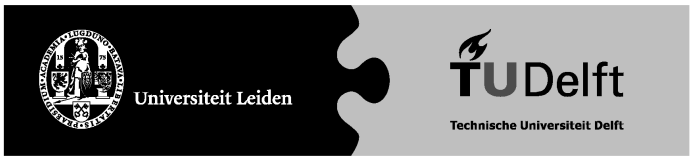
ALGEBRA I

P. Stevenhagen



2015

INHOUDSOPGAVE ALGEBRA I

Verschijningsdatum van deze oplage: januari 2015

Iedere volgende versie bevat hopelijk minder typefouten en onnauwkeurigheden dan de huidige – stuur hiertoe alle op- en aanmerkingen naar psh@math.leidenuniv.nl.

Postadres van de auteur:

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden

Voorwoord

Algebra 1 is het eerste van de drie colleges waaruit het algebra-curriculum aan de Universiteit Leiden bestaat. Met ingang van 2004 maakt dit college deel uit van de geïntegreerde Delfts-Leidse bacheloropleiding wiskunde.

De verdeling van de algebra over drie colleges komt grof gezegd overeen met de traditionele indeling groepen–ringen–lichamen. Dit correspondeert niet zozeer met een opklimmende moeilijkheidsgraad, als wel met een voortschrijdende 'specialisatie': een ring is een groep met een extra bewerking, en een lichaam is een ring met speciale mooie eigenschappen. Deze syllabus, die hoofdzakelijk aan groepentheorie gewijd is, is bedoeld als eerste kennismaking met de algebra. De vereiste voorkennis is gering, en sommige interessante voorbeelden van groepen, zoals matrixgroepen over eindige lichamen of fundamentaalgroepen van topologische ruimten, zullen daarom niet of nauwelijks aan de orde komen.

De lezer wordt geacht een idee te hebben van wat een wiskundig bewijs is, in het bijzonder een bewijs met *volledige inductie* of *uit het ongerijmde*. Eenvoudige begrippen uit de verzamelingenleer als *injectie*, *surjectie*, *bijectie* en *equivalentierelatie* worden zonder verdere uitleg gebruikt. Lineaire algebra is niet strikt noodzakelijk als voorkennis, maar een aantal van de voorbeelden en opgaven neemt bekendheid met basisbegrippen als *lineaire afbeelding*, *matrix* en *determinant* aan.

Een karakteristieke eigenschap van de algebra-syllabi is de grote hoeveelheid *opgaven*. Er zijn er meer dan er als huiswerk opgegeven of voorgemaakt kunnen worden, en iedereen moet voor zichzelf bepalen hoeveel opgaven hij aankan. Het blijkt in de praktijk dat algebra een vak is waarbij het niet voldoende is een aantal stellingen of trucs uit het hoofd te leren. Het is meer als met zwemmen: je kunt het niet leren door te kijken hoe anderen het doen, en als je het eenmaal kunt, begrijp je vaak niet meer wat er ooit zo moeilijk aan was. Het oefenen van zoveel mogelijk opgaven is daarom essentieel, en de tentaminering bestaat dan ook deels uit wekelijks in te leveren *huiswerkopgaven*—een beproefd middel dat bovendien de student veel academische vrijheid in de *keuze* van de opgaven laat. Opgaven met sterretjes zijn voor wie (nog) meer uitdaging zoekt. Ze vereisen een originele gedachte of gebruiken ideeën die enigszins buiten de stof vallen.

Deze syllabus bevat meer stof dan er in het college algebra 1 behandeld kan worden. Paragraaf 7 kan zonder meer worden overgeslagen. Het is mogelijk paragraaf 3 te beperken tot een behandeling van de orthogonale groep en zijn eindige ondergroepen, en het semidirecte product uit paragraaf 8 niet te behandelen. De aldus verkregen extra tijd kan dan besteed worden aan (delen van) de laatste twee paragrafen, die een iets volwassener kijk op de groepentheorie geven. Weer een andere mogelijkheid is reductie van de getaltheoretische paragraaf 6 ten gunste van de 'puur groepentheoretische' latere paragrafen.

Ter verhoging van de bruikbaarheid als naslagwerk is de syllabus voorzien van een uitgebreide index.

1 Wat is algebra?

Enigszins onzorgvuldig kan men zeggen dat de algebra de 'wiskundige structuren' die ons omringen axiomatiseert en in abstracto bestudeert[1]. Op de middelbare school, waar meestal met reële getallen wordt gemanipuleerd, betekent algebra vaak iets als 'rekenen met letters', waarbij veelvuldig haakjes worden weggewerkt of juist teruggehaald door 'uitvermenigvuldigen' dan wel 'ontbinden'. In de wiskunde komen veel meer interessante objecten voor dan alleen de reële getallen en functies daarop, en de algebra die wij zullen ontwikkelen wil in al deze gevallen toepasbaar zijn. Dit betekent dat de symbolen waar wij mee zullen 'rekenen' niet altijd getallen zullen zijn, maar ook vaak matrices, meetkundige afbeeldingen, permutaties van verzamelingen, of wat ons ook maar nuttig lijkt om één of ander probleem op te lossen.

Een wezenskenmerk van de moderne wiskunde is dat zij meestal niet een enkele functie, matrix of vergelijking bekijkt, maar indien mogelijk in één keer een hele verzameling van gelijksoortige objecten. In plaats van functies en matrices komt men daarom 'functieruimtes' en 'matrixgroepen' tegen; dit zijn grote, vaak oneindige collecties van functies dan wel matrices met bepaalde gemeenschappelijke eigenschappen—denk bijvoorbeeld aan verzamelingen van differentieerbare functies of inverteerbare matrices.

De algebra stelt axiomatische regels op voor het 'rekenen' met de elementen van dergelijke verzamelingen. Op het eerste gezicht klinkt dat misschien abstract en dor, meer als iets voor taxonomen of mensen met boekhoudkundige aspiraties. Het doel echter van een dergelijke minimalistische aanpak, waarin men uitgaande van een gering aantal axioma's interessante resultaten probeert af te leiden omtrent de structuur van de onderhavige verzameling, is *toepasbaarheid* en *duidelijkheid*. De axioma's die we in dit college tegen zullen komen zijn dan ook niet toevallige keuzen, maar dienen om interessante wiskunde te 'modelleren'. De abstracte wijze waarop we dit zullen doen heeft grote voordelen: het elimineren van overbodige aannamen en toevalligheden in een gegeven probleem leidt met geringe aanpassingen vaak tot een transparantere redenering en een beter begrip van de situatie. Ten slotte, en dat is misschien wel het belangrijkste, blijkt dat een algemeenheid die men op deze wijze ontdekt ook tot resultaten leidt in op het eerste gezicht totaal verschillende situaties.

De prijs die men voor de ontdekking van universele waarheden betaalt is de inspanning om zich een enigszins abstracte vorm van denken eigen te maken. Dat kost vaak enige tijd, en men ervaart algebra daarom in het begin soms als 'moeilijk'. De geschiedenis heeft echter geleerd dat het verwerven van enige algebraïsche vaardigheden ruimschoots de moeite loont, en sinds de dertiger jaren van de vorige eeuw is 'abstracte algebra' een essentieel instrument voor zowel zuivere als toegepaste wiskundigen.

▶ Groepen, ringen en lichamen

In deze syllabus zullen we ons voornamelijk bezighouden met de studie van verzamelingen waarop een enkele bewerking gedefinieerd is. De elementen van de verzameling zijn in den regel getallen, matrices of bepaalde afbeeldingen; de bewerking, die uit twee

[1] Zie voor deze en volgende referenties de sectie 'Literatuurverwijzingen'.

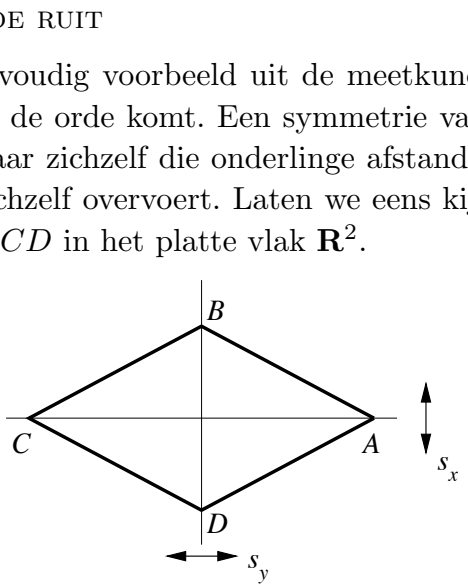
gegeven elementen een derde maakt, is meestal iets als optelling, vermenigvuldiging of samenstelling. De precieze axioma's, die we samenvatten door te zeggen dat de verzameling in kwestie door de gegeven bewerking tot een *groep* gemaakt wordt, stellen we uit tot definitie 2.1 in de volgende paragraaf.

Zoals we aan klassieke voorbeelden als getallen, polynomen en matrices al kunnen zien, komt het vaak voor dat een verzameling op een natuurlijke manier met zowel een optelling als een vermenigvuldiging uitgerust is; deze voldoen aan eenvoudige regeltjes als $a(b+c) = ab + ac$. Dergelijke objecten met twee bewerkingen, die *ringen* worden genoemd, komen overal in de wiskunde voor. We definiëren ze al in 6.8, maar stellen een systematische bestudering uit tot het college algebra 2. In de analyse en de lineaire algebra populaire voorbeelden van ringen zijn $\mathbf{R}$ en $\mathbf{C}$. Hierin kan men behalve optellen en vermenigvuldigen ook nog eens door alle elementen (verschillend van 0) *delen*—iets dat bijvoorbeeld in het geval van ringen van matrices veel minder eenvoudig ligt. Door deze mooie eigenschap zijn $\mathbf{R}$ en $\mathbf{C}$ standaardvoorbeelden van een type ringen dat *lichamen* genoemd wordt. De theorie van lichamen en de inclusies daartussen heet *Galoistheorie*, naar de op jonge leeftijd in een duel gesneuvelde ontdekker[2] Évariste Galois (1810–1831). In deze theorie manifesteerde het abstracte concept van een groep zich het eerst. Men draait tegenwoordig graag de historische volgorde om en bestudeert eerst abstracte groepen, om deze later in de Galoistheorie op effectieve wijze toe te passen. Ook wij zullen dat doen. Het blijkt namelijk dat de groepentheorie eenvoudiger voorbeelden en toepassingen kent dan de Galoistheorie, en dat deze het unificerende karakter van het groepsconcept duidelijker tot uitdrukking brengen.

In deze inleidende paragraaf zullen we enkele voorbeelden ten tonele voeren die duidelijk maken waarom de in 2.1 gegeven axioma's voor een groep nogal voor de hand liggen: het zijn eenvoudig de regeltjes waar het gros van de voorbeelden aan voldoet. De voorbeelden geven een goede indruk van wat we in dit vak tegen zullen komen, en laten zien dat eenzelfde groepsstructuur zich in verschillende gedaantes voor kan doen.

▶ Symmetrieën van de ruit

We beginnen met een eenvoudig voorbeeld uit de meetkunde, waarin het fundamentele begrip *symmetrie* aan de orde komt. Een symmetrie van een vlakke figuur is een afbeelding van het vlak naar zichzelf die onderlinge afstanden tussen punten bewaart en de gegeven figuur in zichzelf overvoert. Laten we eens kijken naar de symmetrieën van de afgebeelde ruit $ABCD$ in het platte vlak $\mathbf{R}^2$.



Twee symmetrieën springen direct in het oog: de ruit gaat in zichzelf over bij spiegeling

in de x-as of de y-as. Het is altijd zo dat het na elkaar uitvoeren van twee symmetrieën weer tot een symmetrie leidt: de *samenstelling*. Het is gemakkelijk in te zien dat de samenstelling $h = s_x \circ s_y$ van de beide spiegelingen in de coördinaatassen een halve draai om de oorsprong is. Merk op dat de *volgorde* waarin we de spiegelingen samenstellen er in dit geval niet toe doet. Doordat we de ruit symmetrisch om de oorsprong gekozen hebben, zijn de symmetrieën s_x, s_y en h *lineaire afbeeldingen* van $\mathbf{R}^2$ naar zichzelf. Wie van matrices houdt kan ze in matrixvorm representeren als

$$s_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad s_y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad h = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Men kan ook opmerken dat iedere symmetrie van de ruit vastligt door zijn werking op de hoekpunten, en een notatie voor die werking verzinnen die tot iets leidt als

$$s_x = (BD), \qquad s_y = (AC), \qquad h = (AC)(BD).$$

Het wordt al snel duidelijk dat we uit de drie gevonden symmetrieën geen nieuwe kunnen maken door samenstelling. Immers, de symmetrieën s_x, s_y en h zijn van *orde* 2, hetgeen betekent dat hun 'kwadraat' de *identiteit* is, de afbeelding die alle punten op hun plaats laat. Bovendien is het 'product' van twee verschillende symmetrieën uit ons drietal steeds de derde. Als we de identiteit als 'triviale symmetrie' meetellen, hebben we een verzameling van symmetrieën gevonden die *gesloten* is onder samenstelling van symmetrieën.

1.1. Stelling. *De verzameling $V_4 = \{\mathrm{id}, s_x, s_y, h\}$ is de volledige verzameling van symmetrieën van de ruit $ABCD$. De drie niet-triviale symmetrieën in V_4 zijn van orde* 2*, en het product van twee verschillende niet-triviale symmetrieën levert de derde.*

Bewijs. We moeten alleen nog laten zien dat er geen andere symmetrieën zijn dan de vier genoemde. Zij dus s een willekeurige symmetrie van de ruit. Omdat s de scherpe hoek A van de ruit alleen vast kan houden of in de andere scherpe hoek C over kan voeren geldt $s(A) = A$ of $(s_y \circ s)(A) = A$. Een symmetrie die A vasthoudt moet ook de andere scherpe hoek C vasthouden, en dat betekent dat hij óf de identiteit is, óf alleen de stompe hoeken B en D verwisselt, en dus gelijk is aan s_x. In het geval $s(A) = A$ hebben we $s = \mathrm{id}$ of $s = s_x$ en zijn we klaar. In het geval $(s_y \circ s)(A) = A$ hebben we $s_y \circ s = \mathrm{id}$ of $s_y \circ s = s_x$. In de identiteit $s_y \circ s = \mathrm{id}$ kunnen we links en rechts met s_y samenstellen, en wegens $s_y \circ s_y = \mathrm{id}$ leidt dit tot $s = s_y$. Voor $s_y \circ s = s_x$ leidt samenstellen met s_y tot $s = s_y \circ s_x = h$, de vierde en laatste mogelijkheid voor s. □

Opgave 1. Ga na welke eigenschappen van het samenstellen van afbeeldingen (in het bijzonder met betrekking tot het 'verplaatsen van haakjes') we hier gebruiken.

De verzameling V_4 van 4 elementen die we zojuist gevonden hebben bestaat uit een 'triviaal element' en drie elementen van orde 2 met de eigenschappen dat het product van twee van die elementen steeds het derde geeft. Deze 'structuur', die ook wel de *viergroep van Klein* heet, treedt op allerlei manieren op.

▶ Rekenen modulo 8

We laten zien hoe de viergroep van Klein ook in de getaltheorie optreedt. Ons doel is om alle gehele getallen x en y te vinden die voldoen aan de vergelijking

$$3x^2 + 2 = y^2. \tag{1.2}$$

Meetkundigen herkennen hierin de vergelijking van een hyperbool in het platte vlak en zeggen dat we kennelijk de punten met geheeltallige coördinaten willen bepalen op deze hyperbool.

Opgave 2. Teken in het platte vlak $\mathbf{R}^2$ de kromme met vergelijking $3x^2 + 2 = y^2$.

Door naar de vergelijking te kijken zien we gemakkelijk dat getallen x en y die aan vergelijking (1.2) voldoen óf beide even, óf beide oneven zijn. Schrijven we de vergelijking als $2 = y^2 - 3x^2$, dan wordt duidelijk dat x en y niet beide even kunnen zijn. Immers, omdat het kwadraat van een even getal deelbaar is door 4 (waarom?) is voor x en y even het getal $y^2 - 3x^2$ deelbaar door 4, en dus niet gelijk aan 2. We blijven zitten met de mogelijkheid dat x en y allebei oneven zijn.

We passen in het geval dat x en y oneven zijn een handigheidje toe dat wel 'rekenen modulo 8' wordt genoemd, en waarover we eerst een stelling gaan bewijzen. We merken op dat ieder oneven getal bij deling door 8 een rest geeft die gelijk is aan 1, 3, 5 of 7. Anders gezegd, de oneven getallen vallen uiteen in vier *restklassen modulo* 8 die we suggestief aan kunnen geven met $\overline{1}$, $\overline{3}$, $\overline{5}$ en $\overline{7}$. Nemen we nu bijvoorbeeld een element a uit de klasse $\overline{3}$ en een element b uit de klasse $\overline{5}$, dan is het niet moeilijk uit te rekenen in welke klasse ab ligt. Immers, indien we $a = 8a' + 3$ en $b = 8b' + 5$ schrijven met a' en b' geheel, dan vinden we $ab = (8a' + 3)(8b' + 5) = 8(8a'b' + 5a' + 3b') + 15$, en dit laat zien dat ab een 8-voud+15 is; dit is precies hetzelfde als een 8-voud+7, dus ab ligt in de restklasse $\overline{7}$. Omdat het resultaat er niet van afhangt welk element we precies kiezen in $\overline{3}$ en $\overline{5}$ zegt men vaak kortweg dat we de *klassen* $\overline{3}$ en $\overline{5}$ kunnen vermenigvuldigen, en noteert de hele berekening eenvoudig als $\overline{3} \cdot \overline{5} = \overline{15} = \overline{7}$.

Op soortgelijke wijze kunnen we elk tweetal restklassen uit de verzameling $V_4' = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ vermenigvuldigen. Vermenigvuldiging met $\overline{1}$ verandert een restklasse niet, dus de klasse $\overline{1}$ gedraagt zich als een soort identiteit. Men zegt wel dat $\overline{1}$ een *eenheidselement* is voor de vermenigvuldiging in V_4'. Voor andere producten vinden we allereerst

$$\overline{3} \cdot \overline{3} = \overline{5} \cdot \overline{5} = \overline{7} \cdot \overline{7} = \overline{1},$$

dus de elementen $\overline{3}$, $\overline{5}$ en $\overline{7}$ zijn elk 'van orde 2'. De identiteiten

$$\overline{3} \cdot \overline{5} = \overline{7}, \qquad \overline{3} \cdot \overline{7} = \overline{5} \quad \text{en} \quad \overline{5} \cdot \overline{7} = \overline{3}$$

laten zien dat het product van twee verschillende klassen in $\{\overline{3}, \overline{5}, \overline{7}\}$ steeds de derde klasse oplevert. Dit levert ons de volgende 'structuurstelling' voor de oneven restklassen modulo 8.

1.3. Stelling. *De verzameling* $V_4' = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ *van oneven restklassen modulo* 8 *heeft een natuurlijke vermenigvuldiging. Onder deze vermenigvuldiging is* $\overline{1}$ *een eenheidselement en zijn de drie overige elementen van orde* 2*. Het product van twee verschillende elementen van orde* 2 *in* V_4' *is gelijk aan het derde element van orde* 2*.* □

We gaan nu terug naar onze vergelijking $3x^2 + 2 = y^2$. Indien x en y oneven zijn, dan laat de structuurstelling 1.3 zien dat x^2 en y^2 in de klasse $\overline{1}$ zitten. Maar indien x^2 in $\overline{1}$ zit, dan zit $3x^2 + 2$ in $\overline{3 \cdot 1 + 2} = \overline{5}$. We concluderen dat $3x^2 + 2$ niet gelijk kan zijn aan y^2, en dat de vergelijking (1.2) geen geheeltallige oplossingen heeft.

Opgave 3. Laat zien dat de vergelijking $11x^2 + 1002 = 87y^2$ geen geheeltallige oplossingen heeft.

Vergelijken we de stellingen 1.1 en 1.3, dan zien we dat V_4 en V_4' kennelijk 'dezelfde structuur' hebben. Nog duidelijker wordt dit als we een *vermenigvuldigtafel* maken voor de waarden van de 'producten' ab van de elementen uit V_4 en V_4'.

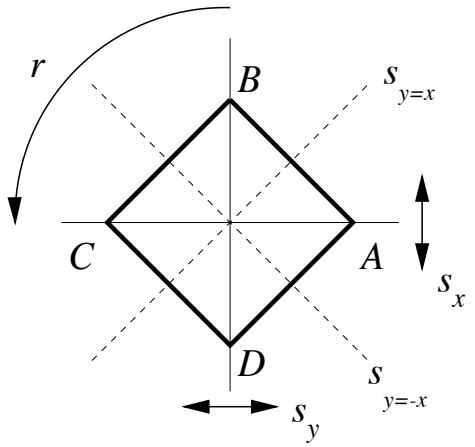
$a \downarrow\ b \rightarrow$	id	s_x	s_y	h
id	id	s_x	s_y	h
s_x	s_x	id	h	s_y
s_y	s_y	h	id	s_x
h	h	s_y	s_x	id

$a \downarrow\ b \rightarrow$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

De bijectie $f : V_4 \to V_4'$ gedefinieerd door $\mathrm{id} \mapsto \overline{1}$, $s_x \mapsto \overline{3}$, $s_y \mapsto \overline{5}$ en $h \mapsto \overline{7}$ heeft de eigenschap dat hij de vermenigvuldiging 'respecteert'. Men noemt zo'n f een *isomorfisme* en zegt dat de symmetriegroep V_4 en de vermenigvuldiggroep V_4' *isomorf* zijn.

► Symmetrieën van het vierkant

Een iets ingewikkelder voorbeeld, dat in eerste instantie erg lijkt op dat van de ruit $ABCD$, krijgen we door de ruit tot een vierkant $ABCD$ te deformeren en wederom te vragen wat de symmetrieën zijn. De symmetrieën in 1.1 zijn natuurlijk ook weer symmetrieën van het vierkant $ABCD$, maar we krijgen er nu meer.



Opvallende 'nieuwe' symmetrieën zijn de rotatie r over een kwartslag om de oorsprong, of de spiegelingen in de lijnen $y = x$ en $y = -x$. De kwartslag r is een symmetrie

van orde 4: pas na 4 keer toepassen van r krijgen we de identiteit. De 'driekwartslag' $r^3 = r \circ r \circ r$, die de *inverse* van r is, is ook een symmetrie van orde 4. De symmetrie r^2, die niets anders is dan h, heeft orde 2. We hebben naast de vier 'oude' symmetrieën uit 1.1 nu vier nieuwe gevonden, te weten r, r^3 en de genoemde spiegelingen. Enig proberen laat al snel zien dat uit deze 8 symmetrieën door samenstellen geen nieuwe te maken zijn.

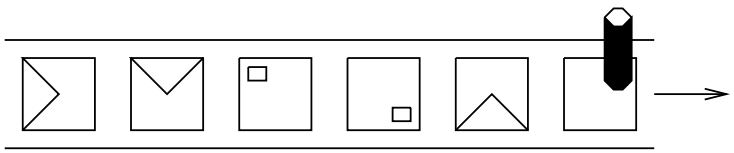
1.4. Stelling. *De verzameling D_4 van symmetrieën van het vierkant $ABCD$ heeft 8 elementen: de 4 rotaties om de oorsprong over veelvouden van $\pi/2$ en de spiegelingen in de 4 lijnen die de oorsprong met een hoekpunt of een middelpunt van een zijde verbinden.*

Bewijs. Laat s een symmetrie van het vierkant zijn. Door s met een aantal kwartslagen samen te stellen kunnen we een symmetrie krijgen die het hoekpunt A vasthoudt. Dan houdt deze symmetrie ook het hoekpunt C vast—immers B en D liggen dichter bij A dan C, dus een symmetrie (die afstanden bewaart) kan C daar niet heen sturen. Voor een symmetrie van het vierkant die A en C vasthoudt zijn er maar twee mogelijkheden: de identiteit en de spiegeling s_x, die B en D verwisselt. We concluderen dat we s door samenstellen met een 'macht' van r over kunnen voeren in de identiteit of de spiegeling s_x. In het eerste geval is s zelf één van de 4 machten van r, en dus gelijk aan één van de vier genoemde rotaties om de oorsprong. In het tweede geval hebben we een identiteit van het type

$$r^j \circ s = s_x,$$

waarbij we $j \in \{0, 1, 2, 3\}$ kunnen kiezen. Door links en rechts met een macht van r samen te stellen kunnen we ervoor zorgen dat links $r^4 \circ s = \mathrm{id} \circ s = s$ komt te staan, en dit geeft $s = r^k \circ s_x$ voor zekere k. Omdat er voor k weer vier keuzes zijn geeft dit 4 elementen, en de lezer mag nagaan dat dit de 4 genoemde spiegelingen zijn. □

Opgave 4. Een *poststempelmachine* is een apparaat dat op een lopende band vierkante enveloppen binnenkrijgt. De 'behandeling' van een envelop is het zetten van een stempel in een vaste (rechterboven)hoek. Tijdens het transport van de envelop op de band kan een robotarm de envelop een kwartslag met de klok mee draaien of (op één vaste manier) 'omdraaien', waarbij de onderkant boven komt.



Laat zien dat een postzegel op een normaal gefrankeerde envelop afgestempeld kan worden door de machine. Hoeveel handelingen van de robotarm zijn maximaal nodig?

Het bewijs van 1.4 laat zien dat we alle symmetrieën van het vierkant kunnen maken door herhaald samenstellen van r en s_x. Men zegt wel dat de groep D_4 van symmetrieën van het vierkant *voortgebracht wordt* door r en s_x.

Een complicatie bij de symmetriegroep D_4, die zich voor de symmetriegroep V_4 van de ruit niet voordoet, is dat de *volgorde* van de samenstelling nu een belangrijke rol speelt. Zo zijn bijvoorbeeld $r \circ s_x$ en $s_x \circ r$ *niet* dezelfde spiegeling in D_4. Wie ooit met matrices gerekend heeft zal hierdoor niet verrast worden, maar wie tot dusverre alleen

maar met reële getallen gerekend heeft, moet zich hiervan goed rekenschap geven. We zeggen wel dat de elementen r en s_x van D_4 niet *commuteren*.

Door de elementen van D_4 in de vorm $r^i s_x^j$ te schrijven met $i \in \{0,1,2,3\}$ en $j \in \{0,1\}$ kunnen we snel elementen in D_4 vermenigvuldigen. De rekenregels $r^{i_1} \cdot r^{i_2} = r^{i_1+i_2}$ en $s_x^{j_1} \cdot s_x^{j_2} = s_x^{j_1+j_2}$ liggen voor de hand. Hierbij nemen we de exponenten respectievelijk modulo 4 en modulo 2. Het 'niet-commuteren' van r en s_x wordt uitgedrukt door de rekenregel

$$s_x \circ r^i = r^{-i} \circ s_x,$$

die de lezer bij wijze van oefening af mag leiden uit de relatie $(r^i \circ s_x) \circ (r^i \circ s_x) = \mathrm{id}$. (Immers, $r^i \circ s_x$ is een spiegeling en heeft dus orde 2.) Merk op dat de elementen s_x en $r^2 = h$, die we kennen uit V_4, wél commuteren.

