat $\mathrm{opp}(\alpha(U)) = \mathrm{opp}(U)$.

(iv) Voor alle "gewone en gebruikelijke" deelverzamelingen $U \subset \mathbb{R}^2$ is $\mathrm{opp}(U)$ *gelijk aan de "gewone en gebruikelijke" oppervlakte van U.*

Eigenschap (iv) is natuurlijk niet nauwkeurig wiskundig gedefinieerd. Voor onze doeleinden is het al genoeg om te zeggen dat de $\mathrm{opp}(U)$ gelijk is aan πr^2 wanneer U een schijf met straal r is. Dan volgt Stelling B meteen uit Stelling 3.4.1. Ga dit na!

[8] Er is geen goed Nederlands woord voor *amenable* of *amenability*. Het probleem is dat er voor het Nederlandse substantief *gemiddelde* geen overeenkomstig adjectief of werkwoord bestaat. Von Neumann gebruikt het Duitse adjectief *messbar*, wat je zou kunnen vertalen als *meetbaar*. Maar vandaag de dag betekent *meetbare groep* iets anders dan *amenable groep*. We houden het dus bij de Engelstalige woorden *amenable* en *amenability*.

Wie vertrouwd is met de theorie van Lebesgue-integratie kan eigenschap (iv) als volgt lezen: voor alle Lebesgue-meetbare deelverzamelingen U van $\mathbb{R}^2$ is opp(U) gelijk aan de Lebesguemaat van U.

In deze laatste les schetsen we het bewijs van Stelling 3.4.1. Deze schets zal minder volledig zijn dan het bewijs van Stelling A dat we in de eerste drie lessen gaven. Om Stelling 3.4.1 in alle details te bewijzen, is er bijkomende achtergrond nodig in topologie en analyse, voornamelijk rond compactheid en het bestaan van limietpunten in compacta.

3.4.1 Amenable groepen

Definitie 3.4.2 ([vNeu29, pagina 78-79])**.** We noemen een groep G *amenable* als er een functie m bestaat die aan elke deelverzameling $U \subset G$ een maat $m(U)$ toekent zodanig dat de volgende eigenschappen gelden.

(i) Voor alle $U \subset G$ is $m(U) \in [0, 1]$.

(ii) Er geldt dat $m(\emptyset) = 0$ en $m(G) = 1$.

(iii) Voor alle disjuncte deelverzamelingen $U, V \subset G$ geldt dat $m(U \cup V) = m(U) + m(V)$.

(iv) Voor alle $U \subset G$ en $g \in G$ geldt dat $m(gU) = m(U)$.

We noemen een functie m zoals hierboven een *invariant gemiddelde* op G.

Ga als oefening na dat elke *eindige* groep G amenable is door $m(U)$ gelijk te stellen aan

$$m(U) = \frac{\#U}{\#G} .$$

De eindige groepen zijn de enige groepen waarvoor een expliciet invariant gemiddelde bestaat. Er zijn heel veel oneindige amenable groepen, zoals we hieronder zullen zien, maar in elk van die gevallen kan je alleen het bestaan van een invariant gemiddelde bewijzen, zonder dat je een invariant gemiddelde expliciet kan construeren.

3.4.2 Een groep met vrije elementen is niet amenable

De uitspraak in de titel van deze paragraaf is een gevolg van het volgende resultaat.

Propositie 3.4.3 ([vNeu29, pagina 82])**.** *(i) Als een groep G voortgebracht wordt door twee vrije elementen a en b, dan is G niet amenable.*

(ii) Een deelgroep van een amenable groep is zelf amenable.

Bewijs. (i) Dit is een onmiddellijk gevolg van Propositie 3.3.3. Als m een invariant gemiddelde op G zou zijn, dan is

$$m(G_1) + m(G_2) + m(G_3) + m(G_4) = m(G_1 \cup G_2 \cup G_3 \cup G_4) = m(G) = 1 \; . \tag{3.5}$$

Anderzijds is dan ook

$$m(G_1) + m(G_2) = m(g_1 G_1) + m(g_2 G_2) = m(g_1 G_1 \cup g_2 G_2) = m(G) = 1$$

en

$$m(G_3) + m(G_4) = m(g_3 G_3) + m(g_4 G_4) = m(g_3 G_3 \cup g_4 G_4) = m(G) = 1 \; .$$

Als we deze vergelijkingen optellen, bekomen we dat $m(G_1) + m(G_2) + m(G_3) + m(G_4) = 2$, wat in tegenspraak is met (3.5).