Opgave 5. Schrijf het product $s_x \circ r \circ s_x \circ r^2 \circ r^{-1} \circ s_x$ in de vorm $r^i s_x^j$.

We kunnen de symmetrieën van het vierkant net als voor de ruit ook weer aangeven door hun werking op de hoekpunten. In de al voor de ruit gesuggereerde *cykelnotatie* krijgen we dan

$$\begin{array}{ll} r^0 = \mathrm{id} = (A) & s_x = (BD) \\ r = (ABCD) & r \circ s_x = s_{y=x} = (AB)(CD) \\ r^2 = h = (AC)(BD) & r^2 \circ s_x = s_y = (AC) \\ r^3 = r^{-1} = (ADCB) & r^3 \circ s_x = s_{y=-x} = (AD)(BC). \end{array}$$

Binnen een cykel wordt steeds ieder punt door de symmetrie op het volgende punt in de cykel afgebeeld, en het laatste punt van de cykel op het eerste. Zo staat $(ABCD)$ voor de permutatie $A \mapsto B \mapsto C \mapsto D \mapsto A$. Punten die vastgehouden worden, vermelden we niet in de notatie—behalve in het geval van de identiteit, waar we maar (A) schrijven.

▶ Permutaties van 4 elementen

De door ons bekeken verzamelingen V_4 en D_4 kunnen we opvatten als deelverzamelingen van de verzameling S_4 van *alle* permutaties van de vier punten van de verzameling $\{A,B,C,D\}$. Een permutatie van een verzameling is zoals bekend een bijectieve afbeelding van een verzameling naar zichzelf, en voor de verzameling $\{A,B,C,D\}$ zijn er $4! = 24$ verschillende permutaties. Met onze zojuist ingevoerde cykelnotatie hebben we een korte manier om ze op te schrijven.

Opgave 6. Schrijf de 24 elementen van S_4 op in cykelnotatie en bepaal hun orde.

De inclusies $V_4 \subset D_4 \subset S_4$ geven aanleiding tot een *deelbaarheid* van de cardinaliteiten 4, 8 en 24 van de verzamelingen. Verder blijkt de orde van een element in elk van de verzamelingen V_4, D_4 en S_4 steeds een deler van het aantal elementen in de verzameling te zijn. We zullen in 4.8 zien dat het hier algemene eigenschappen van groepsinclusies en ordes betreft.

Op de verzameling S_4 hebben we net als op V_4 of D_4 een natuurlijke samenstelling van de elementen. Het 'product' van twee permutaties is immers weer een permutatie.

We schrijven $\alpha \circ \beta$ of kortweg $\alpha\beta$ voor de samenstelling van de permutaties α en β, en spreken ook wel van het *product* van α en β. Merk op dat $\alpha\beta$ betekent: eerst β, dan α toepassen. Zoals we zagen zijn $\alpha\beta$ en $\beta\alpha$ niet altijd hetzelfde.

Opgave 7. Maak een vermenigvuldigtafel voor D_4. Hoe blijkt uit zo'n tafel dat er elementen zijn die niet met elkaar commuteren?

We merkten al op dat de elementen $r = (ABCD)$ en $s_x = (BD)$ alle symmetrieën in D_4 *voortbrengen*: dit betekent dat iedere symmetrie door herhaald toepassen van r en s_x verkregen kan worden. Men kan zich afvragen of de verzameling S_4 op soortgelijke wijze voortgebracht kan worden met een paar elementen; dat is bijvoorbeeld interessant voor wie een sorteermachine wil bouwen. Er zijn heel veel mogelijke keuzes. Men kan bijvoorbeeld de *transposities* in S_4 nemen. Dit zijn per definitie permutaties die twee elementen verwisselen en alle andere op hun plaats laten. Het aantal van dergelijke elementen in S_4 bedraagt $\binom{4}{2} = 6$.

1.5. Stelling. *Zij σ een permutatie van een eindige verzameling X. Dan is σ een product van transposities.*

Bewijs. Noem de elementen van de verzameling $1, 2, 3, \ldots, n$, met n het aantal elementen van X. We voeren het bewijs met volledige inductie naar n. Voor $n = 1$ is σ de identiteit, en dat is het product van 0 transposities.

Stel nu dat iedere permutatie van een verzameling van $n-1$ elementen een product van transposities is. Als voor onze permutatie $\sigma(n) = n$ geldt, dan is σ op te vatten als een permutatie van een verzameling van $n - 1$ elementen en zijn we klaar. Stel dus $\sigma(n) = k \neq n$. Dan is het product $(k\,n) \circ \sigma$ van σ met de transpositie $(k\,n)$ een permutatie die n op zijn plaats laat (waarom?), en we zagen al dat dit betekent dat $(k\,n) \circ \sigma$ een product van transposities is. Vermenigvuldigen we dit product met $(k\,n)$, dan hebben we een product van transposities dat gelijk is aan $(k\,n) \circ (k\,n) \circ \sigma = \sigma$. □

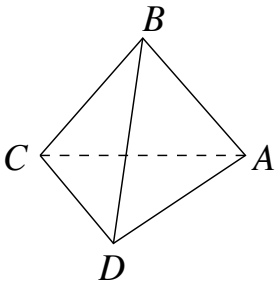
Opgave 8. Laat zien dat ieder element van S_4 als een product van niet meer dan 3 transposities geschreven kan worden.

Het voorafgaande bewijs, waarin we niet $n = 4$ maar willekeurige n namen, laat zien dat het soms gemakkelijk kan zijn een *algemenere* uitspraak te bewijzen. Men spreekt in dergelijke gevallen wel van *verzwaarde inductie*. Een iets subtieler voorbeeld van dit fenomeen wordt gegeven in de laatste opgave van deze paragraaf.

▶ Ruimtelijke symmetrieën

Wij hebben V_4 en D_4 geïntroduceerd als verzamelingen van symmetrieën, en men kan zich afvragen of de abstracte 'permutatieverzameling' S_4 van $\{A, B, C, D\}$ ook zo te interpreteren is. Met punten in het vlak lukt dat niet zo gemakkelijk, maar heel eenvoudig gaat het met ruimtelijke symmetrieën. Dergelijke symmetrieën, die meestal iets moeilijker te visualiseren en te classificeren zijn dan vlakke symmetrieën, worden uitgebreid bestudeerd in de kristallografie. De optredende symmetrieverzamelingen heten *kristallografische groepen*.

Als we de punten A, B, C, D als hoekpunten van een tetraëder nemen, treedt S_4 op als de verzameling van symmetrieën van de tetraëder. Immers, omdat iedere symmetrie eenduidig bepaald is door zijn werking op de hoekpunten vormen de symmetrieën van de tetraëder een deelverzameling van S_4. Omdat samenstellingen van symmetrieën weer symmetrieën geven is het vanwege stelling 1.5 voldoende te laten zien dat de transposities als symmetrieën optreden.



Om bijvoorbeeld de transpositie (AB) te maken neemt men het vlak dat de zijde AB loodrecht middendoor deelt. Omdat de driehoeken ABC en ABD gelijkzijdig zijn liggen C en D in dit vlak. Spiegelen we nu in dit vlak, dan krijgen we de symmetrie die A en B verwisselt en C en D op hun plaats laat.

Het tetraëdervoorbeeld laat zien dat we met 'abstracte argumenten' over permutatieverzamelingen iets meetkundigs kunnen bewijzen over de symmetrieën van een tetraëder. Wie niet van dergelijke indirecte manieren houdt mag natuurlijk ook proberen zich voor te stellen welke ruimtelijke transformatie bijvoorbeeld de hoekpunten A, B, C, D verwisselt in een 4-cykel $(ABCD)$.

Opgaven.

9. Het *symmetrisch verschil* van twee verzamelingen A en B is gedefinieerd als

$$A \,\Delta\, B = (A \cup B) \setminus (A \cap B).$$

Zij X een verzameling met twee elementen, en V de collectie van deelverzamelingen van X. Laat zien dat V een verzameling van 4 elementen is, en dat deze verzameling onder de bewerking Δ de structuur van een viergroep van Klein krijgt.

10. Laat zien dat de verzameling van gehele getallen die niet door 2 of 3 deelbaar zijn uiteenvalt in vier restklassen modulo 12. Is de natuurlijke vermenigvuldigingsstructuur op deze vier klassen die van de viergroep van Klein? Zelfde vraag voor de vier restklassen modulo 5 van de gehele getallen niet deelbaar door 5.

11. Laat zien dat de vergelijking $3x^2 + 2 = y^2$ geen oplossing heeft met x en y oneven door $x = 2a + 1$ en $y = 2b + 1$ te schrijven en een pariteitsargument te gebruiken. (Een *pariteitsargument* is een net woord voor een 'even-oneven-beschouwing'.)

12. Laat zien dat de vergelijking $3x^2 + 2 = y^2$ geen geheeltallige oplossingen heeft door te rekenen modulo 3. Bewijs ook dat de vergelijking geen *rationale* oplossingen heeft.

13. Definieer V_4 en V_4' als in de stellingen 1.1 en 1.3. Laat zien dat er precies 6 verschillende isomorfismen $V_4 \to V_4'$ bestaan.

14. Geef de matrixrepresentaties voor de elementen van D_4. Geeft dit een snellere manier om elementen in D_4 te vermenigvuldigen?

15. Bepaal de verzameling van symmetrieën van een gelijkzijdige driehoek in het vlak. Commuteren deze symmetrieën onder samenstelling?

16. Kan elke permutatie van $\{A, B, C, D\}$ ook gemaakt worden uit de transposities (AB), (BC) en (CD)? Of uit de transpositie (AB) en de 4-cykel $(ABCD)$? Hoeveel vermenigvuldigingen zijn er in deze gevallen maximaal nodig?

17. Laat zien dat de deelverzameling $H \subset D_4$ voortgebracht door de symmetrieën $r \circ s_x$ en $r^3 \circ s_x$ van het vierkant een viergroep van Klein is, en niet gelijk aan $V_4 = \{\mathrm{id}, s_x, s_y, h\}$. [Men kan dus niet spreken van *de* inclusie $V_4 \subset D_4$.]

18. Bepaal de deelverzameling van S_4 die voortgebracht wordt door de acht 3-cykels in S_4. *Kun je bewijzen dat je antwoord correct is?

19. Bestaat er een vierhoek $ABCD$ in het vlak met S_4 als verzameling van symmetrieën?

20. Zij $n > 2$ een geheel getal. Laat zien dat de verzameling van symmetrieën van een regelmatige n-hoek rond de oorsprong in het vlak uit $2n$ elementen bestaat: de n rotaties om de oorsprong over veelvouden van $2\pi/n$ en de spiegelingen om de n lijnen die de oorsprong met een hoekpunt of een midden van een zijde verbinden.

21. Laat zien dat de verzameling van symmetrieën van de eenheidscirkel in het vlak bestaat uit de rotaties om de oorsprong en de spiegelingen in de lijnen door de oorsprong.

*22. Kan de verzameling in de voorafgaande opgave worden voortgebracht met een *eindig* aantal symmetrieën?

23. Bepaal de verzameling van symmetrieën van het onderstaande (oneindige) ruitjespatroon.

Laat zien dat de verzameling met drie spiegelingen kan worden voortgebracht.

24. Laat zien dat er precies 48 ruimtelijke symmetrieën zijn die een gegeven kubus in zichzelf overvoeren. Commuteert ieder tweetal van deze symmetrieën?

25. Laat zien dat de vergelijking $55x^3 + 3 = y^3$ geen geheeltallige oplossingen heeft. [Hint: kijk naar restklassen modulo 7 of 9.]

*26. *(Puzzeltje na de jaarwisseling....)* Bewijs dat de vergelijking

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \ldots + \frac{1}{x_{2014}} + \frac{1}{x_{2015}} = 1$$

maar eindig veel oplossingen in positieve gehele getallen x_i heeft.

2 Permutatiegroepen

De verzamelingen V_4, D_4 en S_4 uit de vorige paragraaf zijn concrete voorbeelden van *groepen*, die we nu algemeen zullen definiëren. We gaan vervolgens in enig detail in op het belangrijke voorbeeld van de *permutatiegroep*.

▶ De groepsaxioma's

Een *bewerking* of *compositievoorschrift* op een verzameling G is een afbeelding

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \circ b, \end{aligned}$$

oftewel een functie die aan elk geordend paar (a, b) van elementen uit G een *compositie* of *samenstelling* $a \circ b$ van a en b in G toevoegt. In plaats van '$\circ$' kan men elk willekeurig symbool gebruiken om $a \circ b$ aan te geven, bijvoorbeeld $a * b$ of $a\#b$. Omdat echter geen enkel belang gediend is bij het gebruik van exotische symbolen schrijven we vaak eenvoudig ab voor $a \circ b$, en noemen de samenstelling van a en b het *product*.

Een *eenheidselement* of *identiteit* voor een bewerking op G is een element $e \in G$ met de eigenschap dat voor alle $a \in G$ de gelijkheden $e \circ a = a \circ e = a$ gelden. Merk op dat er slechts één zo'n element kan zijn: als $e_1, e_2 \in G$ beide eenheidselement zijn, dan geldt $e_1 = e_1 \circ e_2 = e_2$.

2.1. Definitie. *Een verzameling G voorzien van een bewerking $\circ$ heet een groep als aan de volgende drie voorwaarden is voldaan.*

(G1) *G bevat een eenheidselement e voor de bewerking $\circ$;*

(G2) *voor elk drietal elementen $a, b, c \in G$ geldt de associatieve eigenschap*

$$a \circ (b \circ c) = (a \circ b) \circ c;$$

(G3) *voor elk element $a \in G$ bestaat er een element $a^\dagger \in G$ met*

$$a \circ a^\dagger = a^\dagger \circ a = e.$$

Het element $a^\dagger$ in (G3), dat de *inverse* van a wordt genoemd, is uniek bepaald door a. Immers, als $a^\dagger$ en $a^\ddagger$ beide inversen zijn van $a \in G$, dan geldt wegens (G1) en (G2)

$$a^\dagger = a^\dagger \circ e = a^\dagger \circ (a \circ a^\ddagger) = (a^\dagger \circ a) \circ a^\ddagger = e \circ a^\ddagger = a^\ddagger.$$

We kunnen in het vervolg dus verder spreken van *de* inverse van een element, net als we *het* eenheidselement in de groep hebben.

De *groepsaxioma's* (G1), (G2) en (G3) in 2.1 zijn zo gekozen dat veel 'natuurlijke voorbeelden' eraan voldoen. De lezer kan bijvoorbeeld nagaan dat hieronder in het bijzonder de voorbeelden V_4, D_4 en S_4 uit de vorige paragraaf vallen.

Opgave 1. Vormt de verzameling $\mathbf{R}$ van reële getallen een groep onder optelling? En onder vermenigvuldiging?

In de *multiplicatieve notatie* voor de groepsbewerking, die we in deze paragraaf zullen gebruiken, noteert men de inverse van a als a^{-1}. Men schrijft a^n voor een product $a \circ a \circ \ldots \circ a$ van n factoren a, en a^{-n} voor het n-voudig product $a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1}$. Merk op dat het vanwege de associatieve eigenschap (G2) niet nodig is haakjes te zetten in een meervoudig product: de uitkomst hangt daar niet van af.

Men definieert $a^0 = e$ voor alle $a \in G$, zodat voor alle $m, n \in \mathbf{Z}$ de identiteit $a^m a^n = a^{m+n}$ geldt. Algemener is het handig om een product met nul factoren, het *lege product*, per definitie gelijk te nemen aan het eenheidselement e.

Een product $a_1 a_2 a_3 \ldots a_n$ van n elementen $a_i \in G$ wordt wel geschreven als $\prod_{i=1}^{n} a_i$. De *volgorde* van de factoren in zo'n product is belangrijk: het product ab is niet in het algemeen gelijk aan ba. Als dit wel zo is zeggen we dat a en b *commuteren*. Voor niet-commuterende elementen a en b kunnen $(ab)^n = ab\,ab\,ab \ldots ab$ en $a^n b^n = a\,a\,a \ldots ab\,b\,b \ldots b$ totaal verschillend zijn.

Groepen waarin alle elementen met elkaar commuteren heten *abelse groepen*, naar de Noorse wiskundige Niels Henrik Abel[2] (1802–1829).

Opgave 2. Laat zien dat de inverse van het product ab van twee elementen a en b gelijk is aan

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

Deze 'sokken-en-schoenenregel' zegt dat als je het aantrekken van sokken en schoenen ongedaan wilt maken, je eerst schoenen en dan sokken uit moet trekken: de omgekeerde volgorde.

▶ Ordes van groepen en elementen

Het aantal elementen van G, dat zowel eindig als oneindig kan zijn, heet de *orde* van G en wordt aangegeven met $\#G$. De *triviale groep*, die alleen uit een eenheidselement bestaat, heeft orde 1 en is daarmee de 'kleinst mogelijke groep'. Notatie: $G = 1$.

De *orde* van een element $a \in G$ is het kleinste positieve getal n waarvoor $a^n = e$ geldt. Bestaat zo'n n niet, dan zeggen we dat de orde van a oneindig is. In een eindige groep hebben alle elementen eindige orde. Er geldt de volgende preciezere uitspraak.

2.2. Propositie. *Zij G een groep en $a \in G$ een element.*

1. *Als a oneindige orde heeft, dan zijn alle elementen in de rij $(a^k)_{k \in \mathbf{Z}}$ van positieve en negatieve machten van a verschillend.*
2. *Als a eindige orde n heeft, dan zijn er precies n verschillende machten van a, en de rij $(a^k)_{k \in \mathbf{Z}}$ van machten van a is periodiek met periode n.*

Bewijs. Stel dat er twee verschillende waarden $i, j \in \mathbf{Z}$ bestaan, zeg $i > j$, waarvoor $a^i = a^j$ geldt. Vermenigvuldig dan links en rechts met a^{-j}, dan volgt $a^{i-j} = a^{j-j} = a^0 = e$, dus a heeft eindige orde. Dit bewijst (1).

Heeft a eindige orde n, dan laat bovenstaand argument zien dat de machten a^i voor $i = 0, 1, 2, \ldots, n-1$ allemaal verschillend zijn. Omdat voor $i \in \mathbf{Z}$ de gelijkheid $a^{i+n} = a^i a^n = a^i e = a^i$ geldt is de rij van machten van a periodiek met periode n en zijn er precies n verschillende machten. □

Een element $a \in G$ van eindige orde heet ook wel een *torsie-element*: de machten van a 'draaien in een kringetje rond'. In een eindige groep zijn alle elementen torsie.

Opgave 3. Welke macht in het rijtje $e, a, a^2, \ldots, a^{n-1}$ is de inverse van a?

In de voorbeelden in de vorige paragraaf hebben we veelvuldig gebruik gemaakt van de drie *groepsaxioma's* (G1), (G2) en (G3). Zoals de bewijzen van 1.1, 1.4 en 2.2 laten zien gebruiken we ze vaak in de vorm van de equivalentie

$$ax = b \iff x = a^{-1}b \tag{2.3}$$

voor elementen $a, b, x \in G$. Deze equivalentie stelt ons in staat om bij een identiteit in een groep elementen naar de andere kant van een gelijkheid te transporteren. Wat we in feite doen—en dat is het bewijs van (2.3)—is links en rechts vermenigvuldigen met hetzelfde groepselement. Vermenigvuldigen we in de identiteit $ax = b$ aan beide kanten van links met het element a^{-1}, dan zien we dat $a^{-1}(ax) = (a^{-1}a)x = ex = x$ gelijk is aan $a^{-1}b$. Omgekeerd volgt uit de identiteit $x = a^{-1}b$ door linksvermenigvuldiging met a de identiteit $ax = b$.

Uit (2.3) lezen we af dat de afbeelding $\lambda_a : G \to G$ gegeven door $x \mapsto ax$, de *linksvermenigvuldiging* met $a \in G$, bijectief is: voor elke $b \in G$ is er een uniek element $x \in G$ dat door linksvermenigvuldiging met a op b wordt afgebeeld. De inverse van deze afbeelding wordt gegeven door linksvermenigvuldiging met a^{-1}, en wegens (G2) geldt $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Opgave 4. Bewijs de equivalentie $xa = b \iff x = ba^{-1}$. Concludeer dat de rechtsvermenigvuldiging $x \mapsto xa$ met $a \in G$ een bijectie $\rho_a : G \to G$ geeft. Bewijs: $\rho_a \circ \rho_b = \rho_{ba}$.

▶ Permutatiegroepen

Alle in de vorige paragraaf optredende groepen bestaan uit bijecties van één of andere verzameling naar zichzelf. In de rest van deze paragraaf kijken we naar het 'standaard-voorbeeld' van de groep van *alle* bijecties van een verzameling naar zichzelf.

2.4. Stelling. *Zij X een verzameling. Dan is de verzameling $S(X)$ van bijecties $X \to X$ met als bewerking de samenstelling van afbeeldingen een groep.*

Bewijs. Merk eerst op dat een samenstelling van twee bijecties $X \to X$ weer een bijectie geeft. Om (G1) te bewijzen merken we op dat de identiteit id_X zich inderdaad als identiteit gedraagt met betrekking tot de compositie: $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$ voor alle $f \in S(X)$. De associatieve eigenschap is in dit geval een algemeenheid over het samenstellen van afbeeldingen. Er geldt namelijk voor elk drietal afbeeldingen

$$X_1 \xrightarrow{f} X_2 \xrightarrow{g} X_3 \xrightarrow{h} X_4$$

tussen verzamelingen de identiteit $h \circ (g \circ f) = (h \circ g) \circ f$. Nemen we $X_1 = X_2 = X_3 = X_4 = X$, dan krijgen we eigenschap (G2) voor $S(X)$. De inverse f^{-1} van een bijectie $f \in S(X)$ is de inverse afbeelding in de zin van de verzamelingentheorie, die precies gedefinieerd is door eigenschap (G3): $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$. □

De groep $S(X)$ in 2.4 is een zeer algemeen voorbeeld van een groep, want zoals de *stelling van Cayley* in 5.8 laat zien is *iedere* groep G op te vatten als een groep van bijecties van G naar zichzelf.

De groep $S(X)$ behorende bij een verzameling X heet[3] de *permutatiegroep* of *symmetrische groep* op X. In het geval dat X een eindige verzameling van n elementen is geven we deze groep aan met S_n. De verzameling S_4 van permutaties van de verzameling $\{A, B, C, D\}$ in de vorige paragraaf is inderdaad de permutatiegroep S_4 op 4 letters. Zoals we al zagen is de orde van deze groep gelijk aan $4! = 24$. Algemener heeft de permutatiegroep S_n orde $n!$. Immers, voor een bijectie van een verzameling van n elementen naar zichzelf heeft men voor het beeld van het eerste element n mogelijkheden, daarna voor het beeld van het tweede element nog $n-1$, voor het derde nog $n-2$, en zo verder tot er voor het n-de element nog maar 1 mogelijkheid is. Dit geeft $n(n-1)(n-2)\ldots 2\cdot 1 = n!$ mogelijkheden.

Opgave 5. Laat zien dat S_n niet abels is voor $n \geq 3$.

▶ Cykelnotatie

In de vorige paragraaf introduceerden we een cykelnotatie voor de elementen van S_4, die in het gebruik aanzienlijk praktischer is dan het geven van een complete lijst van originelen en beelden. Een element $\sigma \in S(X)$ heet een *k-cykel* of *cyclische permutatie van lengte k* als er k verschillende elementen $x_1, x_2, \ldots, x_k \in X$ bestaan zo dat σ de identiteit is op $X \setminus \{x_1, x_2, \ldots, x_k\}$ en op $\{x_1, x_2, \ldots, x_k\}$ werkt als de cyclische verschuiving

$$x_1 \longmapsto x_2 \longmapsto x_3 \longmapsto \ldots \longmapsto x_{k-1} \longrightarrow x_k$$

We noteren zo'n element als $\sigma = (x_1\ x_2\ x_3\ \ldots\ x_{k-1}\ x_k)$. Deze notatie is slechts éénduidig op cyclische verschuiving na, omdat bijvoorbeeld $(x_1\ x_2\ x_3)$ en $(x_2\ x_3\ x_1)$ dezelfde permutatie aangeven. Een 1-cykel is hetzelfde als de identiteit id_X.

Twee cykels $(x_1\ x_2\ x_3\ \ldots\ x_{k-1}\ x_k)$ en $(x'_1\ x'_2\ x'_3\ \ldots\ x'_{\ell-1}\ x'_\ell)$ in $S(X)$ heten *disjunct* als geen enkel element x_i gelijk is aan een x'_j. Merk op dat disjuncte cykels altijd commuteren.

Voor $X = \{A, B, C, D\}$ gebruikten we in onze inleidende paragraaf al de volgende intuïtief duidelijke stelling.

2.5. Stelling. *Zij X een eindige verzameling. Dan is iedere permutatie $\sigma \in S(X)$ te schrijven als een product van disjuncte cykels.*

Bewijs. We voeren het bewijs met inductie naar $n = \#X$. Voor de triviale groep S_1 is er niets te bewijzen. Immers, het eenheidselement is wegens onze afspraak over lege producten gelijk aan het product van *nul* disjuncte cykels. (Wie zich daar ongemakkelijk bij voelt kan het eenheidselement ook als een 1-cykel schrijven.) De stelling is in ieder geval correct voor $n = 1$.

Neem aan dat de stelling waar is voor verzamelingen met minder dan n elementen, en neem een permutatie $\sigma \in S(X)$ voor een verzameling X met n elementen. Kiezen we $x \in X$, dan komen er in de oneindige rij x, $\sigma(x)$, $\sigma^2(x)$, $\ldots$ slechts eindig veel verschillende elementen voor. Laat $k > 0$ het kleinste positieve getal zijn

waarvoor we $\sigma^j(x) = \sigma^k(x)$ hebben, met $j \in \{0, 1, 2, \ldots, k-1\}$. Passen we op deze gelijkheid σ^{-j} toe, dan vinden we $\sigma^{k-j}(x) = \sigma^{j-j}(x) = x$, dus vanwege de minimaliteit van k hebben we $j = 0$ en $\sigma^k(x) = x$. De elementen van de verzameling $X_0 = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)\}$ zijn nu verschillend, en σ werkt hierop als de k-cykel

$$\sigma_0 = (x \quad \sigma(x) \quad \sigma^2(x) \quad \ldots \quad \sigma^{k-2}(x) \quad \sigma^{k-1}(x)).$$

Omdat σ een bijectie op X is die de deelverzameling $X_0 \subset X$ op zichzelf afbeeldt, wordt ook het complement $X \setminus X_0$ door σ op zichzelf afgebeeld. Omdat $X \setminus X_0$ uit $n - k < n$ elementen bestaat kunnen we de beperking van σ tot deze verzameling schrijven als een product van disjuncte cykels. Vermenigvuldigen we dit product met de cykel σ_0, dan hebben we een schrijfwijze voor σ als product van disjuncte cykels. □

Opgave 6. Bereken het product $(1\ 2)(2\ 3)(3\ 4)\ldots(n-1\ n)$, en leid hiermee 1.5 uit 2.5 af.