(ii) Veronderstel dat H een deelgroep is van G en dat m_G een invariant gemiddelde is op G. We moeten bewijzen dat H amenable is.

Beschouw de nevenklassen $Hg \subset G$ van H in G (zie [Spa24, paragraaf 1.8]). Kies met behulp van het keuzeaxioma een deelverzameling $G_0 \subset G$ die uit elk van deze nevenklassen precies één element bevat. Ga dan na dat $\varphi : H \times G_0 \to G : \varphi(h, g) = hg$ een bijectie is.

Noteer met $\psi : G \to H \times G_0 : \psi(g) = (\pi(g), \theta(g))$ de inverse afbeelding van φ. Ga na dat de afbeelding $\pi : G \to H$ voldoet aan $\pi(hg) = h\pi(g)$ voor alle $h \in H$ en $g \in G$.

Definieer voor elke deelverzameling $U \subset H$,

$$m_H(U) = m_G(\pi^{-1}(U)) \quad \text{waarbij} \quad \pi^{-1}(U) = \left\{ g \in G \;\middle|\; \pi(g) \in U \right\} .$$

Ga na dat m_H een invariant gemiddelde op H is. □

Opmerking 3.4.4. In [Day57, pagina 520] formuleert Day de vraag of ook het omgekeerde van Propositie 3.4.3 waar zou kunnen zijn: heeft elke niet-amenable groep G twee vrije elementen a en b? Hoewel deze vraag niet als dusdanig voorkomt in het werk van von Neumann, staat de vraag bekend als het *probleem van von Neumann en Day.* Pas in [Ols80] vond Ol'shanskii het eerste tegenvoorbeeld door een niet-amenable groep te construeren die geen vrije elementen a en b bevat.

3.4.3 Heel wat groepen, waaronder $\mathcal{E}_2$, zijn wel amenable

Vlak na Definitie 3.4.2 merkten we al op dat elke eindige groep amenable is. Verder bewees von Neumann in [vNeu29] ook de volgende twee resultaten.

Propositie 3.4.5 ([vNeu29, Eigenschap A]). *Elke commutatieve groep G is amenable.*

Herinner uit [Spa24, paragraaf 1.8] de concepten van een normale deelgroep N van een groep G en de bijhorende quotiëntgroep G/N.

Propositie 3.4.6 ([vNeu29, Eigenschap B]). *Veronderstel dat G een groep is met normale deelgroep $N \subset G$ en quotiëntgroep G/N.*
De groep G is amenable als en slechts als N en G/N allebei amenable zijn.

De bewijzen van Propositie 3.4.5 en 3.4.6 zijn niet zo eenvoudig en stellen we uit naar paragrafen 3.4.7 en 3.4.8 die we niet in het college zullen behandelen.

Omdat dit nauwer aansluit bij algemene theorie van groepen, bewijzen we wel het gevolg dat de groep $\mathcal{E}_2$ van isometrieën van het vlak $\mathbb{R}^2$ amenable is.

Gevolg 3.4.7. *De groep $\mathcal{E}_2$ van isometrieën van het vlak $\mathbb{R}^2$ is amenable.*

Bewijs. Noteer met $\mathcal{T}_2 \subset \mathcal{E}_2$ de deelgroep van translaties van $\mathbb{R}^2$. Noteer met $\mathcal{O}_2 \subset \mathcal{E}_2$ de deelgroep van isometrieën van $\mathbb{R}^2$ die de oorsprong bewaren.

Vul zelf de details aan in de volgende stappen van het bewijs.

(i) Herinner uit [Spa24, paragraaf 1.5] dat $\mathcal{O}_2$ bestaat uit de rotaties met middelpunt in de oorsprong en de samenstellingen van een rotatie met middelpunt in de oorsprong met een spiegeling rond een rechte door de oorsprong. In het bijzonder zijn alle elementen van $\mathcal{O}_2$ lineaire transformaties van het vlak.

(ii) Bewijs dat je elk element van $\mathcal{E}_2$ op unieke manier kan schrijven als de samenstelling van een element uit $\mathcal{O}_2$ en een element uit $\mathcal{T}_2$.

(iii) Bewijs dat $\mathcal{T}_2$ een normale deelgroep van $\mathcal{E}_2$ is.

(iv) Gebruik (ii) en (iii) om te bewijzen dat het quotiënt $\mathcal{E}_2/\mathcal{T}_2$ isomorf is met $\mathcal{O}_2$.

(v) Noteer met $\mathcal{R}_2 \subset \mathcal{O}_2$ de deelgroep van rotaties met middelpunt in de oorsprong. Gebruik (i) om te bewijzen dat $\mathcal{R}_2$ een normale deelgroep van $\mathcal{O}_2$ is en dat $\mathcal{O}_2/\mathcal{R}_2$ isomorf is met de unieke groep met 2 elementen.

(vi) Omdat $\mathcal{R}_2$ en de groep met 2 elementen commutatief zijn, volgt uit (v) en Proposities 3.4.5 en 3.4.6 dat $\mathcal{O}_2$ amenable is. Omdat $\mathcal{T}_2$ commutatief is, volgt vervolgens uit (iv) en Proposities 3.4.5 en 3.4.6

dat $\mathcal{E}_2$ amenable is. □

Uit Gevolg 3.4.7 en Propositie 3.4.3 leiden we meteen het volgende resultaat af, dat in schril contrast staat met Stelling 3.2.2.

Gevolg 3.4.8. *De groep $\mathcal{E}_2$ van isometrieën van $\mathbb{R}^2$ bevat geen vrije elementen a, b.*

3.4.4 Tussendoor: gemiddeldes en integralen

Veronderstel dat G een verzameling is en dat m een *gemiddelde* is op G. Hiermee bedoelen we dat m een functie is die aan elke deelverzameling $U \subset G$ een getal $m(U) \in [0,1]$ toekent zodanig dat eigenschappen (i), (ii) en (iii) in Definitie 3.4.2 gelden:

(i) Voor alle $U \subset G$ is $m(U) \in [0,1]$.

(ii) Er geldt dat $m(\emptyset) = 0$ en $m(G) = 1$.

(iii) Voor alle disjuncte deelverzamelingen $U, V \subset G$ geldt dat $m(U \cup V) = m(U) + m(V)$.

Een gemiddelde m op een verzameling G kan gebruikt worden om voor elke begrensde[9] functie $F : G \to \mathbb{R}$ een (bepaalde) integraal $I(F) \in \mathbb{R}$ te definiëren.

We willen dat deze integraal aan de volgende eigenschappen voldoet.

(i) Voor alle begrensde functies $F : G \to \mathbb{R}$ is $I(F) \in \mathbb{R}$.

(ii) Wanneer $U \subset G$ en $F = 1_U$ de functie is die gelijk is aan 1 op U en gelijk aan 0 buiten U, dan is $I(F) = m(U)$.

(iii) De integraal is lineair: wanneer $F_1, F_2 : G \to \mathbb{R}$ begrensde functies zijn en $s_1, s_2 \in \mathbb{R}$, dan is

$$I(s_1F_1 + s_2F_2) = s_1I(F_1) + s_2I(F_2) \ .$$

(iv) De integraal is positief: wanneer $F(g) \geq 0$ voor alle $g \in G$, dan is $I(F) \geq 0$.

Men kan aantonen dat er voor elk gemiddelde m op een verzameling G een *unieke integraal* $I(F)$, gedefinieerd voor alle begrensde functies $F : G \to \mathbb{R}$, is die voldoet aan deze voorwaarden. Het bewijs van deze bewering laten we achterwege.

[9] Hiermee bedoelen we dat er een $s \geq 0$ bestaat zodat $-s \leq F(g) \leq s$ voor alle $g \in G$.

Op een gegeven moment zullen we de integraal $I(F)$ ook nodig hebben voor sommige onbegrensde positieve functies $F : G \to [0, +\infty]$. Wanneer $F : G \to [0, +\infty]$ een positieve functie is, definiëren we $I(F)$ zoals hierboven wanneer F begrensd is, wat wil zeggen dat er een $s \in [0, +\infty)$ bestaat zodat $F(g) \leq s$ voor alle $g \in G$, en definiëren we $I(F) = +\infty$ wanneer F onbegrensd is.

Deze integraal voor willekeurige positieve functies, heeft de volgende eigenschappen.

(i) Voor alle positieve functies $F : G \to [0, +\infty]$ is $I(F) \in [0, +\infty]$.

(ii) Wanneer $U \subset G$ en $F = 1_U$ de functie is die gelijk is aan 1 op U en gelijk aan 0 buiten U, dan is $I(F) = m(U)$.