Om elementen van S_n in cykelnotatie aan te geven moet men een verzameling van n elementen kiezen. Een standaardkeuze voor zo'n verzameling is $\{1, 2, 3, \ldots, n-1, n\}$.

2.6. Voorbeeld. Een element van S_{12} kunnen we aangeven door een 2×12-matrix

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 1 & 11 & 10 & 3 & 4 & 7 & 2 & 12 & 6 & 8 & 9 \end{pmatrix}.$$

Hierbij bestaat iedere kolom uit een element en zijn bijbehorende beeld. Men vindt de disjuncte cykelrepresentatie van σ door een element te kiezen, zeg 1, en te kijken wat onder herhaald toepassen van σ het beeld wordt. We vinden $1 \mapsto 5 \mapsto 3 \mapsto 11 \mapsto 8 \mapsto 2 \mapsto 1$, een cykel van lengte 6. Kies nu een element buiten deze cykel, bijvoorbeeld 4, en herhaal dit procédé. We vinden $4 \mapsto 10 \mapsto 6 \mapsto 4$, een 3-cykel. Er blijven nog elementen buiten deze cykels over, want we hebben nog maar $6 + 3 = 9$ van de 12 elementen gehad. Het element 7, dat op zijn plaats blijft en een 1-cykel geeft, hoeven we niet op te schrijven. Nemen we 9, dan krijgen we nog de 2-cykel (9 12). Het resultaat van de berekening is

$$\sigma = (1\ 5\ 3\ 11\ 8\ 2)(4\ 10\ 6)(9\ 12).$$

Opgave 7. Laat zien dat bovenstaand element $\sigma \in S_{12}$ orde 6 heeft, en bereken de verschillende machten van σ.

Op soortgelijke wijze vinden we de disjuncte cykelrepresentatie van een element dat gegeven is als product van niet-disjuncte cykels, zoals $\tau = (1\ 4\ 3\ 6)(7\ 1\ 6)(2\ 7\ 6\ 5) \in S_7$. Het beeld van 1 onder τ berekent men door eerst (2 7 6 5) toe te passen (resultaat: 1), dan (7 1 6) (resultaat: 6) en ten slotte (1 4 3 6) (resultaat: 1). Dus τ laat 1 vast. Voor 2 vinden we $2 \mapsto 7 \mapsto 1 \mapsto 4$, dus $\tau(2) = 4$. Zo doorgaande krijgen we $\tau(4) = 3$, $\tau(3) = 6$, $\tau(6) = 5$ en ten slotte $\tau(5) = 2$. Dit geeft de 5-cykel (2 4 3 6 5), en omdat behalve 1 ook 7 vastgehouden wordt door τ is τ gelijk aan deze 5-cykel.

Opgave 8. Schrijf de elementen $\sigma, \tau \in S_{12}$ gegeven door respectievelijk

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 5 & 1 & 11 & 10 & 3 & 4 & 7 & 2 & 12 & 6 & 8 \end{pmatrix} \text{ en } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 2 & 12 & 6 & 8 & 9 & 5 & 1 & 11 & 10 & 3 & 4 \end{pmatrix}$$

als producten van disjuncte cykels, en doe hetzelfde voor $\sigma\tau$ en $\tau\sigma$.

De disjuncte cykelrepresentatie van een element $\sigma \in S_n$ is in essentie uniek: twee zulke representaties kunnen slechts verschillen in de volgorde van de cykels en in het al of niet opnemen van cykels van lengte 1. De cykels in de disjuncte cykelrepresentatie van σ corresponderen met de *banen* waarin de verzameling $\{1, 2, \ldots, n\}$ onder het herhaald toepassen van σ uiteenvalt: i en j komen voor in dezelfde cykel dan en slechts dan als i door herhaald toepassen van σ in j kan worden overgevoerd. Een punt in een baan van lengte 1 correspondeert met een element dat door σ op zijn plaats wordt gelaten en heet een *dekpunt* van de permutatie σ.

Als $\sigma \in S_n$ een product van t disjuncte cykels van lengte $k_1, k_2, \ldots, k_t$ is, waarbij we tevens alle cykels van lengte 1 mee tellen, dan geldt $k_1 + k_2 + k_3 + \ldots + k_t = n$. We noemen het rijtje $(k_1, k_2, k_3, \ldots, k_t)$ het *cykeltype* van σ; hierbij is de volgorde van de termen niet van belang. Een cykeltype $(k_1, k_2, k_3, \ldots, k_t)$ is in feite niets anders dan een manier om n als een som van positieve getallen k_i te schrijven. Men noemt de 'opdeling' $(k_1, k_2, k_3, \ldots, k_t)$ van n daarom ook wel een *partitie* van n. Voor het element $\sigma \in S_{12}$ in 2.6 is het cykeltype $(6, 3, 2, 1)$, hetgeen correspondeert met de partitie $12 = 6+3+2+1$.

Opgave 9. Bepaal alle cykeltypes die optreden in S_4 en S_5, en bepaal tevens voor ieder cykeltype hoeveel permutaties er zijn met dit type.

▶ Ondergroepen, cyclische groepen

Aan het voorbeeld van de groep S_4 in §1, die D_4 en V_4 bevatte, zien we dat een groep diverse deelverzamelingen kan bevatten die zelf ook weer groepen zijn. We spreken in zo'n geval van *ondergroepen*.

2.7. Definitie. *Een deelverzameling H van een groep G heet een ondergroep van G als hij aan de volgende voorwaarden voldoet:*

(H1) *H bevat het eenheidselement van G;*
(H2) *voor elk tweetal elementen $a, b \in H$ geldt $ab \in H$;*
(H3) *voor ieder element $a \in H$ geldt $a^{-1} \in H$.*

Eis (H2) zegt dat de beperking van de bewerking $G \times G \to G$ tot $H \times H$ beeld in H heeft, en dus een bewerking op H definieert. Vanwege (H1) en (H3) bevat H een eenheidselement en inversen voor deze bewerking. De associativiteit van de bewerking op H volgt direct uit de associativiteit op G. We concluderen dat een ondergroep $H \subset G$ met de bewerking van G weer een groep is. Omgekeerd ziet men gemakkelijk in dat iedere deelverzameling van een groep G die met de bewerking van G een groep vormt een ondergroep van G is in de zin van 2.7.

Iedere groep G bevat een *triviale ondergroep* $H = \{e\}$. We schrijven hiervoor meestal kortweg $H = 1$. Ook de 'hele groep' $H = G$ is altijd een ondergroep van G.

Opgave 10. Laat zien dat een deelverzameling $H \subset G$ een ondergroep van G is dan en slechts dan als hij aan de volgende voorwaarden voldoet:

(H1′) H is niet-leeg;
(H2′) voor elk tweetal elementen $a, b \in H$ geldt $ab^{-1} \in H$.

Er is een makkelijke manier om uitgaande van één of meer elementen in een groep een kleinste ondergroep te construeren die deze elementen bevat.

2.8. Lemma. *Zij S een deelverzameling van een groep G, en $S^{-1} = \{s^{-1} : s \in S\}$. Laat $\langle S\rangle \subset G$ de verzameling van elementen zijn die geschreven kunnen worden als een eindig product van elementen $s \in S \cup S^{-1}$. Dan is $\langle S\rangle$ een ondergroep van G, en de kleinste ondergroep van G die S bevat.*

Bewijs. We gaan de eisen (H1)–(H3) na voor de deelverzameling $\langle S\rangle \subset G$.

Als S leeg is, dan bevat $\langle S\rangle$ alleen het lege product, dat gelijk is aan e, en is $\langle S\rangle$ de triviale ondergroep van G. Algemeen is aan (H1) automatisch voldaan.

Als a en b producten zijn van elementen $s \in S \cup S^{-1}$, dan is ab ook zo'n product, dus $\langle S\rangle$ voldoet aan (H2). Is $a = s_1 s_2 \dots s_t$ een product van elementen $s_i \in S \cup S^{-1}$, dan geldt wegens de 'sokken-en-schoenenregel' $a^{-1} = s_t^{-1} s_{t-1}^{-1} \dots s_2^{-1} s_1^{-1}$. Voor elk element $s_i \in S \cup S^{-1}$ is de inverse s_i^{-1} ook weer in $S \cup S^{-1}$ bevat, dus er geldt $a^{-1} \in \langle S\rangle$ en aan (H3) is voldaan. We concluderen dat $\langle S\rangle$ een ondergroep is van G.

Iedere ondergroep $H \subset G$ die S bevat, bevat S^{-1} wegens (H3), en $(S \cup S^{-1}) \subset H$ impliceert $\langle S\rangle \subset H$ wegens (H2). □

Opgave 11. Laat zien dat, voor $S \subset G$, de verzameling van eindige producten van elementen uit S niet noodzakelijk een ondergroep is van G. Is dit wel zo als G eindig is?

De ondergroep $\langle S\rangle$ in 2.8 heet de ondergroep van G *voortgebracht door* S. Geldt $\langle S\rangle = G$, dan zeggen we dat G *voortgebracht wordt* door S of dat S een verzameling *voortbrengers* van G is. Een groep die door een eindige verzameling van elementen wordt voortgebracht heet *eindig voortgebracht*. Eindige groepen zijn altijd eindig voortgebracht: we kunnen eenvoudig $S = G$ nemen. Voor kleine S, zoals $S = \{a\}$ of $S = \{a, b\}$, vermijdt men accolades en noteert $\langle S\rangle$ als $\langle a\rangle$ of $\langle a, b\rangle$. Zo heeft men voor de ondergroepen V_4 en D_4 van S_4 in §1 bij de nummering $A = 1$, $B = 2$, $C = 3$ en $D = 4$ van de hoekpunten A, B, C en D

$$\begin{aligned} V_4 &= \langle (1\ 3), (2\ 4)\rangle, \\ D_4 &= \langle (2\ 4), (1\ 2\ 3\ 4)\rangle, \\ S_4 &= \langle (1\ 2), (1\ 2\ 3\ 4)\rangle. \end{aligned}$$

Merk op dat de verkregen injecties $V_4 \to S_4$ en $D_4 \to S_4$ berusten op een *keuze* van de nummering van de hoekpunten. Zie opgave 48.

Opgave 12. Geef een expliciete nummering van $\{A, B, C, D\}$ die aanleiding geeft tot injecties $V_4 \to S_4$ en $D_4 \to S_4$ met een *ander* beeld.

Een groep voortgebracht door 1 element heet een *cyclische groep*. Hij bestaat uit de positieve en negatieve machten van de voortbrenger. Als $a \in G$ oneindige orde heeft, dan heeft de cyclische ondergroep $\langle a\rangle \subset G$ wegens 2.2.1 eveneens oneindige orde. Als $a \in G$ eindige orde n heeft, dan heeft $\langle a\rangle$ wegens 2.2.2 eveneens orde n. Zo is bijvoorbeeld $C_4 = \langle (1\ 2\ 3\ 4)\rangle$ een cyclische ondergroep van S_4 van orde 4. In 4.8 zullen we zien dat in een eindige groep iedere ondergroep een orde heeft die de groepsorde deelt. Door naar cyclische ondergroepen te kijken volgt hieruit dat ordes van elementen in eindige groepen altijd *delers* van de groepsorde zijn.

Opgave 13. Laat zien dat de groepen V_4, D_4 en S_4 niet cyclisch zijn.

Voor een deelverzameling $S \subset S_n$ van meer dan één element geldt (in een precies te maken betekenis[4]) al snel $\langle S \rangle = S_n$. Zie de opgaven 54–56 voor voorbeelden van kleine verzamelingen die S_n voortbrengen.

▶ De tekenafbeelding

We besluiten deze paragraaf met de constructie van een ondergroep $A_n \subset S_n$ die de *alternerende groep* op n elementen wordt genoemd. De constructie berust op het toekennen van een *teken* $\varepsilon(\sigma) \in \{\pm 1\}$ aan een permutatie $\sigma \in S_n$.

2.9. Lemma. *Er bestaat een unieke afbeelding $\varepsilon : S_n \longrightarrow \{\pm 1\}$ met de volgende twee eigenschappen:*
(1) *Als σ een transpositie is, dan geldt $\varepsilon(\sigma) = -1$;*
(2) *Voor elementen $\sigma, \tau \in S_n$ geldt $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.*

Bewijs. Nemen we $\sigma = \tau = \mathrm{id} \in S_n$ in (2), dan zien we dat ε in ieder geval de identiteit naar 1 stuurt, en zijn we voor $n = 1$ direct klaar. Voor $n \geq 2$ weten we wegens stelling 1.5 dat ieder element als een niet-leeg product van transposities geschreven kan worden, dus het is duidelijk dat er *ten hoogste* één afbeelding ε is met de eigenschappen (1) en (2). Omdat een gegeven permutatie echter op heel veel verschillende manieren als product van transposities geschreven kan worden is het geenszins duidelijk dat zo'n afbeelding bestaat.

We definiëren ε door te kijken naar de functie $F : \mathbf{R}^n \to \mathbf{R}$ gegeven door

$$F(x_1, x_2, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

We merken allereerst op dat F niet de nulfunctie is. Voor $\sigma \in S_n$ beschouwt men nu de functie $\sigma F : \mathbf{R}^n \to \mathbf{R}$ gegeven door

$$(\sigma F)(x_1, x_2, \ldots, x_n) = F(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Deze functie is op teken na gelijk aan F, en we definiëren $\varepsilon(\sigma)$ door

$$\sigma F = \varepsilon(\sigma) F.$$

Neemt men σ gelijk aan een transpositie $(i\ j)$, dan ontstaat σF uit F door de factor $x_i - x_j$ in de definitie van F door $x_j - x_i$ te vervangen. Immers, alle andere factoren die x_i of x_j bevatten kunnen we paarsgewijs samennemen, met één paar per element $k \neq i, j$. Voor iedere k krijgen we één van de onderstaande vier paren, afhankelijk van de ligging van k ten opzichte van i en j,

$$(x_i - x_k)(x_j - x_k), \qquad (x_i - x_k)(x_k - x_j), \qquad (x_k - x_i)(x_j - x_k), \qquad (x_k - x_i)(x_k - x_j)$$

en ieder van deze factoren is invariant onder de transpositie $(i\ j)$. Dit laat zien dat $\varepsilon(\sigma) = -1$ geldt voor een transpositie σ.

Uit de relatie $(\sigma\tau)(F) = \sigma(\tau F)$ vinden we gemakkelijk $\varepsilon(\sigma\tau)F = \varepsilon(\sigma)\varepsilon(\tau)F$, en hieruit zien we dat ε ook aan (2) voldoet. □

In plaats van het teken spreekt men ook wel van de *pariteit* van een permutatie. Permutaties $\sigma \in S_n$ met $\varepsilon(\sigma) = 1$ heten *even*, die met $\varepsilon(\sigma) = -1$ *oneven*. Stelling 1.5 zegt dat iedere permutatie een product van transposities is, maar een dergelijke schrijfwijze is niet uniek. Zo kan men de 4-cykel (1 2 3 4) bijvoorbeeld schrijven als

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2) = (2\ 3)(1\ 2)(1\ 3)(2\ 4)(2\ 3).$$

Uit 2.9 zien we echter dat de *pariteit* van het aantal transposities in zo'n schrijfwijze kennelijk wel uniek bepaald is: (1 2 3 4) is *niet* te schrijven als het product van twee, vier of zes transposities. De pariteit van een permutatie is dus hetzelfde als de pariteit van het aantal transposities dat men nodig heeft om deze permutatie te krijgen.

Voor een k-cykel hangt de pariteit $\varepsilon(\sigma)$ slechts van k af. De identiteit

$$(1\ 2)(2\ 3)(3\ 4)(4\ 5)\ldots(k-1\ k) = (1\ 2\ 3\ 4\ \ldots k-1\ k)$$

laat zien dat een k-cykel $\sigma \in S_n$ pariteit $\varepsilon(\sigma) = (-1)^{k-1}$ heeft. Voor $\sigma \in S_n$ van cykeltype $(k_1, k_2, k_3, \ldots, k_t)$ vinden we

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^{t}(k_i-1)} = (-1)^{n-t}.$$

Het bewijs van 2.9 laat nog zien dat de pariteit van een permutatie σ ook de pariteit is van het aantal *inversies* dat σ induceert. Een inversie is een paar (i, j) van indices in $\{1, 2, \ldots, n\}$ waarvoor de ongelijkheden $i < j$ en $\sigma(i) > \sigma(j)$ gelden.

Uit de in 2.9.2 verwoorde *multiplicativiteit* van de tekenafbeelding leiden we gemakkelijk af dat de deelverzameling A_n van even permutaties in S_n een ondergroep is. Allereerst is de identiteit $\mathrm{id} \in S_n$ als product van nul transposities een even permutatie, dus aan (H1) voldaan. Voor alle $\sigma \in S_n$ hebben we nu de identiteit $1 = \varepsilon(\mathrm{id}) = \varepsilon(\sigma\sigma^{-1}) = \varepsilon(\sigma)\varepsilon(\sigma^{-1})$. Deze laat zien dat σ en σ^{-1} hetzelfde teken hebben. Hieruit volgt (H3). Eigenschap (H2) ten slotte is ook een direct gevolg van de multiplicatieve eigenschap in 2.9.2: het product van twee even permutaties is weer even.

We zullen later zien dat de alternerende groep A_n in diverse situaties opduikt. Voor $n = 4$ zagen we in opgave 1.18 dat A_4 voortgebracht wordt door 3-cykels.

2.10. Stelling. *De alternerende groep A_n is de ondergroep van S_n voortgebracht door de 3-cykels. De orde van A_n is $\frac{1}{2}n!$ voor alle $n \geq 2$.*

Bewijs. De eerste uitspraak is correct (maar triviaal) voor $n \leq 2$. Om voor $n \geq 3$ te laten zien dat A_n voortgebracht wordt door de 3-cykels merken we eerst op dat wegens de identiteit

$$(*) \qquad (x\ y\ z) = (x\ y)(y\ z)$$

iedere 3-cykel $(x\ y\ z) \in S_n$ een even permutatie is. Omdat een even permutatie het product van een even aantal transposities is, is het nu verder voldoende te laten zien dat ieder product van twee transposities $\sigma, \tau \in S_n$ te schrijven is als een product van 3-cykels. Voor $\sigma = \tau$ is dit duidelijk, immers dan is $\sigma\tau = \mathrm{id}$, en voor σ en τ verschillend maar niet disjunct volgt het uit $(*)$. In het disjuncte geval kunnen we met een handigheidje $(*)$ ook toepassen:

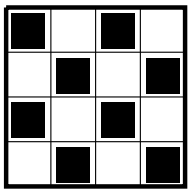
$$(a\ b)(c\ d) = (a\ b)(b\ c) \cdot (b\ c)(c\ d) = (a\ b\ c)(b\ c\ d).$$

Om in te zien dat er voor $n \geq 2$ evenveel even als oneven permutaties in S_n te vinden zijn kiezen we een transpositie in S_n (hier is $n \geq 2$ nodig!) en beschouwen de bijectie $S_n \to S_n$ gegeven door linksvermenigvuldiging met deze transpositie. Deze bijectie verwisselt de even en de oneven permutaties, dus er moeten van beide soorten evenveel zijn. Omdat S_n van orde $n!$ is volgt dat A_n orde $\frac{1}{2}n!$ heeft. □

► Puzzeltje van Loyd

Als recreationele toepassing van het pariteitsbegrip voor permutaties bekijken we een bekend puzzeltje genoemd[5] naar de Amerikaanse puzzelaar Sam Loyd (1841–1911). Men dient 15 blokjes in een vierkant doosje door schuiven in de juiste volgorde te brengen, en indien men aan het eind in de hieronder links afgebeelde situatie raakt lukt het niet om door handig schuiven de blokjes 14 en 15 te verwisselen.

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



WA	AR	IS	HI
ER	HE	TP	AR
IT	EI	TS	PR
OB	EM	LE	

Om te *bewijzen* dat dit onmogelijk is geven we het 'ontbrekende blokje' het nummer 16, en merken op dat een 'zet' in dit spelletje bestaat uit een verwisseling van blokje 16 en een naburig blokje. Wat we uitvoeren zijn kennelijk transposities in de permutatiegroep S_{16}. Als na een aantal zetten blokje 16 zich weer rechtsonder bevindt, dan is dit aantal zetten *even* geweest: immers, in het aangegeven 'schaakbordpatroon' beweegt blokje 16 steeds van een zwart blokje naar een wit blokje, dus na een oneven aantal zetten bevindt hij zich nooit op een zwart blokje. Het product van een even aantal transposities is een *even* permutatie, en dat kan niet de gewenste transpositie (14 15) zijn.

Opgave 14. Laat zien dat het andere afgebeelde puzzeltje, waar de blokjes 'LE' en 'EM' verwisseld moeten worden, wél oplosbaar is.

Veel puzzeltjes van deze soort, zoals de bekende *kubus van Rubik*[6], hebben aanzienlijk ingewikkelder symmetriegroepen dan het puzzeltje van Loyd. Men kan echter op soortgelijke manier vaak de onmogelijkheid van bepaalde oplossingen aantonen.

Opgaven.

In onderstaande opgaven wordt met G steeds een groep aangegeven.

15. Ga in elk van de onderstaande gevallen na of de bewerking $*$ een groepsstructuur op X definieert, en of deze abels is.
    $a * b = ab$ voor $a, b \in X = \mathbf{R} \setminus \{0\}$;
    $a * b = a + b - 1$ voor $a, b \in X = \mathbf{R}$;
    $a * b = a^{\log b}$ voor $a, b \in X = \mathbf{R}_{>1}$;
    $a * b = \max\{a, b\}$ voor $a, b \in X = \mathbf{R}$.

16. De *commutator* van twee elementen $a, b \in G$ is het element $[a, b] = aba^{-1}b^{-1}$. Laat zien dat $ab = [a, b]ba$ geldt, en concludeer dat a en b commuteren dan en slechts dan als de commutator $[a, b]$ gelijk is aan e.

17. Stel dat $(ab)^{-1} = a^{-1}b^{-1}$ geldt voor alle $a, b \in G$. Bewijs dat G abels is.

18. Stel dat $(ab)^n = a^n b^n$ geldt voor alle $a, b \in G$ en alle $n > 1$. Bewijs dat G abels is.

19. Stel dat $a^2 = e$ geldt voor alle $a \in G$. Bewijs dat G abels is.

20. Laat zien dat $a^4 = e$ geldt voor alle $a \in D_4$, en dat D_4 niet abels is.

*21. Bestaat er een niet-abelse groep G met de eigenschap dat $a^3 = e$ geldt voor alle $a \in G$?

22. Laat zien dat in iedere rij en in iedere kolom van de vermenigvuldigtafel van een eindige groep elk element precies één keer voorkomt.

23. Zij G een groep van orde 4. Bewijs: G is óf cyclisch, óf de viergroep van Klein.

24. Zij G een verzameling met een element $e \in G$ en een bewerking $\circ$ die voldoen aan (G2) en de *rechtsaxioma's*:
    (G1′): Voor alle $a \in G$ geldt $a \circ e = a$;
    (G3′): Elk element $a \in G$ heeft een rechtsinverse $a^\dagger \in G$ met de eigenschap $a \circ a^\dagger = e$.
    Bewijs dat G met de bewerking $\circ$ een groep is.

25. Zij X een verzameling. De collectie $P(X)$ van deelverzamelingen van X heet de *machtsverzameling* van X. Definieer het product van twee deelverzamelingen $A, B \in P(X)$ als het symmetrisch verschil $A \,\Delta\, B$. Laat zien dat $P(X)$ hiermee een abelse groep wordt.

26. Zij X een eindige verzameling. Bereken de orde van de groep $P(X)$ uit de vorige opgave, en de orde van de elementen in $P(X)$.

27. Bewijs dat iedere doorsnede $\bigcap_i H_i$ van ondergroepen $H_i \subset G$ een ondergroep van G is.

28. Laat zien dat de vereniging $H_1 \cup H_2$ van twee ondergroepen H_1 en H_2 van G een ondergroep is dan en slechts dan als $H_1 \subset H_2$ of $H_2 \subset H_1$ geldt.

29. Een *keten* van ondergroepen in G is een collectie $\{H_i\}_{i \in I}$ van ondergroepen $H_i \subset G$ met de eigenschap dat voor ieder tweetal ondergroepen H_i, H_j in de collectie een inclusie $H_i \subset H_j$ of $H_j \subset H_i$ geldt. Laat zien dat een eindige keten van $n \geq 1$ ondergroepen bij geschikte indicering voldoet aan

$$H_1 \subset H_2 \subset H_3 \subset \ldots \subset H_{n-1} \subset H_n,$$

en bewijs algemeen dat de vereniging $\bigcup_{i\in I} H_i$ van een niet-lege keten een ondergroep van G is.

30. Bepaal alle ondergroepen van S_3. Wat zijn de ordes van deze ondergroepen?

31. Zij G een eindige *abelse* groep en $x \in G$ willekeurig. Bewijs: $\prod_{g\in G} xg = \prod_{g\in G} g$. Leid hieruit af dat de orde van x de groepsorde deelt.
[Dit is ook waar als G niet abels is: zie 4.8.]

32. Definieer $\sigma, \tau \in S_5$ door $\sigma = (1\ 5)(2\ 4)$ en $\tau = (1\ 2\ 3\ 4\ 5)$. Bepaal de commutator $[\sigma, \tau]$ en de orde van de ondergroep $H = \langle \sigma, \tau \rangle \subset S_5$.

33. Als de vorige opgave, maar nu met $\sigma = (1\ 5)$.

34. Laat zien dat in definitie 2.7 voor *eindige* deelverzamelingen $H \subset G$ de eis (H3) weggelaten kan worden. Laat tevens zien dat dit niet in het algemeen kan.

35. Laat a en b torsie-elementen zijn in een abelse groep G. Bewijs: ab is een torsie-element.

36. Zij $X = \mathbf{Z}$ de verzameling van de gehele getallen, en laat $\sigma, \tau \in S(X)$ gegeven worden door respectievelijk $\sigma(x) = -x$ en $\tau(x) = 1 - x$ voor $x \in \mathbf{Z}$. Laat zien dat σ en τ orde 2 hebben, en dat $\sigma\tau$ en $\tau\sigma$ oneindige orde hebben.