(iii) Wanneer $F_1, F_2 : G \to [0, +\infty]$ positieve functies zijn en $s_1, s_2 \geq 0$, dan is

$$I(s_1 F_1 + s_2 F_2) = s_1 I(F_1) + s_2 I(F_2) \; .$$

Veronderstel tot slot dat G een groep is en dat m een *invariant* gemiddelde op G is. Dat wil zeggen dat m naast de eigenschappen (i), (ii) en (iii) van een gemiddelde ook voldoet aan de invariantie $m(gU) = m(U)$ voor alle $g \in G$ en $U \subset G$.

We kunnen de groepsstructuur van G gebruiken om als volgt functies te verschuiven. Wanneer $F : G \to \mathbb{R}$ een functie is en $g \in G$, definiëren we de verschoven functie $g \cdot F$ als

$$g \cdot F : G \to \mathbb{R} : h \mapsto F(g^{-1}h) \; .$$

Omwille van de uniciteit van de integraal I die hoort bij het gemiddelde m, geldt dan de invariantie

$$I(g \cdot F) = I(F)$$

voor alle $g \in G$ en alle begrensde functies $F : G \to \mathbb{R}$. Dezelfde invariantie geldt voor alle $g \in G$ en alle positieve functies $F : G \to [0, +\infty]$.

3.4.5 Er is geen paradox van Banach-Tarski in dimensie 2

Schets van het bewijs van Stelling 3.4.1. Definieer $G = \mathcal{E}_2$ als de groep van isometrieën van het vlak $\mathbb{R}^2$. Het belangrijkste ingrediënt is de amenability van de groep G, zie Gevolg 3.4.7. Neem dus een invariant gemiddelde m op G.

Noteer zoals in paragraaf 3.4.4 met $I(F)$ de integraal t.o.v. m voor een willekeurige positieve functie $F : G \to [0, +\infty]$. Beschouw zoals in paragraaf 3.4.4 voor elke functie F en $g \in G$, de verschoven functie $g \cdot F$. Herinner dat $I(g \cdot F) = I(F)$ voor alle $g \in G$ en alle positieve functies $F : G \to [0, +\infty]$.

Begin nu met een collectie $\mathcal{C}$ van "gewone en gebruikelijke" deelverzamelingen van $\mathbb{R}^2$ en noteer met $\lambda(U)$ de oppervlakte van elk van deze $U \in \mathcal{C}$. De kenners nemen voor $\mathcal{C}$ de collectie van Lebesguemeetbare verzamelingen en voor λ de Lebesguemaat. Maar je mag voor $\mathcal{C}$ en λ eender welke collectie van deelverzamelingen van $\mathbb{R}^2$ en functie λ nemen die aan de volgende voorwaarden voldoet.

(i) De lege verzameling $\emptyset$ behoort tot $\mathcal{C}$ en $\lambda(\emptyset) = 0$.

(ii) Als $U, V \in \mathcal{C}$, dan behoren de unie $U \cup V$ en het complement $\mathbb{R}^2 \setminus U$ tot $\mathcal{C}$.

(iii) Als $U, V \in \mathcal{C}$ disjunct zijn, dan is $\lambda(U \cup V) = \lambda(U) + \lambda(V)$.

(iv) Als $U \in \mathcal{C}$ en $g \in G$, dan is $g \cdot U \in \mathcal{C}$ en $\lambda(g \cdot U) = \lambda(U)$.

Via een (subtiele) toepassing van het keuzeaxioma is het mogelijk om λ uit te breiden tot een functie γ op *alle* deelverzamelingen van $\mathbb{R}^2$ zodanig dat nog steeds $\gamma(U \cup V) = \gamma(U) + \gamma(V)$ wanneer $U, V \subset \mathbb{R}^2$ disjunct zijn. Het is echter niet a priori mogelijk om ervoor te zorgen dat γ invariant is onder de actie van G. Daarvoor hebben we verderop de amenability van G nodig.

Wanneer $U \subset \mathbb{R}^2$ een willekeurige deelverzameling is, beschouwen we de bijhorende positieve functie

$$F_U : \mathcal{E}_2 \to [0, +\infty] : h \mapsto \gamma(h^{-1} \cdot U) \; .$$

We definiëren nu $\mathrm{opp}(U) = I(F_U)$.

We bewijzen dat $\mathrm{opp}(U)$ aan alle voorwaarden in Stelling 3.4.1 voldoet.

(i) Per constructie is $\mathrm{opp}(U) \in [0, +\infty]$ voor alle $U \subset \mathbb{R}^2$.