37. Geef een voorbeeld van een oneindige groep G waarin ieder element eindige orde heeft.

38. Zij G een eindig voortgebrachte *abelse* groep waarin elk element eindige orde heeft. Bewijs dat G eindig is.

39. Zij G een eindige groep en $S \subset G$ een deelverzameling van orde $\#S > \frac{1}{2}\#G$. Bewijs: $G = \langle S \rangle$.

40. Zij G een groep van orde $\#G < 1000$. Bewijs dat G met minder dan 10 elementen kan worden voortgebracht.

*41. Zij G een oneindige groep. Bewijs: G is eindig voortgebracht $\Rightarrow$ G is aftelbaar oneindig. Geldt de omkering?

*42. Zij X een oneindige verzameling. Bewijs dat $S(X)$ niet eindig voortgebracht is.

43. Twee elementen $x, y \in G$ heten *geconjugeerd* als $y = gxg^{-1}$ geldt voor zekere $g \in G$. Bewijs dat 'geconjugeerd zijn' een *equivalentierelatie* is op de verzameling van elementen van G. De equivalentieklassen heten de *conjugatieklassen* van G.

44. Zij G een eindige groep. Bewijs dat alle conjugatieklassen van G evenveel elementen hebben dan en slechts dan als G abels is.

45. Laat zien dat geconjugeerde elementen in een groep dezelfde orde hebben.

46. Laat zien dat voor $\tau \in S_n$ willekeurig en $\sigma = (x_1\ x_2\ \ldots\ x_k) \in S_n$ een k-cykel de geconjugeerde $\tau\sigma\tau^{-1}$ gelijk is aan

$$(\tau(x_1)\ \tau(x_2)\ \ldots\ \tau(x_k)).$$

Leid hieruit af dat twee elementen in S_n geconjugeerd zijn dan en slechts dan als ze hetzelfde cykeltype hebben.

47. Zij $H \subset G$ een ondergroep en $g \in G$ een element. Bewijs dat de met H *geconjugeerde ondergroep* $gHg^{-1} = \{ghg^{-1} : h \in H\}$ weer een ondergroep is van G.

48. Laat zien dat verschillende keuzen van nummeringen in opgave 12 aanleiding geven tot beelden van V_4 in S_4 die geconjugeerd zijn, en evenzo voor D_4. Hoeveel mogelijke beelden krijgen we in elk van beide gevallen? *Zijn dit *alle* mogelijke beelden onder groepsinbeddingen van V_4 en D_4 in S_4?

49. Zij $\sigma \in S_n$ een product van t disjuncte cykels van lengte $k_1, k_2, \ldots, k_t$. Bewijs dat de orde van σ gelijk is aan het kleinste gemene veelvoud van de getallen k_i. Concludeer dat voor ieder element $\sigma \in S_n$ de orde van σ een deler is van de orde van S_n.

50. Zij X een verzameling en $H \subset S(X)$ een ondergroep. Laat zien dat de relatie $\sim$ op X gedefinieerd door
$$x \sim y \iff (\exists \tau \in H : y = \tau x)$$
een equivalentierelatie is, en concludeer dat X een disjuncte vereniging van H*-banen* is. Wat zijn deze banen als X eindig is en H de cyclische ondergroep voortgebracht door een element $\sigma \in S(X)$?

51. Zij $X = \{1, 2, 3 \ldots\}$ de verzameling van positieve natuurlijke getallen, en vat S_n op als ondergroep van $S(X)$ door zijn natuurlijke werking op $\{1, 2, 3, \ldots, n\}$. Laat zien dat $H = \bigcup_{n>0} S_n$ een ondergroep is van $S(X)$. Is H gelijk aan $S(X)$?

52. Zij $n > 1$ geheel, en laat $f : S_n \to \mathbf{R}$ een *niet-constante* reëelwaardige functie op S_n zijn die voldoet aan de multiplicatieve eigenschap 2.9.2. Bewijs dat f de tekenafbeelding is.

53. Is het waar dat twee elementen geconjugeerd zijn in de groep A_n als ze hetzelfde cykeltype hebben?

54. Laat zien dat S_n wordt voortgebracht door de verzameling $\{(1\ i) : i = 2, 3, \ldots, n\}$.

55. Laat zien dat A_n wordt voortgebracht door de verzameling $\{(1\ 2\ i) : i = 3, 4, \ldots, n\}$.

56. Laat zien dat S_n voor $n \geq 2$ wordt voortgebracht door $(1\ 2)$ en $(1\ 2\ 3\ \ldots\ n)$.

57. Bepaal de grootte van alle conjugatieklassen in S_n voor $n \leq 6$. *Kun je een deelbaarheidseigenschap formuleren en bewijzen voor groottes van conjugatieklassen in S_n?

58. Zij $p(n)$ het aantal mogelijke cykeltypes van elementen uit S_n. Bereken $p(n)$ voor $n \leq 8$.

*59. Bewijs dat de *partitiefunctie*[7] uit de vorige opgave voldoet aan de machtreeksidentiteit
$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k \geq 1} \frac{1}{1 - x^k}.$$
We nemen hier per definitie $p(0) = 1$. *Voor welke reële waarden van x convergeren deze uitdrukkingen?

60. Zij $g(n)$ de maximale orde van een element in S_n. Bepaal $g(n)$ voor $n \leq 20$. *Hoe zou men $g(n)$ voor grote n kunnen bepalen?[8]

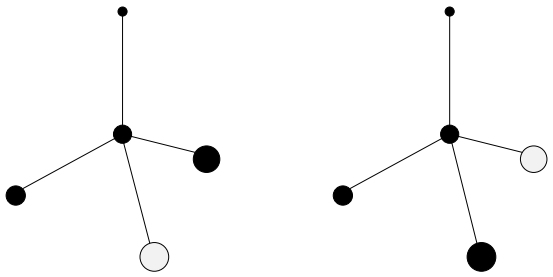
61. Voor $\sigma \in S_n$ definiëren we $d(\sigma)$ als het aantal dekpunten van σ. Bepaal de gemiddelde waarde
$$\delta_n = \frac{1}{n!} \sum_{\sigma \in S_n} d(\sigma)$$
van de functie d op S_n voor $n \leq 5$. *Kun je een algemene formule voor δ_n bewijzen?

62. Voor $\sigma \in S_n$ definiëren we $t(\sigma)$ als het *aantal* cykels in het cykeltype $(k_1, k_2, \ldots, k_t)$ van σ. Bepaal de gemiddelde waarde
$$\tau_n = \frac{1}{n!} \sum_{\sigma \in S_n} 2^{t(\sigma)}$$
van de functie 2^t op S_n voor $n \leq 4$. *Kun je een algemene formule voor τ_n bewijzen?

*63. Laat zien dat het aantal dekpuntvrije permutaties in S_n gelijk is aan $n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}$. Bereken welke fractie van de elementen dit is voor $n \leq 6$, en concludeer dat bij het willekeurig trekken van Sinterklaaslootjes[9] in een niet al te klein gezin de kans dat niemand zichzelf trekt ongeveer gelijk is aan $1/e = 0{,}367879\ldots$.

64. Zij $e_1, e_2, e_3, \ldots, e_n$ een standaardbasis van $\mathbf{R}^n$. Voor $\sigma \in S_n$ definiëren we de lineaire afbeelding $M_\sigma : \mathbf{R}^n \to \mathbf{R}^n$ door $\sum_i a_i e_i \mapsto \sum_i a_i e_{\sigma(i)}$. Bewijs dat het teken $\varepsilon(\sigma)$ van σ gelijk is aan de determinant $\det(M_\sigma)$.
[Men noemt de matrix behorende bij M_σ wel een *permutatiematrix*.]

65. Vat de groep S_4 op als symmetriegroep van de tetraëder $ABCD$ als in §1. Bewijs dat de ondergroep $A_4 \subset S_4$ gelijk is aan de groep van symmetrieën van $ABCD$ voortgebracht door rotaties, oftewel de 'fysiek realiseerbare' symmetrieën. Concludeer dat onderstaande moleculen *enantiomeren*[10] zijn, congruente moleculen die niet door draaiing in elkaar overgevoerd kunnen worden.



*66. Bewijs dat het puzzeltje van Sam Loyd uit de helft van alle mogelijke beginposities oplosbaar is. Hoeveel posities zijn dat? Laat zien dat de overige posities door schuiven in elkaar over te voeren zijn.
[Men zegt wel dat er twee *banen* onder schuiven zijn voor dit puzzeltje.]

*67. Definieer wat we onder een 'positie' verstaan van Rubik's kubus, en bereken het aantal mogelijke posities. Gaan al deze posities door 'legale draaiingen' van de kubus in elkaar over? Kun je een groepsstructuur op de verzameling van posities leggen zo dat de verzameling van 'oplosbare posities' een ondergroep wordt?

3 Symmetrieën van het vlak

Als X een oneindige verzameling is, dan is de permutatiegroep $S(X)$ meestal te groot en te 'structuurloos' om interessant te zijn. Vaak is X echter niet zomaar een oneindige verzameling, maar een verzameling met 'extra structuur'. Men bestudeert dan niet de groep van alle bijecties, maar een ondergroep van bijecties die zich op een bepaalde manier goed gedragen met betrekking tot de structuur van X.

▶ Vlakke meetkunde

In deze paragraaf zullen we voor X het platte vlak nemen. Dit geval speelde een centrale rol in de Griekse wiskunde, en *vlakke meetkunde* was vanaf Euclides (±325–±265 v. Chr.) tot ver in de 20e eeuw het hoofdonderdeel van iedere kennismaking met de wiskunde. Het vlak is het twee-dimensionale geval van wat tegenwoordig een *Euclidische ruimte* genoemd wordt, en veel van wat we in deze paragraaf behandelen kan gegeneraliseerd worden naar de n-dimensionale Euclidische ruimte voor willekeurige $n \geq 1$. Het driedimensionale geval, dat tot *ruimtemeetkunde* of *stereometrie* aanleiding geeft, wordt onder meer toegepast in de *kristallografie*.

Niet alleen in de Euclidische meetkunde, maar ook in de pas in de 19e eeuw ontdekte varianten als de *hyperbolische* en de *elliptische* meetkunde speelt de groepentheorie een fundamentele rol. Men associeert met iedere 'meetkundige ruimte' de *transformatiegroepen* van afbeeldingen van de ruimte naar zichzelf die structurele grootheden als afstand of volume onveranderd laten. Aan deze aanpak van meetkunde, die in 1872 door de Duitser Felix Klein (1849–1925) verwoord werd in zijn inaugurele rede in Erlangen, wordt wel gerefereerd als het *Erlanger Programm*[11]. In het geval van het vlak zijn *hoeken* en *afstanden* belangrijke structurele grootheden, en we zullen dan ook kijken naar groepen die deze grootheden onveranderd ('invariant') laten.

Vanaf de zeventiende eeuw is de meetkunde in toenemende mate beschreven in termen van gekozen *coördinaten*, die ons in staat stellen meetkundige feiten door algebraïsche manipulaties te verifiëren. Voor het platte vlak leidt een dergelijke keuze tot een identificatie met de verzameling $\mathbf{R}^2$ van geordende paren van reële getallen. Men kiest een *assenkruis* van twee loodrecht snijdende lijnen in het vlak, ook wel x_1-as en x_2-as genoemd, en noemt hun snijpunt de *oorsprong* van het vlak. Na keuze van een lengte-eenheid kan men vervolgens ieder punt in het vlak noteren als een geordend paar $x = (x_1, x_2) \in \mathbf{R}^2$. Dergelijke paren kan men coördinaatsgewijs optellen, en de resulterende optelling in het vlak wordt wel de *vectoroptelling* genoemd.

Opgave 1. Ga na dat de vectoroptelling aanleiding geeft tot een groepsstructuur op $\mathbf{R}^2$.

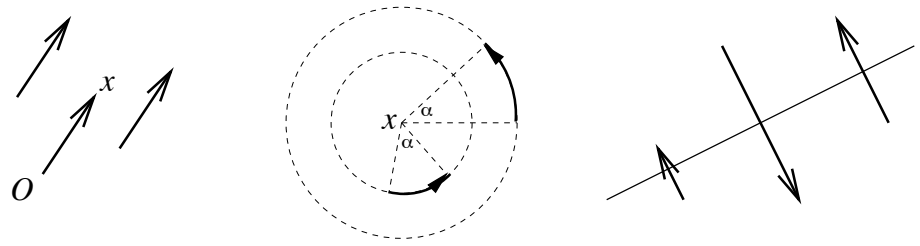
Naast de vectoroptelling hebben we een *scalaire vermenigvuldiging* die ons in staat stelt de punten van $\mathbf{R}^2$ met een reële constante te vermenigvuldigen. Men vat één en ander samen in de lineaire algebra door te zeggen dat $\mathbf{R}^2$ een *vectorruimte* is over $\mathbf{R}$. Ieder punt is een unieke $\mathbf{R}$-lineaire combinatie van de punten $e_1 = (1, 0)$ en $e_2 = (0, 1)$, die samen de *standaardbasis* van $\mathbf{R}^2$ vormen. Men noteert een punt $(x_1, x_2) \in \mathbf{R}^2$ ook wel als de kolomvector $\binom{x_1}{x_2}$.

De lineaire algebra laat zien hoe men klassieke meetkundige begrippen als afstanden tussen punten en hoeken tussen lijnen in $\mathbf{R}^2$ kan uitdrukken in termen van het *inproduct* $\langle \cdot, \cdot \rangle : \mathbf{R}^2 \times \mathbf{R}^2 \to \mathbf{R}$ gegeven door de formule $\langle \binom{x_1}{x_2}, \binom{y_1}{y_2} \rangle = x_1y_1 + x_2y_2$.

Opgave 2. Geven inproductvermenigvuldiging en scalaire vermenigvuldiging groepsoperaties op $\mathbf{R}^2$?

▶ Isometrieën

Bekende voorbeelden van afbeeldingen $\mathbf{R}^2 \to \mathbf{R}^2$ uit de vlakke meetkunde zijn de *translatie* τ_x over de vector $x \in \mathbf{R}^2$, de *rotatie* $\rho_{x,\alpha}$ over een hoek α om een punt x en de *spiegeling* σ_ℓ in een lijn ℓ. Dergelijke afbeeldingen kwamen we in §1 tegen bij de beschouwing van *symmetriegroepen* van vlakke figuren als de ruit en het vierkant.



τ_x $\qquad\qquad$ $\rho_{x,\alpha}$ $\qquad\qquad$ σ_ℓ

De genoemde voorbeelden zijn elk bijecties van het vlak naar zichzelf, met als inversen respectievelijk de translatie τ_{-x}, de rotatie $\rho_{x,-\alpha}$ en de spiegeling σ_ℓ. Omdat ze de oorsprong van het vlak niet noodzakelijk naar zichzelf sturen zijn ze niet in het algemeen lineair. Het zijn voorbeelden van wat men wel als *vlakke symmetrieën*, *congruenties* of *isometrieën* aanduidt. De definitie is geheel in de geest van het Erlanger Programm.

3.1. Definitie. *Een vlakke symmetrie of isometrie is een afbeelding $\varphi : \mathbf{R}^2 \to \mathbf{R}^2$ die afstanden onveranderd laat:*

$$|\varphi(x) - \varphi(y)| = |x - y| \qquad \text{voor alle punten } \; x, y \in \mathbf{R}^2.$$

Geldt $\varphi(O) = O$ voor een isometrie φ, met $O \in \mathbf{R}^2$ de oorsprong, dan heet φ een orthogonale afbeelding.

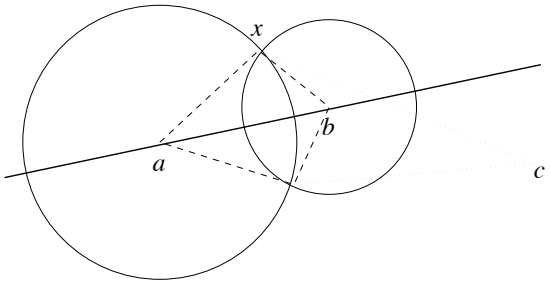
De verzameling van isometrieën van het vlak geven we aan met $I_2(\mathbf{R})$, en we noteren de deelverzameling van orthogonale afbeeldingen met $O_2(\mathbf{R})$. Merk op dat we in 3.1 niet expliciet eisen dat φ een bijectie is. We zullen in 3.4 zien dat dit een *gevolg* van de definitie is, en $I_2(\mathbf{R})$ in feite een ondergroep is van de permutatiegroep $S(\mathbf{R}^2)$.

We bewijzen eerst dat iedere isometrie het product is van een translatie, een rotatie om de oorsprong en eventueel een spiegeling in de x_1-as. Het bewijs, dat sterk doet denken aan de bewijzen van 1.1 en 1.4, berust op een lemma uit de vlakke meetkunde.

We noemen punten in het vlak *collineair* als er een lijn in het vlak is waar al deze punten op liggen. Geldt $\varphi(x) = x$ voor $x \in \mathbf{R}^2$ en $\varphi : \mathbf{R}^2 \to \mathbf{R}^2$, dan zeggen we dat φ het punt x *invariant* laat of dat x een *dekpunt* is van φ.

3.2. Lemma. 1. *Een isometrie die twee verschillende punten invariant laat is de identiteit of de spiegeling in de lijn door deze twee punten.*
2. *Een isometrie die drie niet-collineaire punten invariant laat is de identiteit.*

Bewijs. Stel dat φ twee verschillende punten a en b invariant laat. We laten eerst zien dat φ ieder punt $x \in \mathbf{R}^2$ vasthoudt of spiegelt in de lijn ℓ door a en b. Omdat φ een isometrie is moeten de afstanden van $\varphi(x)$ tot a en b respectievelijk gelijk zijn aan $|x-a|$ en $|x-b|$. Zoals onderstaand plaatje laat zien zijn x zelf en zijn spiegelbeeld $\sigma_\ell(x)$ in ℓ de enige punten die hieraan voldoen. In het bijzonder laat φ alle punten op ℓ invariant.



Stel eerst dat φ een punt c buiten de lijn ℓ invariant laat. Is nu x een punt buiten ℓ, dan hebben x en $\sigma_\ell(x)$ verschillende afstand tot c, en we vinden $\varphi(x) = x$. In dit geval is φ de identiteit, en we krijgen de tweede uitspraak van het lemma. Stel ten slotte dat φ geen enkel punt buiten ℓ invariant laat. Dan geldt $\varphi(x) = \sigma_\ell(x)$ voor alle punten x buiten ℓ, en we vinden $\varphi = \sigma_\ell$. □

3.3. Propositie. 1. *Iedere isometrie is op een unieke manier te schrijven als een product $\tau\psi$ van een translatie τ en een orthogonale afbeelding ψ.*
2. *Een orthogonale afbeelding is óf een rotatie om de oorsprong, óf het product van een rotatie om de oorsprong met een spiegeling in de x_1-as.*

Bewijs. We beginnen met de laatste uitspraak. Zij ψ een orthogonale afbeelding, en a een punt op de x_1-as verschillend van de oorsprong O. Dan is $\psi(a)$ een punt op de cirkel rond de oorsprong met straal $|a|$, dus er bestaat een rotatie ρ om O met $\rho(a) = \psi(a)$. De isometrie $\rho^{-1}\psi$ laat nu O en a invariant, dus wegens 3.2.1 is $\rho^{-1}\psi$ gelijk aan de identiteit of de spiegeling σ in de x_1-as. In het eerste geval is $\psi = \rho$ een rotatie om de oorsprong, in het tweede geval vinden we uit $\rho^{-1}\psi = \sigma$ de identiteit $\psi = \rho\sigma$, zodat ψ het product is van een spiegeling in de x_1-as met een rotatie om de oorsprong. In het bijzonder zien we hieruit dat orthogonale afbeeldingen bijecties zijn.

Zij nu φ een willekeurige isometrie, en $\tau = \tau_{\varphi(O)}$ de translatie over $\varphi(O)$. Dan laat $\psi = \tau^{-1}\varphi$ de oorsprong invariant, dus ψ is een orthogonale afbeelding en $\varphi = \tau\psi$ is een product van de verlangde soort.

Stel nu dat er translaties τ_1, τ_2 en orthogonale afbeeldingen ψ_1, ψ_2 bestaan met $\tau_1\psi_1 = \tau_2\psi_2$. Omdat translaties en orthogonale afbeeldingen bijectief zijn hebben ze een inverse, en door de vorige identiteit achtereenvolgens van links met τ_2^{-1} en van rechts met ψ_1^{-1} te vermenigvuldigen krijgen we $\tau_2^{-1}\tau_1 = \psi_2\psi_1^{-1}$. Links staat een translatie, rechts een orthogonale afbeelding. Omdat de identiteit de enige translatie is die

orthogonaal is vinden we $\tau_2^{-1}\tau_1 = \mathrm{id} = \psi_2\psi_1^{-1}$, en dus $\tau_1 = \tau_2$ en $\psi_1 = \psi_2$. De boven gevonden productrepresentatie $\varphi = \tau\psi$ is dus uniek. □

Opgave 3. Laat zien dat iedere isometrie uniek te schrijven is als een product $\varphi = \psi\tau$ met ψ orthogonaal en τ een translatie. Geeft dit dezelfde τ en ψ als in 3.3.1?

De productrepresentatie $\varphi = \tau\psi$ zullen we in het vervolg op diverse manieren gebruiken.

3.4. Gevolg. *De verzameling $I_2(\mathbf{R})$ van vlakke symmetrieën vormt een groep onder samenstelling, en $O_2(\mathbf{R})$ is de ondergroep van lineaire afbeeldingen in $I_2(\mathbf{R})$.*

Bewijs. Uit 3.3 volgt dat iedere vlakke symmetrie een samenstelling van bijecties $\mathbf{R}^2 \to \mathbf{R}^2$ is, en dus zelf een bijectie. Onder de inclusie $I_2(\mathbf{R}) \subset S(\mathbf{R}^2)$ wordt $I_2(\mathbf{R})$ een ondergroep van $S(\mathbf{R}^2)$ in de zin van 2.7: de identiteit is een isometrie, het samenstellen van twee isometrieën geeft weer een isometrie, en als een bijectie afstanden bewaart, dan doet zijn inverse dat ook. Op soortgelijke manier ziet men in dat de deelverzameling $O_2(\mathbf{R}) \subset I_2(\mathbf{R})$ van isometrieën die de oorsprong vasthouden een ondergroep is van $I_2(\mathbf{R})$. Wegens 3.3.2 is iedere orthogonale afbeelding een product van lineaire afbeeldingen, en dus weer lineair. Omgekeerd laat een lineaire afbeelding in $I_2(\mathbf{R})$ de oorsprong invariant, en daarmee is hij orthogonaal. □

3.5. Gevolg. *Voor een isometrie φ en punten $x_1, x_2, \ldots, x_n \in \mathbf{R}^2$ geldt*

$$\varphi\left(\frac{x_1 + x_2 + \ldots + x_n}{n}\right) = \frac{\varphi(x_1) + \varphi(x_2) + \ldots + \varphi(x_n)}{n}.$$

Bewijs. Het is intuïtief weliswaar duidelijk dat isometrieën 'gemiddeldes bewaren' in de zin van dit gevolg, maar dit is niet een onmiddellijk gevolg van definitie 3.1. We kunnen echter opmerken dat de te bewijzen identiteit correct is voor een lineaire afbeelding, en eveneens voor een translatie. Passen we deze speciale gevallen achter elkaar toe, dan zien we dat de identiteit geldt voor iedere samenstelling $\varphi = \tau\psi$ in 3.3.1. □

▶ De orthogonale groep

De *orthogonale groep* $O_2(\mathbf{R})$ van lineaire vlakke isometrieën bestaat uit 2 soorten elementen. De rotaties om O in $O_2(\mathbf{R})$ hebben in matrixvorm de gedaante

$$\rho_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix},$$

waarbij α de hoek is waarover geroteerd wordt. De overige elementen in $O_2(\mathbf{R})$ krijgt men hieruit door vermenigvuldiging met de spiegeling $\sigma = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Dit geeft de matrices van de vorm

$$\rho_\alpha\sigma = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}.$$

De afbeelding $\rho_\alpha\sigma$ voert de lijn ℓ die een hoek $\alpha/2$ maakt met de positieve x_1-as in zichzelf over, en is de spiegeling in ℓ.

Opgave 4. Ga dit na aan de hand van een plaatje.

Voor iedere rotatie $\rho \in O_2(\mathbf{R})$ is de spiegeling $\rho\sigma$ van orde 2, en dus gelijk aan zijn eigen inverse: $(\rho\sigma)^{-1} = \rho\sigma$. Omdat ook $(\rho\sigma)^{-1} = \sigma^{-1}\rho^{-1} = \sigma\rho^{-1}$ geldt vinden we

$$\rho\sigma = \sigma\rho^{-1}, \tag{3.6}$$

een uiterst nuttige rekenregel die we in §1 (voor opgave 5) al in Latijnse letters tegenkwamen. Hij laat zien dat de spiegeling σ niet met alle rotaties commuteert. De relatie $\rho_\alpha\sigma = \sigma\rho_{-\alpha}$ in (3.6) is samen met de 'commutatieve relatie' $\rho_\alpha\rho_\beta = \rho_\beta\rho_\alpha$ voldoende om te rekenen in $O_2(\mathbf{R})$ zonder ooit matrices te gebruiken.

Opgave 5. Leid (3.6) af met behulp van een plaatje of een expliciete matrixvermenigvuldiging. Geldt dezelfde identiteit als we σ door een willekeurige spiegeling in $O_2(\mathbf{R})$ vervangen?

Net als in het geval van de permutatiegroep S_n heeft men voor de orthogonale groep $O_2(\mathbf{R})$ een *tekenafbeelding* $O_2(\mathbf{R}) \to \{\pm 1\}$ die iedere afbeelding naar de *determinant* van de bijbehorende matrix stuurt. De orthogonale afbeeldingen van determinant 1 zijn de rotaties, die van determinant -1 de spiegelingen. Ze heten respectievelijk *oriëntatie-behoudende* en *oriëntatie-omkerende* afbeeldingen.

Opgave 6. Probeer uit te leggen waarom dit zo heet. Wat is het verband met opgave 2.64?[12]

Net als in het geval van de alternerende groep $A_n \subset S_n$ volgt uit de multiplicativiteit van de determinant dat de oriëntatie-behoudende orthogonale afbeeldingen een ondergroep $O_2^+(\mathbf{R}) \subset O_2(\mathbf{R})$ vormen. Deze ondergroep bestaat uit de rotaties om O.

▶ Vlakke symmetriegroepen

De orthogonale groep, die impliciet al in opgave 1.21 voorkomt, is de *symmetriegroep* van de eenheidscirkel in het vlak. Definiëren we een *vlakke figuur* heel algemeen als een deelverzameling $F \subset \mathbf{R}^2$, dan is er de volgende definitie van de symmetriegroep van F.