(ii) Wanneer $U, V \subset \mathbb{R}^2$ disjunct zijn, is $F_{U \cup V} = F_U + F_V$. Dus zal

$$\begin{aligned} \mathrm{opp}(U \cup V) &= I(F_{U \cup V}) = I(F_U + F_V) \\ &= I(F_U) + I(F_V) = \mathrm{opp}(U) + \mathrm{opp}(V) \; . \end{aligned}$$

(iii) Wanneer $U \subset \mathbb{R}^2$ en $g \in G$, is $F_{g \cdot U} = g \cdot F_U$. Dus zal

$$\mathrm{opp}(g \cdot U) = I(F_{g \cdot U}) = I(g \cdot F_U) = I(F_U) = \mathrm{opp}(U) \; .$$

(iv) Wanneer $U \in \mathcal{C}$, is $F_U(h) = \gamma(h^{-1} \cdot U) = \lambda(h^{-1} \cdot U) = \lambda(U)$ voor alle $h \in G$. Dus is F_U constant gelijk aan $\lambda(U)$. Hieruit volgt dat $\text{opp}(U) = I(F_U) = \lambda(U)$. □

3.4.6 De rol van het keuzeaxioma en de fundamenten van de wiskunde

In het begin van de 20ste eeuw kreeg de wiskunde haar formele en axiomatische basis waarop ze tot op de dag van vandaag verder gebouwd wordt. De grondslagen van de wiskunde liggen in de verzamelingenleer en het axiomatische systeem voor de verzamelingenleer dat ontwikkeld werd door Zermelo en Fraenkel.

Een van de axioma's in het systeem van Zermelo en Fraenkel is het keuzeaxioma. Dit zegt ruwweg het volgende: als een verzameling X onderverdeeld is in deelverzamelingen $Y \in \mathcal{P}$ – denk hierbij bijvoorbeeld aan de banen van een actie van een groep G op X – dan kunnen we een deelverzameling $X_0 \subset X$ kiezen die uit elk van de deelverzamelingen $Y \in \mathcal{P}$ precies één element kiest.

Het keuzeaxioma is anders dan de andere axioma's van Zermelo en Fraenkel omdat die keuze van X_0 helemaal niet expliciet of constructief is.

Omdat het keuzeaxioma leidt tot stellingen zoals de Paradox van Banach-Tarski, is er in de eerste helft van de 20ste eeuw heel wat debat geweest over de status van dit keuzeaxioma. Banach en Tarski anticipeerden op de eerste twee pagina's van hun artikel [BT24] al op deze discussie, zie Figuur 3.2.

Ze herhalen eerst hun twee hoofdresultaten: uitspraak I is de formulering van de paradox in de driedimensionale ruimte (veelvlakken of polyeders kunnen in elkaar omgezet worden) en uitspraak II is de onmogelijkheid van een dergelijke paradox in het tweedimensionale vlak (veelhoeken of polygonen van verschillende grootte kunnen niet in elkaar omgezet worden).

Vervolgens leggen ze uit dat ze voor het bewijs van *beide* resultaten het keuzeaxioma nodig hebben en dat het gebruik van het keuzeaxioma in het bewijs van II veel meer substantieel is dan in het bewijs van I.

Kortom, ze stellen dat je meer keuzeaxioma nodig hebt om de "evidente waarheid" van de afwezigheid van de paradox in het vlak te bewijzen dan om de "evidente absurditeit" van de paradox in de ruimte te bewijzen.

Vandaag weten we dat het zonder het keuzeaxioma onmogelijk is om de paradox van Banach-Tarski te bewijzen. Er is echter wel een bewijs van II dat geen gebruikmaakt van het keuzeaxioma. Dat bewijs volgt een hele-

La démonstration des théorèmes précédents s'appuie sur les résultats de MM. Hausdorff, Vitali et Banach [1]), qui concernent le probléme général de mesure; elle fait donc usage de *l'axiome du choix* de M. Zermelo. Le rôle que joue cet axiome dans nos raisonnements nous semble mériter l'attention.

Envisageons, en effet, les deux théorèmes suivants, qui résultent de nos recherches:

I. Deux polyèdres arbitraires sont équivalents par décomposition finie.

II.[1]) Deux polygones différents, dont l'un est contenu dans l'autre, ne sont jamais équivalents par décomposition finie.

Or, on ne sait démontrer aucun de ces deux théorèmes sans faire appel à l'axiome du choix: ni le premier, qui semble peut-être paradoxal, ni le second, qui est en plein accord avec l'intuition. De plus, en analysant leurs démonstrations, on peut constater que l'axiome du choix intervient dans la démonstration du premier théorème sous une forme bien plus restreinte que dans le cas du second.

Figuur 3.2: Banach en Tarski over het Keuzeaxioma

maal andere methode, want het bestaan van een oppervlaktefunctie zoals in Stelling 3.4.1 kan je evenmin bewijzen zonder het keuzeaxioma. Je kan zonder het keuzeaxioma zelfs niet bewijzen dat de groep $\mathbb{Z}$ amenable is.

Als je het keuzeaxioma helemaal afzweert, dan verdwijnt heel veel van de gebruikelijke wiskunde. Zelfs heel wat van de gebruikelijke analyse en getaltheorie moet je dan opgeven. De overgrote meerderheid van de wiskundigen beschouwt het keuzeaxioma als een integraal deel van de fundamenten van de wiskunde. De overgrote meerderheid van de nieuwe wiskunde die iedere dag gepubliceerd wordt, maakt ergens impliciet gebruik van het keuzeaxioma, bijvoorbeeld omdat gesteund wordt op basisresultaten die op hun beurt steunen op het keuzeaxioma.

Alfred Tarski leverde heel wat belangrijke bijdragen tot de verzamelingenleer en wiskundige logica. Zo toonde hij in 1924 ook aan dat het keuzeaxioma volgt uit de veel onschuldigere bewering dat er voor elke oneindige verzameling X een bijectie bestaat tussen X en $X \times X$. Dit resultaat is gekend als de Stelling van Tarski. Hoewel dit vandaag als een belangrijk resultaat beschouwd wordt, had Tarski moeite om dit werk te publiceren. Hij vertelde aan Jan Mycielski, die dit neerschreef in [Myc06], dat hij zijn

artikel probeerde te publiceren in de *Comptes Rendus de l'Académie des Sciences de Paris*. Maar zowel Fréchet als Lebesgue weigerden om het artikel aan de academie te presenteren. Fréchet schreef dat een dergelijke implicatie tussen twee reeds gekende ware uitspraken geen nieuw resultaat was. En Lebesgue schreef dat een dergelijke implicatie tussen twee manifest foute uitspraken van geen belang was.

Je kan je natuurlijk afvragen in hoeverre het axiomasysteem van Zermelo en Fraenkel *consistent* is. Stel dat op een gegeven dag een wiskundige erin slaagt om uit de axioma's van Zermelo en Fraenkel een contradictie af te leiden, dan valt de hele wiskunde in duigen. Een dergelijke ramp zou alvast niet de schuld zijn van het keuzeaxioma. In 1938 bewees Gödel het volgende resultaat: als de axioma's van Zermelo en Fraenkel zonder het keuzeaxioma consistent zijn, dan zijn ze aangevuld met het keuzeaxioma nog altijd consistent.

In een van zijn fameuze onvolledigheidsstellingen uit 1931 bewees Gödel echter ook dat je binnen het axiomasysteem van Zermelo en Fraenkel nooit de consistentie van het systeem zelf kan bewijzen (tenzij het axiomasysteem inconsistent zou zijn, want dan kan je alles bewijzen). Als we de axiomatische methode van Zermelo en Fraenkel beschouwen als "de correcte manier om aan wiskunde te doen", wat inderdaad al meerdere decennia de standaard is, dan zegt de onvolledigheidsstelling van Gödel dat je met wat vandaag als de correcte wiskundige methode beschouwd wordt, niet kan bewijzen dat de wiskunde consistent is!

3.4.7 Uitbreiding: elke commutatieve groep is amenable

Schets van het bewijs van Propositie 3.4.5. We leggen eerst uit waarom de groep $\mathbb{Z}$ met de optelling amenable is. Hoewel het niet mogelijk is om een expliciet invariant gemiddelde op $\mathbb{Z}$ te construeren, kunnen we wel expliciet een *benaderend invariant gemiddelde construeren.*

Definieer voor elke $n \in \mathbb{N}$ en elke deelverzameling $U \subset \mathbb{Z}$

$$m_n(U) = \frac{\#(U \cap [-n, n])}{2n+1} \; .$$

Alle m_n voldoen aan eigenschappen (i), (ii) en (iii) in Definitie 3.4.2. Hoewel geen enkele m_n voldoet aan eigenschap (iv) in Definitie 3.4.2, geldt wel het volgende: voor alle $a \in \mathbb{Z}$ en alle deelverzamelingen $U \subset \mathbb{Z}$ zal

$$m_n(a + U) - m_n(U) \to 0 \; . \tag{3.6}$$

Een argument van compactheid – en het is hier dat we onnauwkeurig zijn – laat toe om $m(U)$ te definiëren als een limietpunt van de rij $m_n(U)$.