3.7. Definitie. *Zij $F \subset \mathbf{R}^2$ een vlakke figuur. Dan heet de ondergroep*

$$\mathrm{Sym}(F) = \{\varphi \in I_2(\mathbf{R}) : \varphi[F] = F\}$$

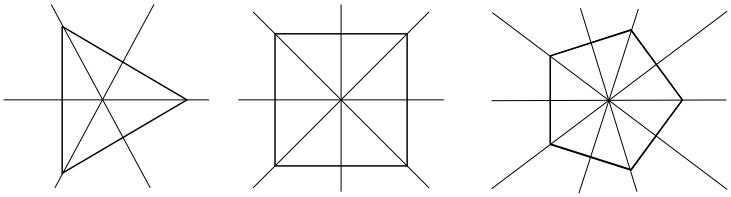
de symmetriegroep van de figuur F.

Merk op dat de verzameling $\mathrm{Sym}(F)$ in 3.7 inderdaad een ondergroep is van $I_2(\mathbf{R})$, en dus zelf weer een groep. De speciale gevallen waarin F een ruit of een vierkant is met de oorsprong als middelpunt kwamen we tegen in §1. Voor $F = \{O\}$ is $\mathrm{Sym}(F)$ de orthogonale groep $O_2(\mathbf{R})$.

Opgave 7. Krijgen we in 3.7 een groep als we geen gelijkheid maar alleen een inclusie $\varphi[F] \subset F$ eisen?

In §1 bestudeerden we de symmetriegroep D_4 van het vierkant. Algemener hebben we voor willekeurige $n \geq 2$ de symmetriegroep D_n van de regelmatige n-hoek. Omdat iedere symmetrie van een regelmatige n-hoek het middelpunt wegens 3.5 als dekpunt heeft krijgen we een inclusie $D_n \subset O_2(\mathbf{R})$ door O als middelpunt te nemen. De rotaties in D_n zijn nu de n rotaties om O over hoeken $2k\pi/n$, met k geheel. Zij vormen een

cyclische ondergroep $C_n \subset O_2(\mathbf{R})$ van orde n die wordt voortgebracht door de rotatie $\rho = \rho_{2\pi/n}$ over een hoek $2\pi/n$. Als in 1.4 krijgen we D_n uit C_n door de samenstellingen met een spiegeling in de lijn door O en een hoekpunt toe te voegen. Dit geeft de n spiegelingen in de lijnen door O en een hoekpunt en in de lijnen door O en het midden van een zijde. We noemen D_n wel de *dihedrale groep* of *diëdergroep* van orde $2n$.



Kiezen we een hoekpunt op de x_1-as en σ de spiegeling in de x_1-as, dan vinden we

$$\begin{aligned} D_n = \langle \rho, \sigma \rangle &= C_n \cup \sigma C_n = \\ &= \{\rho^k : \ k = 0, 1, 2, \ldots, n-1\} \cup \{\sigma\rho^k : \ k = 0, 1, 2, \ldots, n-1\}. \end{aligned}$$

Met behulp van relatie (3.6) kunnen we rekenen in D_n in termen van ρ en σ.

Voor $n = 1$ is D_n per definitie gelijk aan de groep $D_1 = \langle \sigma \rangle$ van orde 2 voortgebracht door σ. Zijn ondergroep van rotaties is de triviale groep C_1.

Opgave 8. Laat zien dat D_1 en D_2 de enige abelse diëdergroepen zijn.

De groepen C_n en D_n zijn de enige voorbeelden van eindige symmetriegroepen.

3.8. Stelling. *Iedere eindige ondergroep van $I_2(\mathbf{R})$ is voor een geschikte keuze van de coördinaten gelijk aan C_n of D_n.*

Bewijs. Zij $G \subset I_2(\mathbf{R})$ eindig. We laten eerst zien dat er een punt in het vlak is dat door alle $\varphi \in G$ invariant wordt gelaten. Neem hiertoe een willekeurig punt $x \in \mathbf{R}^2$, en kijk naar de *baan* van x onder G, d.w.z. de verzameling van beelden van x onder de symmetrieën in G. Omdat G eindig is, is deze baan ook eindig, zeg gelijk aan $\{x_1, x_2, \ldots, x_n\}$. De baan van x wordt door de elementen van G op zichzelf afgebeeld, en wegens de bijectiviteit van symmetrieën zijn deze afbeeldingen permutaties. Het 'gemiddelde' van de punten in de baan van x is nu wegens 3.5 een dekpunt:

$$\varphi\left(\frac{x_1 + x_2 + \ldots + x_n}{n}\right) = \frac{\varphi(x_1) + \varphi(x_2) + \ldots + \varphi(x_n)}{n} = \frac{x_1 + x_2 + \ldots + x_n}{n}.$$

Nemen we dit punt als de oorsprong, dan wordt G een eindige ondergroep van de orthogonale groep $O_2(\mathbf{R})$.

We bepalen eerst de ondergroep $G^+ = G \cap O_2^+(\mathbf{R})$ van rotaties in G. Omdat G^+ eindig is, is er een *minimale* waarde $\alpha \in (0, 2\pi]$ waarvoor $\rho = \rho_\alpha$ bevat is in G. Zij n het kleinste positieve getal waarvoor $n\alpha \geq 2\pi$ geldt. Dan is $\rho^n \in G^+$ een rotatie over $n\alpha \in [2\pi, 2\pi + \alpha)$, en wegens de minimaliteit van α geldt $n\alpha = 2\pi$, dus $\rho_\alpha = \rho_{2\pi/n}$. Iedere andere rotatie in G^+ is na vermenigvuldiging met een geschikte macht van $\rho_{2\pi/n}$ van de vorm ρ_β met $0 \leq \beta < 2\pi/n$, en uit de minimaliteit van $\alpha = 2\pi/n$ volgt dan

$\beta = 0$ en $\rho_\beta = \mathrm{id}$. We concluderen dat G^+ uit de machten van $\rho_{2\pi/n}$ bestaat en dus gelijk is aan C_n.

Bevat G tevens een spiegeling, dan krijgen we door de spiegelas daarvan als x_1-as te nemen $\sigma \in G$. Voor iedere andere spiegeling $\tilde{\sigma} \in G$ is nu $\sigma\tilde{\sigma} = \rho$ een rotatie in G, dus de spiegelingen in G zijn de elementen $\sigma\rho$, met ρ in de ondergroep G^+ van rotaties in G. We vonden al dat G^+ gelijk is aan $C_n = \langle \rho_{2\pi/n} \rangle$ voor zekere n, dus in dit geval krijgen we $G = D_n$. □

De techniek die we in het voorafgaande bewijs gebruikten om de groep G^+ van rotaties cyclisch te praten komt in vele varianten voor. Een variant voor gehele getallen vind je in 6.2.

Opgave 9. Laat zien dat de verzameling $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$ van complexe getallen een groep vormt onder vermenigvuldiging, en dat iedere *eindige* ondergroep $H \subset \mathbf{C}^*$ cyclisch is.

Er is een analogon van 3.8 voor ruimtelijke symmetrieën. Enigszins verrassend blijken er in drie dimensies niet heel veel meer mogelijkheden te zijn dan in twee.[13]

▶ Teken van een isometrie

We kunnen aan een willekeurige isometrie een teken toekennen door de decompositie $\varphi = \tau\psi$ uit 3.3.1 te gebruiken. Laten we aan de orthogonale afbeelding ψ in zo'n decompositie refereren als de *lineaire component* $\psi = L(\varphi)$ van de isometrie φ.

3.9. Propositie. *De afbeelding $L : I_2(\mathbf{R}) \to O_2(\mathbf{R})$ die aan een isometrie zijn lineaire component toevoegt is multiplicatief, d.w.z. er geldt*

$$L(\varphi_1\varphi_2) = L(\varphi_1)L(\varphi_2) \qquad \text{voor } \varphi_1, \varphi_2 \in I_2(\mathbf{R}).$$

Bewijs. Schrijf $\varphi_1 = \tau_1\psi_1$ en $\varphi_2 = \tau_2\psi_2$ voor de decomposities van φ_1 en φ_2. Omdat translaties en orthogonale afbeeldingen niet in het algemeen commuteren moeten we enig werk doen om de decompositie van $\varphi_1\varphi_2 = \tau_1\psi_1\tau_2\psi_2$ te vinden.

Is τ_a de translatie over a en ψ een willekeurige lineaire afbeelding, dan geldt

$$(\psi\tau_a)(x) = \psi(x + a) = \psi(x) + \psi(a) = (\tau_{\psi(a)}\psi)(x)$$

voor ieder punt $x \in \mathbf{R}^2$. De gevonden relatie

$$\psi\tau_a = \tau_{\psi(a)}\psi \tag{3.10}$$

laat zien dat we $\psi_1\tau_2 = \tau_2'\psi_1$ hebben voor één of andere translatie τ_2', en dat de gezochte decompositie gegeven wordt door $\varphi_1\varphi_2 = (\tau_1\tau_2')(\psi_1\psi_2)$. In het bijzonder hebben we $L(\varphi_1\varphi_2) = \psi_1\psi_2 = L(\varphi_1)L(\varphi_2)$. □

We definiëren de *tekenafbeelding* $I_2(\mathbf{R}) \to \{\pm 1\}$ door $\varphi \longmapsto \det L(\varphi)$. Uit 3.9 volgt dat deze afbeelding als samenstelling van twee multiplicatieve afbeeldingen zelf ook weer multiplicatief is:

$$\det L(\phi_1\phi_2) = \det(L(\phi_1)L(\phi_2)) = \det L(\phi_1) \cdot \det L(\phi_2).$$

Net als voor de orthogonale groep vinden we dat $I_2(\mathbf{R})$ een ondergroep $I_2^+(\mathbf{R})$ van oriëntatie-bewarende isometrieën bevat, bestaande uit isometrieën met teken 1.

▶ Meetkunde met complexe getallen

Een op het oog enigszins verschillende, maar in feite met 3.3 equivalente beschrijving van de groep $I_2(\mathbf{R})$ kan men geven in termen van complexe getallen door het vlak $\mathbf{R}^2$ op de bekende wijze te identificeren met de complexe getallen $\mathbf{C}$. De elementen van de standaardbasis worden dan 1 en i, en de isometrieën krijgen de volgende gedaante.

3.11. Stelling. *De oriëntatie-bewarende isometrieën van het complexe vlak* $\mathbf{C}$ *zijn de afbeeldingen*

$$\varphi^+_{a,b} : z \longmapsto az + b \qquad \textit{met } a, b \in \mathbf{C} \textit{ en } |a| = 1$$

en de oriëntatie-omkerende isometrieën de afbeeldingen

$$\varphi^-_{a,b} : z \longmapsto a\overline{z} + b \qquad \textit{met } a, b \in \mathbf{C} \textit{ en } |a| = 1.$$

Hier geeft $\overline{z}$ *de complex geconjugeerde van* $z \in \mathbf{C}$ *aan.*

Bewijs. Onder de identificatie van $\mathbf{R}^2$ met $\mathbf{C}$ correspondeert de spiegeling in de x_1-as met complexe conjugatie, de rotatie om O over een hoek α met de vermenigvuldiging met het complexe getal $a = e^{i\alpha}$ van absolute waarde 1 en de translatie over een punt b met de optelling $z \mapsto z + b$. Schrijven we nu de decomposities in 3.3 in termen van complexe getallen, dan krijgen we precies de in de stelling genoemde afbeeldingen. De afbeeldingen $z \mapsto az + b$ hebben als samenstelling van een rotatie en een translatie teken 1. Voorafgegaan door de spiegeling $z \mapsto \overline{z}$ van teken -1 krijgen we een afbeelding $z \mapsto a\overline{z} + b$, die kennelijk teken -1 heeft. □

De identificatie van $\mathbf{R}^2$ met $\mathbf{C}$, die anders dan de meeste andere argumenten in deze paragraaf geen direct analogon in hogere dimensie heeft, kan soms efficiënt gebruikt worden in de vlakke meetkunde. We bewijzen als toepassing dat het 'type' van een isometrie op onderstaande manier bepaald wordt door zijn teken en het al of niet hebben van een dekpunt.

	met dekpunt	zonder dekpunt
det = +1	rotatie	(echte) translatie
det = −1	spiegeling	(echte) glijspiegeling

In de kolom 'zonder dekpunt' wordt met '(echte) translatie' een translatie over een vector verschillend van nul bedoeld. Evenzo is een (echte) *glijspiegeling* een spiegeling, gevolgd door een (echte) translatie evenwijdig aan de spiegelas.

Isometrieën met een dekpunt zijn orthogonaal als we het dekpunt als oorsprong nemen. We zagen al dat dit rotaties en spiegelingen zijn, en dat we ze kunnen onderscheiden door hun teken. Dit geeft de eerste kolom van de tabel.

Een isometrie van teken +1 zonder dekpunt correspondeert met een afbeelding $\phi^+_{a,b} : z \mapsto az + b$ in 3.11 waarvoor de vergelijking $z = az + b$ geen oplossing heeft. Voor

$a \neq 1$ is er de oplossing $z = b/(1-a) \in \mathbf{C}$, dus we hebben $a = 1$ en $\phi^+_{a,b} : z \mapsto z + b$ is een translatie. Voor $b \neq 0$ heeft die geen dekpunt.

Om te kijken wanneer de afbeelding $\varphi^-_{a,b} : z \mapsto a\overline{z} + b$ van teken -1 in 3.11 een dekpunt heeft schrijven we $a = w^2$ en merken op dat $\varphi^-_{a,b}$ een spiegeling in de lijn $w\mathbf{R}$ is, gevolgd door een translatie over b. Wegens $|a| = |w| = 1$ hebben we $\overline{w} = w^{-1}$ en kunnen we de vergelijking $z = a\overline{z} + b$ herschrijven als

$$2i \cdot \mathrm{Im}(z/w) = \overline{w}z - w\overline{z} = b/w.$$

Deze vergelijking heeft een oplossing dan en slechts dan als b/w zuiver imaginair is, hetgeen betekent dat b loodrecht op de spiegellijn $w\mathbf{R}$ staat. Voor zulke b is $\varphi^-_{a,b}$ de spiegeling in de lijn $b/2 + w\mathbf{R}$. Algemener kunnen we $b = b_1 + b_2$ schrijven met b_1 loodrecht op $w\mathbf{R}$ en $b_2 \in w\mathbf{R}$. Als er geen dekpunt is hebben we $b_2 \neq 0$, en dan is $\varphi^-_{a,b}$ een spiegeling in de lijn $b_1/2 + w\mathbf{R}$ gevolgd door een translatie evenwijdig aan die lijn. Dit bewijst dat onze tabel correct is. □

Opgave 10. Ga het laatste argument na aan de hand van een plaatje.

▶ Vlakke transformatiegroepen

Ter afsluiting van deze paragraaf merken we op dat er nog andere groepen dan $I_2(\mathbf{R})$ zijn die men met het platte vlak kan associëren. In de lineaire algebra kijkt men vaak naar de verzameling $\mathrm{GL}_2(\mathbf{R})$ van bijecties van het vlak die *lineair* zijn. Deze verzameling is een groep die men kan identificeren met de groep van *inverteerbare* 2×2-matrices met reële coëfficiënten. De notatie 'GL' is een afkorting van het Engelse 'general linear'. Wegens 3.4 hebben we

$$\mathrm{GL}_2(\mathbf{R}) \cap I_2(\mathbf{R}) = O_2(\mathbf{R}).$$

Eist men niet zoals in 3.1 dat alle afstanden behouden blijven, maar alleen de *verhoudingen* tussen afstanden, dan krijgt men de groep $\mathrm{Sim}_2(\mathbf{R})$ van vlakke *gelijkvormigheidstransformaties*. De afkorting komt hier van het Engelse 'similarity'. De gelijkvormigheidstransformaties zijn de afbeeldingen die rechte lijnen in rechte lijnen overvoeren en bovendien de hoeken daartussen bewaren.

Laat men ten slotte niet alleen samenstellingen van translaties en orthogonale afbeeldingen toe als in 3.3.1, maar samenstellingen van translaties met willekeurige elementen van $\mathrm{GL}_2(\mathbf{R})$, dan onstaat (opgave 31) de groep $\mathrm{Aff}_2(\mathbf{R})$ van vlakke *affiene* afbeeldingen. Dit zijn de afbeeldingen die rechte lijnen in rechte lijnen overvoeren. We zien (opgave 31) dat er natuurlijke inclusies

$$I_2(\mathbf{R}) \subset \mathrm{Sim}_2(\mathbf{R}) \subset \mathrm{Aff}_2(\mathbf{R})$$

zijn, en dat ieder van deze groepen bestaat uit bijecties van het vlak die in de geest van het Erlanger Programm 'iets invariant laten'. Voor verdere details verwijzen we naar de opgaven.

Opgaven.

11. Laat zien dat de verzameling $\mathrm{GL}_2(\mathbf{R})$ van inverteerbare lineaire afbeeldingen $\mathbf{R}^2 \to \mathbf{R}^2$ een groep vormt, en dat deze uit de 2×2-matrices van determinant ongelijk 0 bestaat. Is $O_2(\mathbf{R})$ een ondergroep van $\mathrm{GL}_2(\mathbf{R})$?

12. Vormt de verzameling $\mathrm{Mat}_2(\mathbf{R})$ van *alle* reële 2×2-matrices een groep onder vermenigvuldiging? Is er een natuurlijke *optelling* op $\mathrm{Mat}_2(\mathbf{R})$ die een groepsstructuur geeft?

13. Zij $\varphi : \mathbf{R}^2 \to \mathbf{R}^2$ een lineaire afbeelding. Bewijs dat equivalent zijn:
    1. φ is een isometrie;
    2. voor alle $x \in \mathbf{R}^2$ geldt $|\varphi(x)| = |x|$;
    3. voor alle $x, y \in \mathbf{R}^2$ voldoet het inproduct aan $\langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$.

14. Laat zien dat een isometrie hoeken tussen lijnen invariant laat.

15. Bewijs: een element in $I_2(\mathbf{R})$ dat geconjugeerd is met een translatie is zelf een translatie.

16. Schrijf de elementen van de groep $D_6 \subset O_2(\mathbf{R})$ expliciet in matrixvorm.

17. Laat zien dat D_2 'dezelfde' groep is als de *viergroep van Klein* uit §1.

18. Bepaal de symmetriegroepen van elk van de letters in een eenvoudig blokletteralfabet. Welke groep komt het meeste voor? Kun je voor elk van de gevonden symmetriegroepen ook een *woord* maken dat (als woord!) deze symmetriegroep heeft?

19. Zij F een 'woord in het vlak' in de zin van de vorige opgave, en neem aan dat $\mathrm{Sym}(F)$ de triviale groep is. Zij G een willekeurige eindige symmetriegroep. Bewijs dat F uit te breiden is tot een figuur $\overline{F}$ met $\mathrm{Sym}(\overline{F}) = G$.

20. Laat zien dat iedere symmetrie van een vlakke figuur F een bijectie $F \to F$ geeft, en zij $f : \mathrm{Sym}(F) \to S(F)$ de bijbehorende afbeelding. Bewijs dat f injectief is dan en slechts dan als F niet bevat is in een lijn in $\mathbf{R}^2$. Concludeer dat we voor dergelijke 'echte' vlakke figuren $\mathrm{Sym}(F)$ op kunnen vatten als ondergroep van $S(F)$.

21. Zij F een vlakke figuur met symmetriegroep S en α een isometrie. Bewijs dat de symmetriegroep van de figuur $\alpha F = \{\alpha(x) : x \in F\}$ gelijk is aan de met S geconjugeerde ondergroep $\alpha S \alpha^{-1} = \{\alpha\sigma\alpha^{-1} : \sigma \in S\}$.

22. Bewijs dat de 'structuur' van de symmetriegroep van een figuur niet van de keuze van coördinaten afhangt. [Formuleer eerst *precies* wat dit moet betekenen.]

23. Laat met behulp van een plaatje zien dat de samenstelling van een rotatie om O over een hoek $\alpha \neq 0$ en een translatie weer een rotatie over α geeft, en bepaal het nieuwe rotatiecentrum.

24. Bewijs de volgende stellingen uit de vlakke meetkunde. Er is steeds een 'direct meetkundig' bewijs en een heel kort bewijs met behulp van 3.11.
    1. De samenstelling van de spiegelingen in twee evenwijdige lijnen is een translatie.
    2. Het kwadraat van een glijspiegeling is een translatie.
    3. De samenstelling van de spiegelingen in twee snijdende lijnen is een rotatie.
    4. De samenstelling van twee rotaties over hoeken α en $-\alpha$ is een translatie.
    5. De samenstelling van twee rotaties over hoeken α en $\beta \neq -\alpha$ is een rotatie over $\alpha + \beta$.

25. Bepaal in de vorige opgave de translatievectoren (in 1, 2 en 4), de rotatiehoek (in 3) en het rotatiecentrum (in 5).

*26. Zij $F \subset \mathbf{R}^2$ een niet-lege deelverzameling van $\mathbf{R}^2$ die *begrensd* is. Bewijs dat $\mathrm{Sym}(F)$ voor een geschikte keuze van coördinaten een ondergroep is van $O_2(\mathbf{R})$.

27. Zij $G \subset I_2(\mathbf{R})$ een groep van vlakke symmetrieën. Laat zien dat de *translatieondergroep* $G_T = \{\phi \in G : L(\phi) = \mathrm{id}\}$ van G een ondergroep van G is, en dat hij uit de translaties in G bestaat. Laat eveneens zien dat de *puntgroep* $\overline{G} = \{L(\phi) : \phi \in G\}$ van G een ondergroep is van $O_2(\mathbf{R})$.

*28. Een groep $G \subset I_2(\mathbf{R})$ van vlakke symmetrieën heet een *vlakke kristallografische groep* als zijn translatieondergroep voortgebracht wordt door twee onafhankelijke translaties, d.w.z. translaties τ_x en τ_y waarvoor x en y een basis voor $\mathbf{R}^2$ vormen. Bewijs dat de puntgroep van een vlakke kristallografische groep gelijk is aan C_n of D_n met $n \in \{1, 2, 3, 4, 6\}$.

29. Een *gelijkvormigheid* is een niet-constante afbeelding $\phi : \mathbf{R}^2 \to \mathbf{R}^2$ die verhoudingen van afstanden invariant laat: voor alle viertallen punten $a, b, c, d \in \mathbf{R}^2$ met $a \neq b$ en $c \neq d$ geldt

$$\frac{|\phi(a) - \phi(b)|}{|a - b|} = \frac{|\phi(c) - \phi(d)|}{|c - d|}.$$

Bewijs dat een gelijkvormigheid alle afstanden met dezelfde positieve factor vermenigvuldigt, en dat de verzameling $\mathrm{Sim}_2(\mathbf{R})$ van gelijkvormigheden een ondergroep van $S(\mathbf{R}^2)$ is die $I_2(\mathbf{R})$ bevat.

30. Laat zien dat het analogon van 3.11 voor gelijkvormigheden verkregen wordt door de voorwaarde $|a| = 1$ te vervangen door $a \neq 0$.

31. Een *vlakke affiene afbeelding* is een afbeelding $\mathbf{R}^2 \to \mathbf{R}^2$ die verkregen kan worden door een inverteerbare lineaire afbeelding met een translatie samen te stellen. Bewijs dat de verzameling $\mathrm{Aff}_2(\mathbf{R})$ van affiene afbeeldingen een ondergroep van $S(\mathbf{R}^2)$ is die $\mathrm{Sim}_2(\mathbf{R})$ bevat.

32. Laat zien dat de determinantafbeelding op $\mathrm{GL}_2(\mathbf{R})$ een natuurlijke uitbreiding heeft tot een multiplicatieve functie op $\mathrm{Aff}_2(\mathbf{R})$.

33. Definieer de groepen $I_1(\mathbf{R})$, $\mathrm{Sim}_1(\mathbf{R})$ en $\mathrm{Aff}_1(\mathbf{R})$ van *lineaire* isometrieën, gelijkvormigheden en affiene afbeeldingen $\mathbf{R} \to \mathbf{R}$; bewijs vervolgens de analoga van 3.3, 3.4, 3.9 en 3.11, en concludeer dat de affiene groep $\mathrm{Aff}_1(\mathbf{R})$ over $\mathbf{R}$ samenvalt met $\mathrm{Sim}_1(\mathbf{R})$ en bestaat uit de lineaire afbeeldingen $x \mapsto ax + b$ met $a, b \in \mathbf{R}$, $a \neq 0$.

34. Definieer een vermenigvuldiging op de productverzameling $\mathbf{C} \times \mathbf{C}^*$ door

$$(b_1, a_1) \cdot (b_2, a_2) = (b_1 + a_1 b_2, a_1 a_2).$$

Bewijs dat $\mathbf{C} \times \mathbf{C}^*$ onder deze vermenigvuldiging een groep wordt, de *affiene groep* over $\mathbf{C}$. Is deze groep abels?

4 Homomorfismen

Het is een algemene constatering in de wiskunde dat voor iedere interessante categorie van objecten er een 'bijbehorend' soort *afbeeldingen* tussen die objecten bestaat. Deze afbeeldingen, die in den regel op één of andere manier de structuur van de objecten in kwestie respecteren, heten de *homomorfismen* of kortweg *morfismen* in de categorie[14]. Zo zijn bijvoorbeeld de morfismen in de lineaire algebra de *lineaire* afbeeldingen, en die in de topologie de *continue* afbeeldingen.

▶ Homomorfismen, isomorfismen, automorfismen

Voor groepen, waar de structuur op de onderliggende verzameling gegeven wordt door een groepsbewerking, ligt het voor de hand te kijken naar de afbeeldingen die de bewerking respecteren.

4.1. Definitie. *Een homomorfisme van een groep G naar een groep G' is een afbeelding $f : G \to G'$ met de eigenschap dat voor ieder tweetal elementen $x, y \in G$ de identiteit*

$$f(xy) = f(x)f(y)$$

geldt. Een bijectief homomorfisme heet een isomorfisme.

De verzameling $\mathrm{Hom}(G, G')$ van homomorfismen van G naar G' bevat altijd het *triviale homomorfisme*, dat alle elementen van G naar het eenheidselement $e' \in G'$ stuurt. Soms is dit het enige homomorfisme van G naar G'.

Als $f : G \to G'$ een isomorfisme is, schrijft men $f : G \xrightarrow{\sim} G'$ en noemt men de groepen G en G' *isomorf*. Notatie: $G \cong G'$. In dit geval hebben G en G' 'dezelfde groepsstructuur'.

We zijn reeds diverse voorbeelden van isomorfismen tegengekomen. In §1 zagen we dat de symmetriegroep V_4 van de ruit isomorf is met de vermenigvuldigingsgroep $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ van oneven resten modulo 8. In dit geval is iedere bijectie die de identiteit $\mathrm{id} \in V_4$ naar $\overline{1}$ stuurt een isomorfisme.

De ondergroep $D_1 = \langle\sigma\rangle \subset O_2(\mathbf{R})$ van orde 2 voortgebracht door de spiegeling σ in de x_1-as is isomorf met de *tekengroep* $\{\pm 1\}$. De determinantafbeelding geeft hier een isomorfisme $\det : D_1 \xrightarrow{\sim} \{\pm 1\}$. De ondergroep $C_2 \subset O_2(\mathbf{R})$ voortgebracht door de halve slag is óók isomorf met $\{\pm 1\}$. De determinantafbeelding $\det : C_2 \to \{\pm 1\}$ is echter het triviale homomorfisme, en dus geen isomorfisme.

Opgave 1. Bewijs dat alle groepen van orde 2 isomorf zijn. Zijn alle groepen van orde 3 ook isomorf?

Voorbeelden van homomorfismen uit de voorafgaande paragrafen zijn de tekenafbeelding $\varepsilon : S_n \to \{\pm 1\}$ in 2.9, de lineaire-component-afbeelding $L : I_2(\mathbf{R}) \to O_2(\mathbf{R})$ in 3.9 en de determinantafbeelding $\det : O_2(\mathbf{R}) \to \{\pm 1\}$. Ook de samenstelling $\det \circ L : I_2(\mathbf{R}) \to \{\pm 1\}$ geeft weer een homomorfisme, de tekenafbeelding voor isometrieën. Algemener gaat men gemakkelijk na dat een samenstelling van een homomorfisme $G \to G'$ met een homomorfisme $G' \to G''$ een homomorfisme $G \to G''$ geeft.

De homomorfismen $G \to G$ van een groep G naar zichzelf worden *endomorfismen* genoemd. Men schrijft wel $\mathrm{End}(G)$ voor $\mathrm{Hom}(G, G)$. Voor *abelse* groepen G is voor ieder geheel getal n de afbeelding $x \mapsto x^n$ een endomorfisme van G. Voor niet-abelse groepen G krijgt men interessante voorbeelden van endomorfismen door de *conjugatie-afbeeldingen* $\sigma_g : x \mapsto gxg^{-1}$ te beschouwen voor $g \in G$. De in 4.1 verwoorde *homomorfie-eigenschap* voor σ_g volgt uit de identiteit

$$\sigma_g(xy) = gxyg^{-1} = gxg^{-1} \cdot gyg^{-1} = \sigma_g(x)\sigma_g(y).$$

Bijectieve endomorfismen $G \to G$ heten *automorfismen* van G. De conjugatie-afbeelding σ_g, die als inverse de conjugatie-afbeelding $\sigma_{g^{-1}}$ heeft, is er een voorbeeld van. De automorfismen van G zijn de isomorfismen van G met zichzelf, en men kan ze zien als de abstracte 'symmetrieën' van de groep G. Op grond van deze analogie zal het weinig verbazing wekken dat de verzameling $\mathrm{Aut}(G)$ van automorfismen van G een *groep* vormt onder samenstelling, de *automorfismengroep* van G. De lezer die nog aarzelend tegenover zoveel abstractie staat dient zich er bij wijze van nuttige oefening van te overtuigen dat $\mathrm{Aut}(G)$ daadwerkelijk aan alle groepsaxioma's voldoet.

Opgave 2. Zij G een groep waarvoor $\mathrm{End}(G)$ een groep is onder samenstelling. Bewijs: $G = 1$.

▶ Additieve notatie

In de 'homomorfie-identiteit' in 4.1 vindt de vermenigvuldiging xy plaats in G en de vermenigvuldiging $f(x)f(y)$ in G'. Indien de groepsbewerkingen in G en G' niet op dezelfde wijze genoteerd worden ziet de identiteit er minder 'symmetrisch' uit.

De enige andere manier om een groepsbewerking te noteren die men veelvuldig tegenkomt is de *additieve notatie*. Deze notatie wordt alleen gebruikt voor abelse groepen. In de additieve notatie schrijft men in plaats van een product xy een *som* $x + y$. De inverse x^{-1} van x wordt in deze notatie $-x$, ook wel de *tegengestelde* van x genoemd. Algemener schrijft men voor x^n met $n \in \mathbf{Z}$ hier nx. In plaats van een eenheidselement spreekt men additief liever van het *nulelement* van de groep en schrijft men 0.

Zoals we al opmerkten is de keuze van het symbool om de groepsbewerking aan te geven in principe irrelevant, en men kan abelse groepen zowel additief als multiplicatief noteren. Er zijn echter veel abelse groepen die al sinds Euler (1707–1783) een standaardnotatie voor hun groepsbewerking hebben. De bekendste voorbeelden zijn de optelgroepen $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ en $\mathbf{C}$ van respectievelijk gehele, rationale, reële en complexe getallen. Niemand zal het hier bij deze additieve groepen in zijn hoofd halen voor de optelling een ander symbool dan $+$ te gebruiken, al was het maar omdat op deze verzamelingen ook een productoperatie gedefinieerd is. Indien men uit de verzamelingen $\mathbf{Q}$, $\mathbf{R}$ en $\mathbf{C}$ het nulelement weglaat geeft de 'gewone' vermenigvuldiging een groepsstructuur. De corresponderende groepen $\mathbf{Q}^*$, $\mathbf{R}^*$ en $\mathbf{C}^*$ zijn de *multiplicatieve groepen* van respectievelijk rationale, reële en complexe getallen.

Opgave 3. Zijn er deelverzamelingen $\mathbf{Z}^* \subset \mathbf{Z} \setminus \{0\}$ waarop vermenigvuldiging een groepsstructuur induceert? Is er een *grootste*?

Bekende voorbeelden van homomorfismen in de analyse zijn de *exponentiaalafbeelding* $\exp : \mathbf{R} \to \mathbf{R}^*$ gegeven door $x \mapsto e^x$ en de *logaritme* $\log : \mathbf{R}_{>0} \to \mathbf{R}$ gegeven door $x \mapsto \log x$. De homomorfie-eigenschappen worden hier geschreven als $e^{x+y} = e^x e^y$ en $\log(xy) = \log x + \log y$.

▶ Kern en beeld

Omdat een homomorfisme de groepsbewerking respecteert moet het eenheidselementen naar eenheidselementen sturen en inversen bewaren.

4.2. Lemma. *Voor een homomorfisme $f : G \to G'$ geldt:*
1. *$f(e) = e'$, met $e \in G$ en $e' \in G'$ de eenheidselementen;*
2. *$f(x^{-1}) = f(x)^{-1}$ voor alle $x \in G$.*

Bewijs. Met behulp van de equivalentie (2.3) vinden we uit de identiteit $f(e) = f(ee) = f(e)f(e)$ gemakkelijk $f(e) = e'$. Voor $x \in G$ geldt nu $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$, en dus $f(x^{-1}) = f(x)^{-1}$. □

Met behulp van de tekenafbeeldingen $S_n \to \{\pm 1\}$ en $I_2(\mathbf{R}) \to \{\pm 1\}$ construeerden we in de voorafgaande paragrafen ondergroepen A_n en $I_2^+(\mathbf{R})$. Deze constructie blijkt van grote algemeenheid: *ieder* homomorfisme $f : G \to G'$ geeft aanleiding tot ondergroepen $\ker(f) \subset G$ en $f[G] \subset G'$ die de *kern* en het *beeld* van f heten.

4.3. Stelling. *Voor een homomorfisme $f : G \to G'$ geldt:*
1. *de kern $\ker(f) = \{x \in G : f(x) = e'\}$ van f is een ondergroep van G;*
2. *het beeld $f[G] = \{f(x) : x \in G\}$ van f is een ondergroep van G'.*

Bewijs. We gaan de eigenschappen (H1)–(H3) uit 2.7 na voor $\ker(f)$. De kern $\ker(f)$ bevat e wegens 4.2. Voor $x, y \in \ker(f)$ geldt $f(xy) = f(x)f(y) = e'e' = e'$, dus we hebben $xy \in \ker(f)$. Voor $x \in \ker(f)$ geldt $f(x^{-1}) = f(x)^{-1} = e'^{-1} = e'$, dus ook $x^{-1} \in \ker(f)$, en we zijn klaar.

Het bewijs van (2) is soortgelijk. Wegens $e' = f(e) \in f[G]$ hebben we (H1). De identiteit $f(x)f(y) = f(xy)$ geeft de geslotenheidsrelatie (H2), en (H3) volgt weer uit $f(x)^{-1} = f(x^{-1}) \in f[G]$. □

In het hoofdresultaat van deze paragraaf, de isomorfiestelling 4.9, zullen we zien dat er een directe relatie bestaat tussen de kern en het beeld van een homomorfisme.

Opgave 4. Bewijs dat voor een homomorfisme $f : G \to G'$ en ondergroepen $H \subset G$ en $H' \subset G'$ geldt:
1. het beeld $f[H] = \{f(x) : x \in H\}$ van H is een ondergroep van G';
2. het inverse beeld $f^{-1}[H'] = \{x \in G : f(x) \in H'\}$ van H' is een ondergroep van G.

Als illustratie van 4.3 en bovenstaande opgave bekijken we de determinantafbeelding $\det : \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}^*$. Dit is een homomorfisme dat de groep $\mathrm{GL}_2(\mathbf{R})$ van inverteerbare reële 2×2-matrices afbeeldt naar de vermenigvuldigingsgroep $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ van reële getallen verschillend van 0. De kern van dit homomorfisme is de groep $\mathrm{SL}_2(\mathbf{R})$ van matrices van determinant 1. Het beeld van de orthogonale groep $O_2(\mathbf{R}) \subset \mathrm{GL}_2(\mathbf{R})$ is

de tekenondergroep $\{\pm 1\} \subset \mathbf{R}^*$. Het inverse beeld van de tekenondergroep is de ondergroep $V \subset \mathrm{GL}_2(\mathbf{R})$ van lineaire afbeeldingen met determinant 1 of -1. De orthogonale groep $O_2(\mathbf{R})$ is een ondergroep van V.

*__Opgave 5.__ Laat zien dat V de ondergroep van oppervlaktebewarende afbeeldingen is in $\mathrm{GL}_2(\mathbf{R})$.

▶ Injectiviteit

Is $f : G \to G'$ een homomorfisme en $y \in G'$ een willekeurig element, dan heet het volledig origineel $f^{-1}(y) = \{x \in G : f(x) = y\}$ van een element $y \in G'$ de *vezel* van f boven y. Voor elementen $y \notin f[G]$ is de vezel $f^{-1}(y)$ leeg.

De vezel boven het eenheidselement $e' \in G'$ is de kern van f, hetgeen een ondergroep van G is. Aan deze vezel kunnen we zien of f injectief is.

4.4. Stelling. *Voor een homomorfisme $f : G \to G'$ geldt:*

$$f \text{ is injectief} \iff \ker(f) = \{e\}.$$

Bewijs. Voor elementen $g_1, g_2 \in G$ geldt wegens de homomorfie-eigenschap en 4.2

$$f(g_1) = f(g_2) \iff f(g_1)^{-1} f(g_2) = e' \iff f(g_1^{-1} g_2) = e' \iff g_1^{-1} g_2 \in \ker(f). \tag{4.5}$$

Geldt $\ker(f) = \{e\}$, dan volgt uit de laatste identiteit $g_1 = g_2$ en is f injectief. Omgekeerd is voor een injectief homomorfisme f duidelijk dat $\ker(f) = \{e\}$ geldt. □

Voorbeeld. De reële exponentiaalafbeelding $\exp : \mathbf{R} \to \mathbf{R}^*$ is een injectief homomorfisme met kern $\ker(\exp) = \{0\}$. De complexe exponentiaalafbeelding $\exp : \mathbf{C} \to \mathbf{C}^*$ heeft wegens Euler's formule $e^{a+bi} = e^a(\cos b + i \sin b)$ kern $2\pi i\mathbf{Z} = \{2k\pi i : k \in \mathbf{Z}\}$ en is dus niet-injectief.

Opgave 6. Zijn de beide bovenstaande exponentiaalafbeeldingen surjectief?

▶ Nevenklassen

Stelling 4.4 zegt dat als de vezel $N = \ker(f)$ boven het eenheidselement uit 1 element bestaat, dan bestaan alle niet-lege vezels uit 1 element. Door iets beter naar (4.5) te kijken kunnen we laten zien dat de niet-lege vezels altijd 'even groot' zijn als de kern. Immers, indien we in (4.5) het element g_1 vast nemen en nagaan wat de elementen $g_2 \in G$ zijn in de vezel boven $f(g_1)$, dan zien we dat dit de elementen $g_2 \in G$ zijn waarvoor $g_1^{-1} g_2 = n \in N$ geldt, oftewel $g_2 = g_1 n$ met $n \in N$. Anders gezegd: de vezel van een homomorfisme f boven een punt $f(g)$ in zijn beeld is de verzameling

$$gN = \{gn \in G : n \in N\} = \{x \in G : x = gn \text{ voor zekere } n \in N\}.$$

Een dergelijke verzameling heet een *linkernevenklasse* van de ondergroep $N \subset G$. De linksvermenigvuldiging $\lambda_g : G \to G$ met g is een bijectie die N op de nevenklasse gN afbeeldt. In het geval dat N eindig is, betekent dit dat alle nevenklassen gN evenveel elementen bevatten. Voor oneindige N betekent het bestaan van bijecties tussen de

nevenklassen van N dat ze allemaal 'even groot' zijn in de zin van de verzamelingentheorie: ze hebben alle dezelfde *cardinaliteit*.

De elementen van G worden kennelijk keurig verdeeld over de verschillende nevenklassen van $N = \ker(f)$. In het geval dat f de tekenafbeelding $\varepsilon : S_n \to \{\pm 1\}$ is, kwamen we deze gelijkverdeling reeds tegen in 2.10: voor $n > 1$ valt de groep S_n uiteen in een ondergroep A_n van even permutaties en een linkernevenklasse $(1\ 2)A_n$ van oneven permutaties; elk van beide klassen krijgt de helft, namelijk $n!/2$, van de elementen. Ook de symmetriegroep D_n van de regelmatige n-hoek, die als iedere vlakke symmetriegroep een tekenafbeelding toestaat, valt uiteen in een ondergroep C_n van n rotaties met teken $+1$ en een linkernevenklasse σC_n van n spiegelingen met teken -1.

Aan de gelijkverdeling van groepselementen over de nevenklassen van een ondergroep is de naam verbonden van de Fransman Joseph Louis Lagrange (1736–1813). We nemen een willekeurige ondergroep H van een groep G en beschouwen de collectie G/H van linkernevenklassen van H in G, d.w.z. de collectie deelverzamelingen van G van de vorm

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

Indien twee nevenklassen g_1H en g_2H een gemeenschappelijk element $g_1h_1 = g_2h_2$ bevatten, dan geldt $g_1H = g_1h_1H = g_2h_2H = g_2H$. Verschillende linkernevenklassen zijn dus altijd disjunct, en omdat ieder element $g \in G$ in een linkernevenklasse van H ligt (bijvoorbeeld in gH) zien we dat G een *disjuncte vereniging* is van de linkernevenklassen in G/H. Er geldt

$$g_1H = g_2H \quad \Longleftrightarrow \quad g_1^{-1}g_2 \in H. \tag{4.6}$$

Opgave 7. Laat zien dat de relatie $g_1 \sim g_2 \Longleftrightarrow g_1^{-1}g_2 \in H$ een equivalentierelatie op G is, en dat de equivalentieklassen van deze relatie de linkernevenklassen van H in G zijn.

Men noemt de afbeelding $G \to G/H$ van de *groep* G naar de *verzameling* G/H gegeven door $g \mapsto gH$ de *natuurlijke* of *kanonieke afbeelding*. Het aantal verschillende linkernevenklassen van H in G is de *index* $[G : H] = \#(G/H)$ van H in G. Voor oneindige G kan deze index oneindig zijn. Als G eindig is, dan is de index ook eindig en kan men de orde van G vinden door de index met het aantal elementen per nevenklasse te vermenigvuldigen.

4.7. Stelling van Lagrange. *Zij G een eindige groep en $H \subset G$ een ondergroep. Dan geldt*

$$\#G = [G : H] \cdot \#H. \qquad \square$$

Wie grafisch ingesteld is kan de ligging van een ondergroep in een groep op onderstaande manier schematisch weergeven: een ondergroep is een 'bouwsteen' H die samen met zijn 'getransleerden' gH de groep G netjes overdekt. Wie van het plaatje een 'echt' voorbeeld wil maken kan $G = D_7$ nemen en $H = \langle\sigma\rangle$ de ondergroep voortgebracht door een spiegeling σ.

H	g_1H	g_2H	$\cdots$	g_iH	$\cdots$	$\cdots$

Stelling 4.7 verklaart de diverse deelbaarheidsrelaties voor ordes van elementen en ondergroepen die we tegenkwamen in §1 en §2. Algemeen geldt het volgende.

4.8. Gevolg. *Voor een eindige groep G geldt:*
1. *de orde $\#H$ van een ondergroep $H \subset G$ deelt $\#G$;*
2. *de orde van een element $x \in G$ deelt $\#G$.*

Bewijs. De eerste uitspraak volgt direct uit 4.7. Voor (2) nemen we $H = \langle x \rangle$ en merken op dat de orde van de ondergroep $\langle x \rangle$ is gelijk aan de orde van het element x. □

Opgave 8. Bewijs dat iedere groep van *priemorde* $\#G = p$ isomorf is met de cyclische groep C_p.

▶ De isomorfiestelling

We zagen dat voor een homomorfisme $f : G \to G'$ met kern $N = \ker(f)$ de verzameling G/N van linkernevenklassen van N bestaat uit de vezels van f boven de punten van het beeld van f. We hebben dus een bijectie $G/N \leftrightarrow f[G]$ die de nevenklasse gN met het element $f(g) \in f[G]$ laat corresponderen. Nu is $f[G]$ wegens 4.3 een ondergroep van G', en dus zelf een groep. We concluderen, door *transport van structuur*, dat G/N kennelijk *óók* een groepsstructuur heeft. Deze observatie is één van de basisstellingen in de groepentheorie.

4.9. Isomorfiestelling. *Zij $f : G \to G'$ een homomorfisme met kern N, en definieer een bewerking op G/N door $g_1N \cdot g_2N = g_1g_2N$. Dan wordt G/N hiermee een groep, en de afbeelding*

$$\overline{f} : G/N \xrightarrow{\sim} f[G]$$

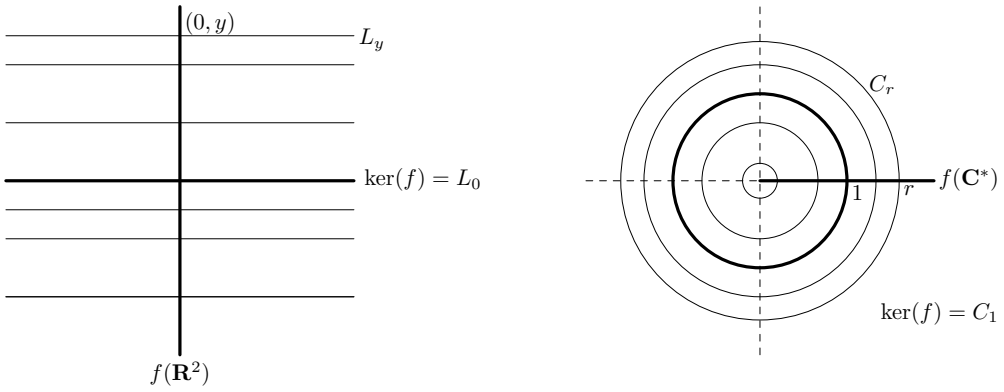
gegeven door $gN \mapsto f(g)$ een groepsisomorfisme.

Bewijs. Omdat we al weten dat $\overline{f} : G/N \to f[G]$ een bijectie van G/N naar $f[G]$ geeft hoeven we slechts na te gaan dat de productklasse $g_1N \cdot g_2N = g_1g_2N$ in G/N de nevenklasse is die met het product $f(g_1)f(g_2) \in f[G]$ correspondeert. De gewenste relatie $f(g_1g_2) = f(g_1)f(g_2)$ is precies de homomorfie-eigenschap van f. □

De isomorfiestelling laat zien dat het *beeld* van een homomorfisme op isomorfie na bepaald wordt door zijn *kern*. Het is *de* fundamentele stelling over homomorfismen, en we zullen hem nog veelvuldig tegenkomen.

4.10. Voorbeelden. Om een gevoel te krijgen voor wat stelling 4.9 ons vertelt geven we een drietal voorbeelden. Neem eerst $G = G' = \mathbf{R}^2$, en laat $f : \mathbf{R}^2 \to \mathbf{R}^2$ de afbeelding zijn gegeven door $(x, y) \mapsto (0, y)$. Dit is een lineaire afbeelding, dus zeker een homomorfisme, en hij beschrijft de projectie van het vlak op de y-as. De kern van deze afbeelding is de ondergroep $N = \{(x, 0) : x \in \mathbf{R}\}$ van punten op de x-as, en het beeld is de ondergroep $f[G] = \{(0, y) : y \in \mathbf{R}\}$ van punten op de y-as. De vezels van f zijn de horizontale lijnen $L_y = \{(x, y) : x \in \mathbf{R}\}$, en dit zijn de nevenklassen van N in $G = \mathbf{R}^2$. De groep $G = \mathbf{R}^2$ is de disjuncte vereniging van de lijnen L_y, en elk van deze

lijnen correspondeert met een uniek punt $(0, y) \in f[G]$. De natuurlijke optelling die $\overline{f}$ ons geeft op de verzameling G/N van horizontale lijnen in $G = \mathbf{R}^2$ is het 'optellen van y-coördinaten' gegeven door $L_{y_1} + L_{y_2} = L_{y_1+y_2}$. Onder de identificatie $L_y \leftrightarrow (0, y)$ zijn nu G/N en $f[G]$ inderdaad 'hetzelfde'.



Als tweede voorbeeld nemen we de afbeelding $f : \mathbf{C}^* \to \mathbf{R}^*$ gegeven door $z \mapsto |z|$. De multiplicatieve eigenschap $|z_1 z_2| = |z_1||z_2|$ van de absolute waarde zegt dat dit een homomorfisme is. De kern N van f is de *cirkelgroep* $\{z \in \mathbf{C}^* : |z| = 1\}$ van complexe getallen van absolute waarde 1. Merk op dat dit inderdaad een ondergroep is van $G = \mathbf{C}^*$. Het beeld van f is de ondergroep $f[G] = \mathbf{R}_{>0} = \{r \in \mathbf{R} : r > 0\}$ van positieve reële getallen in $\mathbf{R}^*$, en de nevenklassen van N in $G = \mathbf{C}^*$ zijn de verzamelingen van complexe getallen met gegeven absolute waarde $r > 0$. In ons plaatje zijn dit de cirkels C_r met straal r om de oorsprong. We zien weer dat G een disjuncte vereniging van dergelijke cirkels is. Iedere cirkel correspondeert met een unieke straal $r \in f[G]$, en de via $\overline{f}$ verkregen vermenigvuldiging op de verzameling G/N van cirkels is $C_{r_1} \cdot C_{r_2} = C_{r_1 r_2}$. Als groep is $G/N = \{C_r : r \in \mathbf{R}_{>0}\}$ wederom 'hetzelfde' als de groep $f[G] = \mathbf{R}_{>0}$.

Opgave 9. Maak een soortgelijk plaatje voor het homomorfisme $\mathbf{C}^* \to \mathbf{C}^*$ gegeven door $z \mapsto \frac{z}{|z|}$.

Als derde en laatste voorbeeld bekijken we het 'abstracte' homomorfisme

$$\begin{aligned} f : G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto (\sigma_g : x \mapsto gxg^{-1}) \end{aligned}$$

dat aan $g \in G$ de conjugatieafbeeldingen $\sigma_g : G \xrightarrow{\sim} G$ gedefinieerd door $\sigma_g(x) = gxg^{-1}$ toekent. We zagen al dat σ_g inderdaad een automorfisme van G is. De homomorfie-eigenschap van f komt neer op de identiteit $\sigma_{g_1 g_2} = \sigma_{g_1}\sigma_{g_2} \in \mathrm{Aut}(G)$. Voor alle $x \in G$ geldt inderdaad

$$\sigma_{g_1 g_2}(x) = g_1 g_2 x (g_1 g_2)^{-1} = g_1 (g_2 x g_2^{-1}) g_1^{-1} = \sigma_{g_1}\sigma_{g_2}(x).$$

De kern van f is de ondergroep

$$Z(G) = \{g \in G : gx = xg \text{ voor alle } x \in G\} \subset G$$

van elementen uit G die met alle elementen uit G commuteren. Men noemt $Z(G)$ het *centrum* van G. Het beeld van f is de ondergroep $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ van *inwendige automorfismen* van G. De isomorfiestelling geeft in dit geval een isomorfisme

$$G/Z(G) \xrightarrow{\sim} \mathrm{Inn}(G)$$

dat zich niet makkelijk in een plaatje laat vangen. Intuïtief is wel duidelijk dat er 'meer' inwendige automorfismen zijn naarmate er minder elementen in G zijn die met alle groepselementen commuteren. Voor abelse groepen geldt $Z(G) = G$ en zijn $G/Z(G)$ en $\mathrm{Inn}(G)$ beide de triviale groep. Voor $G = S_n$ hebben we $Z(S_n) = 1$ voor $n \neq 2$ (opgave 29), en in dit geval geeft de conjugatieactie een isomorfisme $S_n \xrightarrow{\sim} \mathrm{Inn}(S_n)$.

Inwendige automorfismen treden veelvuldig op. In de lineaire algebra komt men ze tegen indien men een lineaire afbeelding gegeven door een matrix A ten opzichte van een andere dan de standaardbasis als matrix wil schrijven: is T de matrix die de basistransformatie beschrijft, dan wordt TAT^{-1} de nieuwe matrix.

Algemener vindt men ze in allerhande situaties die betrekking hebben op een 'coördinatenkeuze'. Voor de inclusies $\mathrm{Sym}(F) \to I_2(\mathbf{R})$ in §3 die optreden voor verschillende keuzes van een 'assenkruis' in $\mathbf{R}^2$ zagen we dit in opgave 3.21, opgave 2.48 is hier een discrete variant van, en we zullen ook later nog voorbeelden tegenkomen (opgave 5.11). In de fysica kan men de relatie tussen metingen van verschillende waarnemers op soortgelijke wijze met elkaar in verband brengen.

▶ Normaaldelers

De isomorfiestelling laat zien dat voor een ondergroep $H \subset G$ de verzameling G/H een natuurlijke groepsstructuur bezit indien H optreedt als de kern van een homomorfisme f. In feite zegt 4.9 dat *als* H de kern is van het homomorfisme $f : G \to f[G]$, dan wordt f verkregen door een 'natuurlijk homomorfisme' $G \to G/H$ met een isomorfisme samen te stellen. We willen nu nagaan voor welke ondergroepen H er zo'n natuurlijk homomorfisme $G \to G/H$ bestaat.