Eigenschappen (i), (ii) en (iii) zullen geldig blijven voor zo'n limietpunt, terwijl uit (3.6) zal volgen dat $m(a+U)-m(U)=0$, zodat ook eigenschap (iv) geldt.

Veronderstel nu dat G een willekeurige commutatieve groep is. We noteren de elementen van G met de letters $a, b, c, \ldots$ en we noteren de groepsoperatie als optelling $a+b$. In een eerste stap leggen we uit dat er voor elk eindig aantal elementen $a_1, \ldots, a_k$ van G een functie m bestaat die voldoet aan (i), (ii) en (iii), en die ook voldoet aan $m(a_i+U)=m(U)$ voor alle $i=1,\ldots,k$ en $U \subset G$. Kortom, in deze stap bewijzen we het bestaan van een gemiddelde dat invariant is onder het gegeven eindig aantal elementen $a_1, \ldots, a_k$.

Om deze eerste stap te bewijzen, definiëren we het groepshomomorfisme $\pi : \mathbb{Z}^k \to G : \pi(s) = s_1 a_1 + \cdots + s_k a_k$. Definieer voor alle $U \subset G$,

$$m_0(U) = \begin{cases} 1 & \text{als } 0 \in U, \\ 0 & \text{als } 0 \notin U. \end{cases}$$

Dan is m_0 een gemiddelde dat voldoet aan (i), (ii) en (iii). De precieze keuze van m_0 is trouwens irrelevant, zolang m_0 maar voldoet aan (i), (ii) en (iii).

Definieer voor alle $n \in \mathbb{N}$ en alle $U \subset G$,

$$m_n(U) = (2n+1)^{-k} \sum_{s \in [-n,n]^k} m_0(\pi(s)+U) \; .$$

Opnieuw gebruiken we een argument van compactheid om $m(U)$ te definiëren als limietpunt van $m_n(U)$. Net zoals in het argument voor de groep $\mathbb{Z}$, zal volgen dat de resulterende m nog steeds voldoet aan (i), (ii) en (iii), en dat m nu daarenboven voldoet aan $m(a_i+U)=m(U)$ voor alle $i=1,\ldots,k$.

Om het bewijs van Propositie 3.4.5 af te ronden, definiëren we voor elk element $a \in G$ de verzameling $\mathcal{M}_a$ van functies m die voldoen aan (i), (ii) en (iii), en die voldoen aan $m(a+U)=m(U)$ voor alle $U \subset G$. Uit de vorige stap volgt dat voor eindig veel elementen $a_1, \ldots, a_k$ de doorsnede

$$\mathcal{M}_{a_1} \cap \cdots \cap \mathcal{M}_{a_k}$$

niet-leeg is. Uit opnieuw een argument van compactheid zal volgen dat de doorsnede van alle $\mathcal{M}_a$, $a \in G$, niet-leeg is. Elk element m in die doorsnede is een invariant gemiddelde op G. □

3.4.8 Uitbreiding: amenability, normale deelgroepen en quotiëntgroepen

Schets van het bewijs van Propositie 3.4.6. Veronderstel eerst dat G amenable is. Uit Propositie 3.4.3 volgt dat N amenable is. Noteer met $\varphi : G \to G/N : \varphi(g) = gN$ het quotiënthomomorfisme. Neem een invariant gemiddelde m op G. Dan definieert de uitdrukking

$$m_{G/N}(U) = m(\varphi^{-1}(U)) \quad \text{waarbij} \quad \varphi^{-1}(U) = \big\{ g \in G \;\big|\; \varphi(g) \in U \big\}$$

een invariant gemiddelde op G/N. Dus is G/N amenable.

Veronderstel dan omgekeerd dat N en G/N amenable zijn. Neem een invariant gemiddelde m_N op N en een invariant gemiddelde $m_{G/N}$ op de quotiëntgroep G/N. Neem een deelverzameling $U \subset G$. We willen $m(U)$ definiëren en bewijzen dat m een invariant gemiddelde op G is.

Noteer zoals in paragraaf 3.4.4 met $I_{G/N}(F)$ de integraal t.o.v. $m_{G/N}$ voor een willekeurige begrensde functie $F : G/N \to \mathbb{R}$. Zoals in paragraaf 3.4.4 noteren we met $(gN) \cdot F$ de verschuiving van een functie $F : G/N \to \mathbb{R}$ met een element $gN \in G/N$.