Het blijkt dat zich alleen problemen voordoen als de verzameling G/H van *linker*nevenklassen, waar we ons tot dusver zo asymmetrisch op geconcentreerd hebben, verschilt van de collectie $H\backslash G$ van *rechternevenklassen* $Hg = \{hg : h \in H\}$ van H in G. In de situaties waarin we tot dusver linkernevenklassen gebruikten, zoals in de definitie van de index $[G : H]$ en de bewijzen van 4.7 en 4.8, kan men namelijk evengoed rechternevenklassen gebruiken – zie de opgaven 44 en 45. In *abelse* groepen geldt $gH = Hg$ en is onderscheid tussen linker- en rechternevenklassen overbodig. In het algemeen is dit echter niet het geval. Nemen we bij wijze van voorbeeld de ondergroep $H = \langle(1\ 2)\rangle$ in $G = S_3$, dan zien we dat de drie linkernevenklassen

$$H = \{(1), (1\ 2)\}, \qquad (1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}, \quad \text{en} \quad (2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$$

in G/H niet dezelfde zijn als de drie rechternevenklassen

$$H = \{(1), (1\ 2)\}, \qquad H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}, \quad \text{en} \quad H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$$

in $H\backslash G$. We gaan bewijzen dat er een *quotiëntgroep* G/H bestaat dan en slechts dan als G/H en $H\backslash G$ *niet* verschillen.

4.11. Definitie. *Een ondergroep $H \subset G$ heet een normale ondergroep of normaaldeler van G als hij aan de volgende equivalente eigenschappen voldoet:*

1. *voor ieder element $g \in G$ geldt $gH = Hg$;*
2. *voor ieder element $g \in G$ is $gHg^{-1} = \{ghg^{-1} : h \in H\}$ gelijk aan H.*

De equivalentie van beide genoemde eigenschappen ziet men in door rechtsvermenigvuldiging met respectievelijk g^{-1} en g toe te passen. De tweede formulering is prettiger omdat hij een goede manier geeft om aan normale ondergroepen te denken: het zijn de ondergroepen die onder alle inwendige automorfismen $\sigma_g \in \mathrm{Inn}(G)$ in zichzelf overgaan.

Opgave 10. Laat zien dat het in 4.11.2 voldoende is te eisen dat de *inclusie* $gHg^{-1} \subset H$ geldt.

In een abelse groep is iedere ondergroep een normaaldeler. In sommige andere groepen, zoals S_n, blijken ondergroepen slechts zelden normaal te zijn. Men schrijft $H \triangleleft G$ om aan te geven dat een ondergroep $H \subset G$ normaal is in G.

4.12. Propositie. *De kern van een groepshomomorfisme $f : G \to G'$ is normaal in G.*

Bewijs. Voor $h \in \ker(f)$ en $g \in G$ hebben we $f(ghg^{-1}) = f(g)e'f(g)^{-1} = e' \in G'$, dus $ghg^{-1} \in \ker(f)$. Wegens 4.11.2 (en opgave 10) is $\ker(f)$ nu normaal in G.

Een alternatief bewijs, met 4.11.1, krijgt men door op te merken dat de vezel boven een element $f(g)$, die we beschreven als *linker*nevenklasse gN van $N = \ker(f)$, even goed beschreven kan worden als de *rechter*nevenklasse Ng van N. □

Uit 4.12 volgt dat alleen voor normaaldelers $H \triangleleft G$ de verzameling G/H een groepsstructuur 'erft' van G. Immers, we willen dat de natuurlijke afbeelding $G \to G/H$ gegeven door $g \mapsto gH$ een homomorfisme wordt met kern H.

4.13. Stelling. *Zij G een groep en $N \triangleleft G$ een normaaldeler van G. Dan definieert de bewerking*

$$g_1N \cdot g_2N = g_1g_2N$$

een groepsstructuur op de verzameling G/N van nevenklassen van N in G. Hiermee wordt de natuurlijke afbeelding $G \to G/N$ een groepshomomorfisme met kern N.

Bewijs. We hoeven in feite slechts na te gaan dat de bewerking $g_1N \cdot g_2N = g_1g_2N$ *welgedefinieerd* is op G/N. Dit betekent dat indien we $g_1N = g_1'N$ en $g_2N = g_2'N$ hebben, ook $g_1g_2N = g_1'g_2'N$ moet gelden. De aannamen impliceren dat we $g_1' = g_1n_1$ en $g_2' = g_2n_2$ hebben voor zekere $n_1, n_2 \in N$, en dit geeft

$$g_1'g_2'N = g_1n_1g_2n_2N = g_1g_2(g_2^{-1}n_1g_2)n_2N.$$

Wegens de normaliteit van N geldt $g_2^{-1}n_1g_2 \in N$, en dit levert het gewenste resultaat.

Nu we eenmaal weten dat de 'nevenklassevermenigvuldiging' welgedefinieerd is op G/N volgen de groepsaxioma's uit 2.1 gemakkelijk. Het eenheidselement in G/N is de nevenklasse $eN = N$, en de inverse van gN in G/N is $g^{-1}N$. Associativiteit voor G/N is een direct gevolg van de associativiteit van de vermenigvuldiging op G.

De afbeelding $G \to G/N$ is per definitie van de bewerking op G/N een homomorfisme. De nevenklasse gN van N die g bevat is alleen gelijk aan N voor $g \in N$, dus de kern van dit homomorfisme is N. □

Uit 4.12 en 4.13 zien we dat de normaaldelers van een groep G precies de ondergroepen van G zijn die als kernen van homomorfismen op kunnen treden. Merk op dat *iedere* ondergroep $H \subset G$ als beeld van een homomorfisme optreedt: de inclusieafbeelding $H \to G$ is een eenvoudig voorbeeld.

▶ Quotiëntgroepen

De vorming van de *factorgroep* of *quotiëntgroep* G/N uit G en N is een fundamentele constructie die ook in de lineaire algebra ('*quotiëntruimtes*') en elders in de algebra uitgevoerd wordt. Men zegt wel dat men G *uitdeelt naar* N en noemt de quotiëntafbeelding $G \to G/N$ het *natuurlijke homomorfisme*.

Bij het rekenen in G/N schrijft men vaak $\overline{g}$ voor de *restklasse* gN van g *modulo* N. Deze notatie is alleen zinnig als uit de context duidelijk is modulo welke normaaldeler wordt gerekend; is dit niet het geval, dan schrijft men ook wel g mod N voor gN. Voor additief geschreven groepen noteert men de restklasse van g als $\overline{g}$ of $g+N$. Het element g heet een *representant* voor de restklasse gN. In het algemeen zijn er vele keuzen voor een dergelijke representant. Vaak definiëren we afbeeldingen op G/N door te zeggen wat er met een representant g van gN gebeurt. Men dient dan altijd te verifiëren dat de gegeven definitie onafhankelijk is van de keuze van de representant. Is dit het geval, dan is de afbeelding *welgedefinieerd*. We kwamen dit fenomeen tegen in het bewijs van 4.13, maar ook al in de definitie van de vermenigvuldiging modulo 8 in §1.

4.14. Voorbeelden. Men kan denken aan elementen van de factorgroep G/N als elementen van G waarbij men een 'welgekozen' deel van de informatie 'vergeet'. Nemen we voor $N = \{\pm 1\}$ de tekenondergroep in $G = \mathbf{R}^*$, dan is $G/N = \mathbf{R}^*/\{\pm 1\}$ de groep van reële getallen waarbij men het teken verwaarloost. Alleen de absolute waarde van het getal blijft dan over. Formeler gezegd: de afbeelding $\mathbf{R}^* \to \mathbf{R}^*$ gegeven door $x \mapsto |x|$ is een homomorfisme met kern $\{\pm 1\}$ en beeld $\mathbf{R}_{>0}$, en de isomorfiestelling geeft een isomorfisme $\mathbf{R}^*/\{\pm 1\} \cong \mathbf{R}_{>0}$.

Op soortgelijke wijze kan men aan de factorgroep $\mathbf{R}^*/\mathbf{R}_{>0}$ denken als de groep van reële getallen 'waarbij de grootte er niet toe doet'. Alleen de tekeninformatie blijft nu over, en we hebben een isomorfisme $\mathbf{R}^*/\mathbf{R}_{>0} \cong \{\pm 1\}$. Men krijgt het door 4.9 toe te passen op de *tekenafbeelding* $\mathbf{R}^* \to \{\pm 1\}$ gegeven door $x \mapsto \operatorname{sgn}(x)$.

Neem nu $G = \mathbf{R}$ de additieve groep van reële getallen en $\mathbf{Z} \subset \mathbf{R}$ de ondergroep van gehele getallen. De quotiëntgroep $\mathbf{R}/\mathbf{Z}$ bestaat uit reële getallen x waarvan men 'het gehele deel vergeet'. Immers, het additieve analogon van 4.6 zegt dat twee reële getallen $x, y \in \mathbf{R}$ in dezelfde restklasse in $\mathbf{R}/\mathbf{Z}$ liggen precies wanneer hun verschil $y - x$ geheel is. Iedere restklasse, die we nu additief schrijven als $x + \mathbf{Z}$, bevat een unieke representant $x - [x]$ in het halfopen eenheidsinterval $[0, 1)$. Hierbij geeft $[x]$ het grootste gehele getal $\leq x$ aan, ook wel de *entier* van x genoemd.

De situatie met $\mathbf{R}/\mathbf{Z}$ doet een beetje denken aan de grootte van hoeken in de vlakke meetkunde. De grootte van een hoek is een reëel getal, maar hoeken die een geheel veelvoud van 2π verschillen beschouwen we in de praktijk vaak als gelijk. We kunnen dit precies maken door de grootte van een hoek te zien als elementen van de 'hoekengroep' $\mathbf{R}/2\pi\mathbf{Z}$. Deze groep is isomorf met $\mathbf{R}/\mathbf{Z}$, want de vermenigvuldiging $x \mapsto 2\pi x$ geeft een isomorfisme $\mathbf{R}/\mathbf{Z} \xrightarrow{\sim} \mathbf{R}/2\pi\mathbf{Z}$.

Het 'cirkel-gevoel' dat de hoekengroep $\mathbf{R}/2\pi\mathbf{Z}$ geeft kan precies gemaakt worden met behulp van 4.9. Het homomorfisme $f : \mathbf{R} \to \mathbf{C}^*$ gegeven door $x \mapsto e^{ix}$ heeft wegens Eulers formule

$$e^{ix} = \cos x + i \sin x$$

als kern $2\pi\mathbf{Z}$ en als beeld de cirkelgroep $\mathbf{T} = \{z \in \mathbf{C}^* : |z| = 1\}$ uit 4.10. De isomorfiestelling 4.9 geeft nu een isomorfisme $\mathbf{R}/2\pi\mathbf{Z} \xrightarrow{\sim} \mathbf{T}$: de hoekengroep 'is' een cirkelgroep.

Opgave 11. Geef een expliciet isomorfisme $\mathbf{R}/\mathbf{Z} \xrightarrow{\sim} \mathbf{T}$.

Een ander bekend voorbeeld van een factorgroep is de additieve groep $\mathbf{Z}/n\mathbf{Z}$ van *gehele getallen modulo n*. Men spreekt hier van 'rekenen modulo n', waarbij $n \geq 1$ een willekeurig geheel getal is. Zoals de notatie suggereert krijgt men $\mathbf{Z}/n\mathbf{Z}$ door de optelgroep $\mathbf{Z}$ uit te delen naar de ondergroep $n\mathbf{Z} = \{nx : x \in \mathbf{Z}\}$ van n-vouden. Het geval $n = 60$ is bijvoorbeeld populair bij de Nederlandse Spoorwegen, waar men dienstregelingen heeft die zich in essentie iedere 60 minuten herhalen. De groep $\mathbf{Z}/n\mathbf{Z}$ is een cyclische groep van orde n voortgebracht door de restklasse $\overline{1}$. Hij is isomorf met de groep C_n uit 3.8. We komen in §6 nog uitgebreid terug op het rekenen modulo n. Ook de *vermenigvuldiging* van restklassen blijkt namelijk interessant te zijn.

Opgaven.

In onderstaande opgaven is, tenzij anders vermeld, G steeds een groep.

12. Laat zien dat 'isomorf zijn' van groepen een equivalentierelatie is.

13. Laat zien dat de afbeelding $\mathbf{C}^* \to \mathrm{GL}_2(\mathbf{R})$ gegeven door $a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ een injectief groepshomomorfisme is.

14. Laat zien dat de afbeelding $G \to G$ gegeven door $x \mapsto x^2$ een homomorfisme is dan en slechts dan als G abels is.

15. Laat zien dat de afbeelding $G \to G$ gegeven door $x \mapsto x^{-1}$ een homomorfisme is dan en slechts dan als G abels is.

16. Zij $f : G \to G'$ een homomorfisme en $x \in G$ van eindige orde. Bewijs: de orde van $f(x)$ deelt de orde van x.

17. Laat zien dat voor ieder tweetal groepen G_1 en G_2 de productverzameling $G = G_1 \times G_2$ onder de componentsgewijze bewerking $(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$ een groep wordt, de *productgroep*.

18. Laat zien dat de productgroep $C_2 \times C_2$ een viergroep van Klein is, en $C_2 \times C_3$ een cyclische groep van orde 6.

19. Laat $S \subset G$ een deelverzameling zijn die G voortbrengt, en $f, g : G \to G'$ twee homomorfismen die overeenstemmen op S. Bewijs: $f = g$.
['Een homomorfisme ligt vast door zijn waarden op een stel voortbrengers van de groep.']

20. Bestaat er een injectief homomorfisme $D_6 \to S_5$?

21. Laat zien dat er geen injectief homomorfisme $D_6 \to A_5$ bestaat.

22. Zij G een cyclische groep voortgebracht door $x \in G$. Bewijs dat G isomorf is met $\mathbf{Z}$ als x oneindige orde heeft, en met $\mathbf{Z}/n\mathbf{Z}$ als x eindige orde n heeft.

23. Zij G een cyclische groep van orde n. Bewijs dat G voor iedere deler d van n precies één ondergroep van orde d bevat.

24. Zij G een eindige groep van even orde. Bewijs: G bevat een element van orde 2.
[Hint: kijk naar de banen van de permutatie $G \to G$ gegeven door $x \mapsto x^{-1}$.]

25. Laat zien dat ieder endomorfisme $f \in \mathrm{End}(\mathbf{Z})$ van de vorm $x \mapsto kx$ is voor zekere $k \in \mathbf{Z}$. Concludeer dat er een bijectie $\mathrm{End}(\mathbf{Z}) \leftrightarrow \mathbf{Z}$ is gegeven door $f \leftrightarrow f(1)$. Is $\mathrm{End}(\mathbf{Z})$ een groep onder samenstelling?

26. Laat zien dat $\mathrm{Aut}(\mathbf{Z})$ isomorf is met de tekengroep $\{\pm 1\}$.

27. Laat G en G' isomorfe groepen zijn. Bewijs dat het *aantal* isomorfismen $G \to G'$ gelijk is aan de orde van de groep $\mathrm{Aut}(G)$.

28. Bestaat er een groep G en een endomorfisme $G \to G$ dat injectief is maar niet surjectief? Bestaat er een groep G en een endomorfisme $G \to G$ dat surjectief is maar niet injectief? Kun je in eventuele voorbeelden G eindig nemen?

29. Laat zien dat het centrum $Z(S_n)$ van S_n triviaal is voor $n \neq 2$. Wat is $Z(S_2)$?

30. Bepaal het centrum $Z(D_n)$ van de dihedrale groep D_n voor alle $n \geq 1$.

31. Bepaal het centrum van de matrixgroep $\mathrm{GL}_2(\mathbf{R})$.

32. Bepaal de centra van $O_2(\mathbf{R})$ en van $I_2(\mathbf{R})$.

33. Laat zien dat een groep G van orde $\#G \leq 5$ abels is.

34. Stel dat $G/Z(G)$ cyclisch is. Bewijs: G is abels, en $G/Z(G)$ is de triviale groep.

35. Zij V_4 de viergroep van Klein. Bewijs: $\mathrm{Aut}(V_4) \cong S_3$. Hoe volgt opgave 1.13 hier uit?

36. Bewijs: $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$.

37. Laat H_1 en H_2 ondergroepen van G zijn, en stel dat $G = H_1 \cup H_2$ geldt. Bewijs: $G = H_1$ of $G = H_2$. Geldt een vergelijkbare uitspraak voor de identiteit $G = H_1 \cup H_2 \cup H_3$?

38. Zij $n > 1$ geheel. Laat zien dat de natuurlijke vermenigvuldiging van restklassen in $\mathbf{Z}/n\mathbf{Z}$ *geen* groepsoperatie is.

39. Zij G een verzameling met een bewerking die aan de axioma's (G1) en (G2) uit 2.1 voldoet. Bewijs dat de deelverzameling

$$G^* = \{g \in G : \text{ er bestaat } x \in G \text{ met } xg = gx = e\}$$

van G een groep is onder de gegeven bewerking.

40. Laat zien dat de volgende voorbeelden van verzamelingen G aan de eisen uit de vorige opgave voldoen, en bepaal de bijbehorende groep G^*.
    1. $G = \mathbf{R}$ en de bewerking is vermenigvuldiging;
    2. $G = \mathbf{Z}$ en de bewerking is vermenigvuldiging;
    3. $G = \mathbf{Z}/8\mathbf{Z}$ en de bewerking is de natuurlijke vermenigvuldiging;
    4. X is een verzameling, en G bestaat uit de afbeeldingen $X \to X$ met als bewerking de samenstelling;
    5. X is een groep, en $G = \mathrm{End}(X)$ heeft als bewerking de samenstelling.

41. Laat A en B additief geschreven abelse groepen zijn. Bewijs dat $\mathrm{Hom}(A, B)$ een groep wordt indien we de som $f_1 + f_2$ van twee homomorfismen definiëren door de formule $(f_1 + f_2)(a) = f_1(a) + f_2(a)$. Is de beperking tot abelse groepen A noodzakelijk? Is de beperking tot abelse groepen B noodzakelijk?

42. Zij X een verzameling en A een abelse groep. Bewijs dat de verzameling $\mathrm{Map}(X, A)$ van A-waardige functies op X een groep is onder de 'functiesom' $(f_1 + f_2)(x) = f_1(x) + f_2(x)$. Is de beperking tot abelse groepen noodzakelijk?

43. Zij X een verzameling en $P(X)$ de machtsverzameling van X. Laat zien dat het symmetrisch verschil $A \,\Delta\, B = (A \cup B) \setminus (A \cap B)$ een groepsoperatie op $P(X)$ definieert, en dat $P(X)$ isomorf is met $\mathrm{Map}(X, \mathbf{Z}/2\mathbf{Z})$.
    [Hint: construeer eerst een bijectie $P(X) \to \mathrm{Map}(X, \mathbf{Z}/2\mathbf{Z})$ en 'transporteer structuur'. (Dit is een efficiënte manier om opgave 2.25 te maken.)]

44. Zij G een groep en $H \subset G$ een ondergroep. Laat zien dat de relatie

$$g_1 \sim g_2 \iff g_2 g_1^{-1} \in H$$

    een equivalentierelatie op G is, en dat de equivalentieklassen van deze relatie de rechternevenklassen van H in G zijn. Concludeer: G is een disjuncte vereniging van rechternevenklassen van H.

45. Zij G een groep en $H \subset G$ een ondergroep. Laat zien dat de bijectie $G \to G$ gegeven door $x \mapsto x^{-1}$ een bijectie $G/H \longrightarrow H\backslash G$ induceert. Concludeer dat de index $[G : H]$ van een ondergroep ook gedefinieerd kan worden als het aantal *rechter*nevenklassen van H in G.

46. Laat zien dat iedere ondergroep $H \subset G$ van index 2 een normaaldeler is.

47. Stel dat iedere linkernevenklasse van H in G ook een rechternevenklasse van H in G is. Bewijs dat H normaal is in G.

48. Laat zien dat de enige linkernevenklasse van $O_2(\mathbf{R})$ in $I_2(\mathbf{R})$ die tevens rechternevenklasse is de klasse van $O_2(\mathbf{R})$ zelf is.

49. Laat zien dat de ondergroep $T \subset I_2(\mathbf{R})$ van translaties een normaaldeler is in $I_2(\mathbf{R})$, en dat $I_2(\mathbf{R})/T$ isomorf is met de orthogonale groep $O_2(\mathbf{R})$.

50. Bewijs dat voor ieder punt $x \in \mathbf{R}^2$ de *stabilisator*

$$\mathrm{Stab}_x = \{\varphi \in I_2(\mathbf{R}) : \varphi(x) = x\} \subset I_2(\mathbf{R})$$

een ondergroep van $I_2(\mathbf{R})$ is die geconjugeerd is met $O_2(\mathbf{R})$. Concludeer dat $I_2(\mathbf{R})$ oneindig veel verschillende ondergroepen bevat die isomorf zijn met $O_2(\mathbf{R})$.

51. Laat zien dat de ondergroepen $H_1 = \langle (1\ 2), (3\ 4)\rangle$ en $H_2 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ van S_4 beide isomorf zijn met V_4. Laat zien dat H_1 niet normaal is in S_4 maar H_2 wel. Welke groep van orde 6 is S_4/H_2?

52. Laat n en k positieve getallen zijn met $k \leq n$, en $H \subset S_n$ de verzameling van permutaties die de deelverzameling $\{1, 2, 3, \ldots, k\} \subset \{1, 2, 3, \ldots, n\}$ op zichzelf afbeelden. Bewijs: H is een ondergroep van S_n van index $\binom{n}{k}$.
[Er zijn ook andere manieren om te bewijzen dat de binomiaalcoëfficiënt $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ een geheel getal is....]

53. Een ondergroep $H \subset G$ heet *karakteristiek* als $\sigma[H] = H$ geldt voor alle $\sigma \in \mathrm{Aut}(G)$. Laat zien dat karakteristieke ondergroepen normaal zijn, en geef een voorbeeld van een niet-karakteristieke normaaldeler.

54. Laat zien dat het centrum $Z(G)$ een karakteristieke ondergroep van G is.

55. Laat zien dat de ondergroep $\mathrm{Inn}(G)$ van inwendige automorfismen normaal is in de groep $\mathrm{Aut}(G)$ van alle automorfismen.
[Niet-inwendige automorfismen heten *uitwendig*, in het Engels *outer*. Men definieert $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$. (Dit is dus niet de 'groep van uitwendige automorfismen'!)]

56. Zij A een *abelse* groep. De *torsie-ondergroep* A^{tor} van A is de verzameling van elementen van eindige orde in A. Bewijs dat A^{tor} een ondergroep van A is, en dat A/A^{tor} buiten het eenheidselement geen elementen van eindige orde bevat.
[De aanname dat A abels is, is essentieel: zie opgave 2.36.]

57. Bepaal A^{tor} voor $A = \mathbf{Q}$, $\mathbf{Q}/\mathbf{Z}$ en $\mathbf{R}^*$. Bewijs: $(\mathbf{C}^*)^{\mathrm{tor}} \cong \mathbf{Q}/\mathbf{Z}$.

58. Laat H_1 en H_2 ondergroepen van een eindige groep G zijn met $H_1 \subset H_2 \subset G$. Bewijs: H_1 is een ondergroep van H_2, en er geldt

$$[G : H_1] = [G : H_2][H_2 : H_1].$$

*Is dit ook waar als H_1 van eindige index in een oneindige groep G is?

59. Laat N_1 en N_2 normaaldelers van G zijn met $N_1 \subset N_2 \subset G$. Bewijs dat de natuurlijke afbeelding $G/N_1 \to G/N_2$ een surjectief homomorfisme is met kern

$$N_2/N_1 = \{n_2 N_1 : n_2 \in N_2\}.$$

Concludeer: er is een natuurlijk isomorfisme

$$(G/N_1)/(N_2/N_1) \xrightarrow{\sim} G/N_2.$$

[Dit heet wel 'stapsgewijs uitdelen': men kan G eerst naar de kleine normaaldeler N_1 uitdelen, en vervolgens G/N_1 naar het beeld van de grote normaaldeler N_2 hierin.]

*60. Laat H_1 en H_2 ondergroepen van eindige index zijn in G. Bewijs dat $H_1 \cap H_2$ een ondergroep van eindige index in G is. Is $[G : (H_1 \cap H_2)]$ noodzakelijk een deler van $[G : H_1] \cdot [G : H_2]$?

5 Groepswerkingen

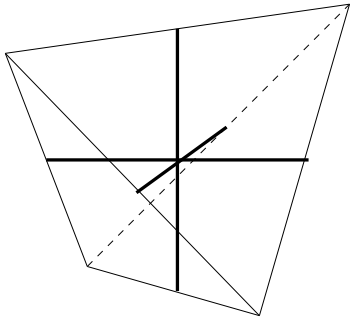
Veel van de groepen die we tot dusver tegen zijn gekomen hebben de eigenschap dat ze een 'bijbehorende' verzameling X permuteren. Voor de permutatiegroep $S(X)$ in §2 is dit precies de definitie van de groep, voor de diverse groepen van afbeeldingen in §3 zoals $I_2(\mathbf{R})$ en $\mathrm{GL}_2(\mathbf{R})$ hadden we steeds $X = \mathbf{R}^2$. In de meetkunde en de algebra maakt men vaak bij een object X een 'symmetriegroep' van X, die 'op X werkt'.

▶ Kubus- en tetraëdergroep

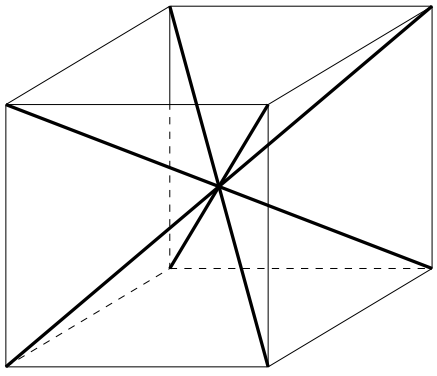
Voor vlakke figuren definieerden we de symmetriegroep in 3.7. Deze definitie generaliseert men zonder moeite tot het geval van symmetriegroepen $\mathrm{Sym}(X)$ van ruimtelijke objecten $X \subset \mathbf{R}^3$. Indien we voor X een tetraëder nemen, dan is $T = \mathrm{Sym}(X)$ een ondergroep van $S(X)$. In §1 zagen we dat het niet nodig is de werking op de hele tetraëder X te bekijken: omdat een symmetrie vastligt door zijn werking op de 4 hoekpunten is er een 'inclusie' $T \subset S_4$, en dit blijkt een groepsisomorfisme te zijn. Hiermee is de 'structuur' van de tetraëdergroep T bepaald: T is isomorf met de permutatiegroep S_4.