Gegeven $U \subset G$, definiëren we de functie

$$F_U : G \to [0,1] : F_U(h) = m_N(h^{-1}U \cap N) \; .$$

Omdat m_N invariant is, volgt dat $F_U(hn) = F_U(h)$ voor alle $h \in G$ en $n \in N$. Je kan F_U dus beschouwen als een functie van G/N naar $[0,1]$, goed gedefinieerd als

$$F_U : G/N \to [0,1] : F_U(hN) = m_N(h^{-1}U \cap N) \; .$$

We definiëren $m(U) = I_{G/N}(F_U)$. We bewijzen dat m een invariant gemiddelde op G is. We moeten dus bewijzen dat m voldoet aan eigenschappen (i), (ii), (iii) en (iv) in Definitie 3.4.2.

(i) Omdat $0 \leq F_U(h) \leq 1$ voor alle $h \in G$, zal ook $I_{G/N}(F_U) \in [0,1]$, zodat $m(U) \in [0,1]$.

(ii) Omdat $F_\emptyset = 0$ en $F_G = 1$, zal $m(\emptyset) = 0$ en $m(G) = 1$.

(iii) Wanneer $U, V \subset G$ disjunct zijn, is $F_{U \cup V} = F_U + F_V$. Hieruit volgt dat $m(U \cup V) = m(U) + m(V)$.

(iv) Wanneer $U \subset G$ en $g \in G$, is $F_{gU} = (gN) \cdot F_U$. Hieruit en uit de invariantie van $I_{G/N}$ volgt dat $m(gU) = m(U)$. □

Bibliografie

[Ban24] S. Banach, *Un théorème sur les transformations biunivoques*. Fundam. Math. **6** (1924), 236–239. Downloaden[10]

[BT24] S. Banach en A. Tarski, *Sur la décomposition des ensembles de points en parties respectivement congruentes*. Fundam. Math. **6** (1924), 244–277. Downloaden[11]

[Day57] M.M. Day, *Amenable semigroups*. Ill. J. Math. **1** (1957), 509–544. Downloaden[12]

[Hau14] F. Hausdorff, *Bemerkung über den Inhalt von Punktmengen*. Math. Ann. **75** (1914), 428–434. Downloaden[13]

[Myc06] J. Mycielski, *A system of axioms of set theory for the rationalists*. Notices Amer. Math. Soc. **53** (2006), 206-213. Downloaden[14]

[Ols80] A.Y. Ol'shanskii, *On the problem of the existence of an invariant mean on a group*. Russian Math. Surveys **35** (1980), 180-181. Downloaden[15]

[Spa24] J. Spandaw, *Inleiding groepentheorie*. *Vakantiecursus Wiskunde*, Platform Wiskunde Nederland & Platform Wiskunde Vlaanderen, 2024, pp. 1–46. Hoofdstuk 1 van dit boek. Downloaden[16]

[Tao04] T. Tao, *The Banach-Tarski paradox*. Lecture notes UCLA. Downloaden[17]

[TW16] G. Tomkowicz en S. Wagon, *The Banach-Tarski paradox. Second edition*. Encyclopedia Math. Appl. **163**, Cambridge University Press, New York, 2016. Kopen[18]

[vNeu29] J. von Neumann, *Zur allgemeinen Theorie des Masses*. Fundam.

[10] eudml.org/doc/214277
[11] eudml.org/doc/214280
[12] doi.org/10.1215/ijm/1255380675
[13] gdz.sub.uni-goettingen.de/id/PPN235181684_0075
[14] www.ams.org/notices/200602/fea-mycielski.pdf
[15] iopscience.iop.org/article/10.1070/RM1980v035n04ABEH001876
[16] platformwiskunde.nl/vakantiecursus
[17] www.math.ucla.edu/∼tao/preprints/Expository/banach-tarski.pdf
[18] www.cambridge.org/core/books/banachtarski-paradox/9C1FEAACF5EF6EB51C99F67136C8FCCB

Math. **13** (1929), 73-116. Downloaden[19]

[Wap05] L.M. Wapner, *The pea and the sun: a mathematical paradox*. A.K. Peters Ltd., 2005.

[19] eudml.org/doc/211921

platform
wiskunde nederland

PLATFORM
WISKUNDE
VLAANDEREN