Op soortgelijke wijze kan men de groep K van symmetrieën van de kubus opvatten als ondergroep van S_8. Immers, iedere symmetrie in K ligt vast door zijn werking op de 8 hoekpunten van de kubus. Omdat er een boel manieren zijn om de hoekpunten van een kubus te nummeren is er in feite geen vaste inclusie $K \subset S_8$. Iedere keuze van een nummering geeft aanleiding tot een injectief groepshomomorfisme $K \to S_8$. In plaats van injectieve groepshomomorfismen spreekt men meestal van *inbeddingen* van K in S_8. Merk op dat zo'n inbedding niets anders is dan een isomorfisme van K met een ondergroep van S_8. Omdat niet alle verwisselingen van de 8 hoekpunten door symmetrieën in K gerealiseerd worden zijn de inbeddingen $K \to S_8$ zelf geen isomorfismen: het beeld is niet de hele groep S_8. Het is daarom niet direct duidelijk wat de 'structuur' of zelfs maar de orde van K is.

Zowel voor de tetraëdergroep S_4 als de kubusgroep K kan men de werking van de symmetrieën bestuderen op andere delen van tetraëder en kubus dan de hoekpunten.



$T \longrightarrow S_3$



$K \longrightarrow S_4$

Bekijken we bijvoorbeeld de actie van de tetraëdergroep $T \cong S_4$ op de drie lijnstukken die de middens van 'overstaande' ribben verbinden, dan krijgen we door keuze van

een nummering een 'meetkundig homomorfisme' $S_4 \to S_3$. Merk op dat het a priori helemaal niet duidelijk is dat er zo'n homomorfisme bestaat. Voor de kubusgroep K kan men de actie op de 4 lichaamsdiagonalen van de kubus bestuderen. Dit geeft na nummering aanleiding tot een homomorfisme $K \to S_4$.

De gevonden homomorfismen $T \to S_3$ en $K \to S_4$ zijn niet injectief. In het eerste geval is dat duidelijk op cardinaliteitsgronden: men kan de groep T van orde 24 niet injectief naar een groep van orde 6 afbeelden. In het tweede geval kan men gemakkelijk de kern uitrekenen: de symmetrieën van de kubus die de lichaamsdiagonalen vasthouden zijn de identiteit en de puntspiegeling in het middelpunt van de kubus.

Voor de tetraëder geven de spiegelingen in de vlakken door een 'verbindingslijnstuk' en één van de bijbehorende ribben de drie 2-cykels in S_3, en voor de kubus kan men door te spiegelen in het vlak door twee lichaamsdiagonalen de twee andere lichaamsdiagonalen verwisselen. Omdat S_3 en S_4 wegens 1.5 door hun 2-cykels worden voortgebracht volgt dat de homomorfismen $T \to S_3$ en $K \to S_4$ surjectief zijn.

Opgave 1. Ga na welke kubussymmetrieën de 3-cykels en 4-cykels in S_4 geven.

Voor de tetraëdergroep T bestaat de kern N van de surjectie $T \to S_3$ naast de identiteit uit de drie halve slagen om de ingetekende verbindingslijnstukken. Vatten we T als S_4 op, dan is het de normaaldeler $\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong V_4$ van S_4. Op 'meetkundige wijze' krijgen we zo een isomorfie

$$T/N = S_4/V_4 \xrightarrow{\sim} S_3.$$

Voor de kubusgroep K vertelt het bestaan van een surjectief homomorfisme $K \to S_4$ met kern $\{\pm 1\}$ voortgebracht door de centrale puntspiegeling -1 ons een boel: er geldt $K/\{\pm 1\} \cong S_4$ wegens de isomorfiestelling 4.9, en in het bijzonder $\#K = 2 \cdot 24 = 48$. Definiëren we het *teken* van een ruimtelijke symmetrie als na 3.9 via de determinant, dan is de ondergroep $K^+ \subset K$ van kubussymmetrieën van teken $+1$ een groep van orde 24 die injectief naar S_4 afbeeldt. Omgekeerd geeft nu het isomorfisme

$$K^+ \xrightarrow{\sim} S_4$$

een 'meetkundige interpretatie' van S_4 als *draaiingsgroep van de kubus* (cf. opgave 2.67).

Net als in bovenstaande voorbeelden is heel algemeen een *werking* van een groep op een verzameling niets anders dan een homomorfisme $G \to S(X)$.

5.1. Definitie. *Een werking of actie van een groep G op een verzameling X is een homomorfisme $\phi : G \to S(X)$.*

Als G op X werkt zeggen we dat X een *G-verzameling* is. Als ϕ injectief is heet de werking *trouw*. Voor $\phi(g)(x)$ schrijft men liever $g \circ x$, $g(x)$ of zelfs kortweg gx. Wegens de homomorfie-eigenschap hebben we $g_1 g_2 \circ x = g_1 \circ (g_2 \circ x)$ voor $g_1, g_2 \in G$, en werkt het eenheidselement $e \in G$ als de identiteit op X.

Opgave 2. Zij gegeven een afbeelding $G \times X \to X$, genoteerd als $(g, x) \mapsto g \circ x$. Laat zien dat dit tot een werking van G op X aanleiding geeft dan en slechts dan als aan de volgende twee voorwaarden voldaan is:

(W1) $e \circ x = x$ voor alle $x \in X$;
(W2) $gh \circ x = g \circ (h \circ x)$ voor alle $g, h \in G$ en $x \in X$.

In sommige situaties is het natuurlijker om een groep G 'van rechts' op de verzameling X te laten werken, en afbeeldingen $X \times G \to X$ te beschouwen die voldoen aan $x \circ (gh) = (x \circ g) \circ h$. Anders dan voor de werking in 5.1, die ook wel een *linkswerking* van G op X wordt genoemd, correspondeert zo'n rechtswerking niet met een homomorfisme $G \to S(X)$ maar met een *anti-homomorfisme* $G \to S(X)$. Zie de opgaven 19 en 20 voor details.

▶ Baan, stabilisator, dekpunt

De begrippen 'baan' en 'stabilisator' zijn in de context van werkingen erg natuurlijk.

5.2. Definitie. *Laat G een groep zijn die werkt op X. De stabilisator of isotropiegroep van een punt $x \in X$ in G is de ondergroep*

$$G_x = \{g \in G : gx = x\} \subset G,$$

en de baan van x onder G de deelverzameling

$$Gx = \{gx : g \in G\} \subset X.$$

Men ziet gemakkelijk in dat de stabilisator G_x een ondergroep is van G. De kern van het werkingshomomorfisme $\phi : G \to S(X)$ in 5.1 is gelijk aan de doorsnijding $\bigcap_{x \in X} G_x$ van alle stabilisatoren.

Het aantal elementen in de baan Gx, dat voor oneindige groepen G oneindig kan zijn, heet de *lengte* van de baan van x. Als er een $x \in X$ bestaat met $Gx = X$, dan heet de werking van G op X *transitief*.

Geldt $gx = x$ voor $g \in G$ en $x \in X$, dan heet x een *dekpunt* van g. Is x een gemeenschappelijk dekpunt van alle $g \in G$, dan heet x een dekpunt voor de werking van G op X. De dekpunten voor de werking van G op X zijn de punten $x \in X$ waarvoor de baan $Gx = \{x\}$ lengte 1 heeft. De verzameling van dekpunten wordt vaak aangegeven met X^G. Is X^G de lege verzameling, dan werkt G *dekpuntsvrij* op X.

De natuurlijke werking van $I_2(\mathbf{R})$ op $\mathbf{R}^2$ is transitief en dekpuntsvrij. De stabilisator van de oorsprong is de orthogonale groep $O_2(\mathbf{R})$. De stabilisatoren van de andere punten zijn met $O_2(\mathbf{R})$ geconjugeerde ondergroepen (opgave 4.50).

Algemeen geldt dat de stabilisator van een punt gx in de baan van x gelijk is aan gG_xg^{-1}, en dus geconjugeerd is met G_x. Dit volgt gemakkelijk uit de equivalenties

$$\widetilde{g}gx = gx \iff g^{-1}\widetilde{g}gx = x \iff g^{-1}\widetilde{g}g \in G_x \iff \widetilde{g} \in gG_xg^{-1}.$$

Het is weer één van de vele situaties waarin conjugatie-automorfismen optreden.

De lengte van de baan Gx van x kan men aflezen aan de grootte van de stabilisator G_x van x, en wel als volgt.

5.3. Stelling. *Zij X een G-verzameling en $x \in X$. Dan induceert de afbeelding $g \mapsto gx$ een bijectie*

$$G/G_x \longleftrightarrow Gx$$

tussen de verzameling van linkernevenklassen van G_x in G en de baan van x. In het bijzonder is de lengte van de baan Gx gelijk aan de index $[G : G_x]$.

Bewijs. Analoog aan de situatie in 4.6 hebben we equivalenties

$$gx = hx \iff h^{-1}gx = x \iff h^{-1}g \in G_x \iff gG_x = hG_x,$$

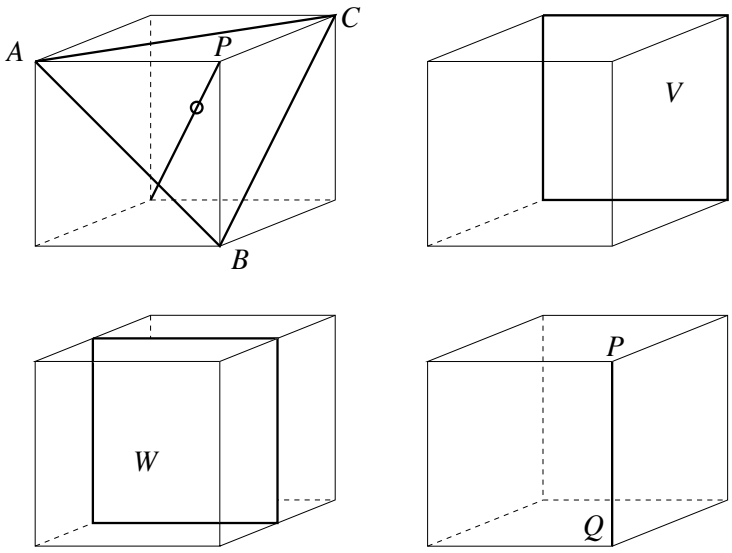
dus de afbeelding $g \mapsto gx$ stuurt linkernevenklassen van G_x injectief naar elementen van Gx. Surjectiviteit is duidelijk uit de definitie van Gx. □

Stelling 5.3 geeft ons voor iedere werking van een eindige groep G op een verzameling X de nuttige identiteit

$$\#Gx \cdot \#G_x = \#G.$$

In woorden: voor ieder punt is het product van zijn baanlengte en zijn stabilisatororde gelijk aan de groepsorde. Dit geeft ons een manier om de orde van allerhande symmetriegroepen te bepalen.

5.4. Voorbeeld. Neem de groep K van symmetrieën van de kubus. Dan kan men de orde van K op diverse manieren uitrekenen.



Neemt men een hoekpunt P van de kubus, dan bestaat de baan van P uit de 8 hoekpunten van de kubus. Een element van de stabilisator K_P van P ligt vast door zijn werking op de drie 'aangrenzende' hoekpunten A, B en C. Uit een plaatje is direct duidelijk dat $K_P \cong D_3 \cong S_3$ de groep van symmetrieën van de gelijkzijdige driehoek ABC is. Er volgt dat de kubusgroep orde $8 \cdot 6 = 48$ heeft. Neemt men in plaats van P het achtervlak V, dan heeft de baan van V lengte 6 en is de stabilisator K_V de groep D_4 van symmetrieën van het vierkant V. Weer is het product van de baanlengte en stabilisatororde gelijk aan $6 \cdot 8 = 48$. Voor het 'middenvlak' W in de kubus heeft de

baan lengte 3 en de stabilisator K_W orde 16. Immers, K_W bestaat uit K_V en de samenstellingen van de elementen uit K_V met de spiegeling in het vlak door W. Neemt men ten slotte een ribbe PQ, dan heeft de baan lengte 12 en is de stabilisator $K_{PQ} \cong V_4$ de groep voortgebracht door de spiegelingen in het middelloodvlak van PQ en in het vlak door PQ en de lichaamsdiagonaal uit P.

Opgave 3. Welke punten op de zijvlakken hebben een baan van lengte 48 onder de werking van K?

Als de banen van twee elementen $x, y \in X$ een niet-lege doorsnede hebben, dan zijn er $g_1, g_2 \in G$ zodat $g_1 x = g_2 y$. De baan van x is dan gelijk aan $Gx = Gg_1x = Gg_2y = Gy$, dus beide banen vallen samen. Twee G-banen zijn kennelijk of disjunct, of gelijk.

Opgave 4. Laat zien dat de banen van X onder G de equivalentieklassen in X zijn onder de equivalentierelatie $x \sim y \iff x = gy$ voor zekere $g \in G$.

We concluderen dat X onder de actie van G in banen uiteenvalt.

5.5. Stelling. *Een G-verzameling X is een disjuncte vereniging van banen.* □

In het geval van een transitieve werking is er slechts 1 baan, voor een dekpuntsvrije werking zijn er geen banen van lengte 1. De verzameling van banen van X onder de actie van G heet de *banenruimte* of *quotiëntruimte* van X onder de actie van G en wordt met $G\backslash X$ aangegeven.

5.6. Voorbeeld. Voor de actie van de orthogonale groep $G = O_2(\mathbf{R})$ op het vlak $\mathbf{R}^2$ is de oorsprong O een dekpunt. Voor $x \neq O$ is de baan Gx een cirkel om de oorsprong door x en de stabilisator G_x een groep van 2 elementen voortgebracht door de spiegeling σ_{ℓ_x} in de lijn ℓ_x door O en x. Inderdaad is $\mathbf{R}^2$ de disjuncte vereniging van O en de cirkels om O. Voor $x \neq O$ is de stabilisator G_x niet normaal in G; de nevenklassen in G/G_x zijn van de vorm ρG_x voor een rotatie $\rho \in G$, en de correspondentie $\rho G_x \leftrightarrow \rho x$ geeft de bijectie uit 5.3. De werking van $O_2(\mathbf{R})$ op $\mathbf{R}^2$ is noch transitief, noch dekpuntsvrij.

Opgave 5. Laat zien dat de natuurlijke actie van $O_2(\mathbf{R})$ op $\mathbf{R}^2 \setminus \{O\}$ niet transitief is, maar dat de stabilisatoren van de punten wel alle geconjugeerd zijn. Is de actie dekpuntsvrij?

▶ Banenformule

Er is voor een groep G die op een eindige verzameling X werkt een formule om het *aantal* banen onder de werking te tellen. Deze *banenformule*, die vaak aan de Engelsman William Burnside (1852–1927) wordt toegeschreven, gaat terug op werk van de Fransman Augustin-Louis Cauchy (1789–1857) en de Duitser Georg Ferdinand Frobenius (1849–1917). Hij maakt gebruik van het *permutatiekarakter* behorende bij de werking. Dit is de geheeltallige functie $\chi : G \to \mathbf{Z}$ die aan een element $g \in G$ het aantal

$$\chi(g) = \#\{x \in X : gx = x\}$$

van dekpunten van g in X toevoegt.

5.7. Banenformule. *Zij G een eindige groep die werkt op een eindige verzameling X, en χ het bijbehorende permutatiekarakter. Dan is het aantal G-banen in X gelijk aan*

$$\#(G \setminus X) = \frac{1}{\#G} \sum_{g \in G} \chi(g).$$

Bewijs. We kunnen het aantal G-banen van X als een som over de elementen van X schrijven, waarbij iedere $x \in X$ 'gewicht' $\frac{1}{\#Gx}$ krijgt. Met behulp van 5.3 volgt dan

$$\#(G \setminus X) = \sum_{x \in X} \frac{1}{\#Gx} = \frac{1}{\#G} \sum_{x \in X} \#G_x.$$

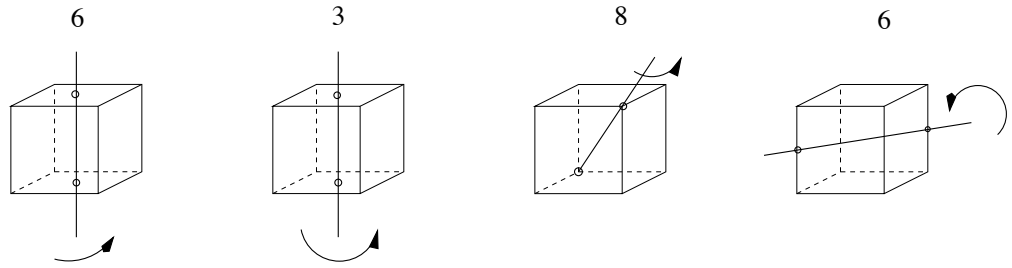
Het aantal elementen $\#G_x$ van de stabilisator van x laat zich schrijven als $\sum_{g \in G} \delta_{g,x}$, waarbij we $\delta_{g,x}$ gelijk nemen aan 1 als $gx = x$ geldt, en gelijk aan 0 als $gx \neq x$ geldt. Een verwisseling van de sommatievolgorde geeft dan voor het aantal banen

$$\frac{1}{\#G} \sum_{x \in X} \sum_{g \in G} \delta_{g,x} = \frac{1}{\#G} \sum_{g \in G} \sum_{x \in X} \delta_{g,x} = \frac{1}{\#G} \sum_{g \in G} \chi(g). \qquad \square$$

De banenformule zegt in woorden dat het aantal banen gelijk is aan het *gemiddelde* aantal dekpunten per element van de groep. Hij is bijzonder nuttig in de combinatoriek om aantallen configuraties te tellen in situaties waar symmetrie een rol speelt.

▶ Combinatorische toepassingen

Een *Hollandse kubus* is een kubus waarvan ieder van de 6 zijvlakken rood, wit of blauw is. Omdat er voor elk van de zijvlakken precies 3 kleurmogelijkheden zijn kunnen we een gegeven kubus op $3^6 = 729$ manieren kleuren. De verzameling X van de 729 kubussen die op deze manier ontstaan bevat minder dan 729 'echt verschillende' kubussen. Immers, veel van deze kubussen kunnen door draaiingen in elkaar worden overgevoerd. Om te weten te komen hoeveel verschillende Hollandse kubussen er bestaan, moeten we het aantal *banen* uitrekenen in X onder de werking van de draaiingsgroep van de kubus K^+. Zoals we voor 5.1 zagen is de groep K^+ isomorf met S_4.



Naast de identiteit $\mathrm{id} \in K^+$, die alle 729 elementen van X invariant laat, bestaan er vier typen van draaiingen van de kubus. Om elk van de drie centrale assen evenwijdig aan de ribben heeft men steeds twee kwartslagen. Een Hollandse kubus die onder één van deze 6 kwartslagen invariant is heeft de eigenschap dat de 4 zijvlakken die cyclisch verwisseld

worden alle dezelfde kleur hebben. Zo'n kubus heeft ten hoogste 3 verschillende kleuren, dus per kwartslag vinden we $3^3 = 27$ invariante kubussen in X.

De drie halve slagen om de bovengenoemde assen laten twee zijvlakken van een kubus op hun plaats en verwisselen de overige vier in twee paren van overstaande zijvlakken. Voor een hieronder invariante kubus hebben deze overstaande paren van zijvlakken dezelfde kleur. Dit laat vier kleurmogelijkheden over, en we vinden $3^4 = 81$ invariante kubussen in X voor elk van deze drie elementen in K^+.

De 8 slagen over $\pm 2\pi/3$ om één van de vier lichaamsdiagonalen verwisselen de 6 zijvlakken in twee 3-cykels. Dit geeft per element $3^2 = 9$ invariante kubussen in X.

Als laatste type hebben we de 6 halve slagen om de lijnen die het midden van een ribbe met het midden van de diametraal gelegen ribbe verbinden. Zij verwisselen de zijvlakken in drie paren, zodat we $3^3 = 27$ invariante kubussen vinden in X.

De banenformule geeft nu

$$\#(K^+ \setminus X) = \frac{1}{24}(1 \cdot 729 + 6 \cdot 27 + 3 \cdot 81 + 8 \cdot 9 + 6 \cdot 27) = 57$$

banen voor de actie van K^+ op X, en dit is het aantal verschillende Hollandse kubussen.

Opgave 6. Laat zien dat bij gebruik van n verschillende kleuren het aantal mogelijke kubussen gelijk is aan

$$\frac{n^2}{24}(n^4 + 3n^2 + 12n + 8).$$

Zie de opgaven 16–18 voor soortgelijke problemen met andere symmetriegroepen.

▶ Reguliere werking

Naast de meer meetkundige voorbeelden van werkingen van groepen op verzamelingen die we al noemden zijn er 'abstracte werkingen' die men voor alle groepen kan definiëren, en die we kunnen gebruiken om de structuur van eindige groepen te analyseren. De rest van deze paragraaf geeft een indruk van de mogelijkheden. In §9 komen we nog uitgebreid op dergelijke methoden terug.

Het meest directe voorbeeld van een abstracte groepswerking is de *reguliere werking* van een groep op zichzelf door linksvermenigvuldiging. We vinden hiermee dat *iedere* groep als ondergroep van een geschikt gekozen permutatiegroep is op te vatten.

5.8. Stelling van Cayley. *Zij G een groep en $S(G)$ de permutatiegroep op de verzameling G. Geef voor $g \in G$ met $\lambda_g : G \to G$ de linksvermenigvuldiging $x \mapsto gx$ aan. Dan is*

$$\begin{aligned} f : G &\longrightarrow S(G) \\ g &\longmapsto \lambda_g \end{aligned}$$

een inbedding, en G is isomorf met een ondergroep van $S(G)$.

Bewijs. We zagen na (2.3) dat λ_g voor iedere $g \in G$ een bijectie $G \to G$ geeft. Voor elementen g_1, g_2 en x in G hebben we

$$\lambda_{g_1 g_2}(x) = g_1 g_2 x = \lambda_{g_1}(g_2 x) = \lambda_{g_1}(\lambda_{g_2}(x)) = (\lambda_{g_1}\lambda_{g_2})(x),$$

dus f is een homomorfisme. Uit $\lambda_g(e) = g$ zien we dat λ_{g_1} en λ_{g_2} verschillend zijn voor $g_1 \neq g_2$, dus f is injectief en G is isomorf met de ondergroep $f[G] \subset S(G)$. □

Stelling 5.8, genoemd naar de Engelsman Arthur Cayley (1821–1895), is voornamelijk van theoretisch belang. De stelling drukt uit dat groepselementen op te vatten zijn als een soort permutaties, namelijk van G naar zichzelf. In de praktijk is de groep $S(G)$ meestal te groot voor expliciete berekeningen, en de keuze in de stelling van Cayley niet erg 'zuinig'. Zo kan men de diëdergroep D_5 van orde 10 in de permutatiegroep S_5 van orde 120 inbedden door te kijken naar zijn werking op de 5 hoekpunten van een regelmatige vijfhoek. Met de stelling van Cayley krijgen we een inbedding in een groep van orde $10! = 3628800$.

Opgave 7. Welke inbedding krijgen we voor $G = S_5$? Is deze wel 'zuinig'?

Indien we een ondergroep $H \subset G$ door linksvermenigvuldiging op G laten werken, dan is de banenruimte $H \setminus G$ precies de verzameling van rechternevenklassen van H in G. Deze verzameling gaven we voor 4.11 al aan met $H\backslash G$. Men kan banenruimtes kennelijk opvatten als een soort gegeneraliseerde verzamelingen van rechternevenklassen. Voor de reguliere werking van een normale ondergroep N op G 'erft' de banenruimte $N\backslash G = G/N$ een groepsstructuur van G zoals aangegeven in 4.13.

In de meetkunde komt het vaak voor dat een groep G van transformaties op een gegeven ruimte X werkt. Onder geschikte voorwaarden op de werking 'erft' de quotiëntruimte $G \setminus X$ meetkundige eigenschappen van X, bijvoorbeeld een afstandsbegrip. Voor X het platte vlak en G een geschikte groep van isometrieën kan men aardige voorbeelden als cylinders en tori krijgen – zie hiervoor de opgaven 25 en 26.

Een nuttige variant van de werking in 5.8 krijgen we door G niet op zichzelf, maar op de verzameling G/H van linkernevenklassen van een ondergroep H in G te nemen. De *reguliere werking* van G op G/H is nu gegeven door $g \circ xH = gxH$.

5.9. Stelling. *De reguliere werking $G \to S(G/H)$ van G op G/H is een homomorfisme met kern $\bigcap_{x\in G} xHx^{-1}$.*

Bewijs. Het is gemakkelijk na te gaan dat linksvermenigvuldiging met g de linkernevenklassen van H permuteert, en dat de gegeven afbeelding een werking is. Geldt $gxH = xH$ voor een nevenklasse xH, dan hebben we $x^{-1}gx \in H$ en $g \in xHx^{-1}$. Er volgt dat g alle nevenklassen vasthoudt dan en slechts dan als het een element is van $\bigcap_{x\in G} xHx^{-1}$. □

Opgave 8. Laat zien dat $N = \bigcap_{x\in G} xHx^{-1}$ de grootste normaaldeler van G is die bevat is in H.

De reguliere werking van G op G/H in 5.9 is een voorbeeld van een transitieve werking. De stabilisator van $H \in G/H$ is de ondergroep H zelf, en de bijectie in 5.3 is in dit

geval de identiteit. De stabilisatoren van de andere nevenklassen $xH \in G/H$ zijn de geconjugeerde ondergroepen xHx^{-1}.

Voor een normaaldeler N is de reguliere werking van G op G/N de samenstelling van de natuurlijke afbeelding $G \to G/N$ met de reguliere werking van G/N op zichzelf, en krijgen we uit 5.9 een nieuw bewijs van stelling 4.13. In het algemeen levert 5.9 een normaaldeler $N \subset H$ in G op.

Als toepassing van 5.9 generaliseren we het uit opgave 4.46 bekende resultaat dat iedere ondergroep van index 2 een normaaldeler is.

5.10. Stelling. *Zij $G \neq 1$ een eindige groep en p de kleinste priemdeler van $\#G$. Dan is iedere ondergroep $H \subset G$ van index p normaal in G.*

Bewijs. We laten zien dat de kern N van de afbeelding f in 5.9 gelijk is aan H. Dan is H normaal wegens 4.12. Omdat $S(G/H)$ isomorf is met de permutatiegroep S_p is de orde van $G/N \cong f[G] \subset S(G/H)$ een deler van de groepsorde $p!$ van $S(G/H)$. Er geldt $N \subset H \subset G$, dus $[G : N] = p \cdot [H : N]$ is een deler van zowel $p!$ als $\#G$. Dan is $[H : N]$ een deler van zowel $(p-1)!$ als $\#G$. Omdat $(p-1)!$ en $\#G$ vanwege de aanname geen gemeenschappelijke delers hebben vinden we $[H : N] = 1$ en $H = N$. □

▶ Conjugatiewerking

Een tweede standaardvoorbeeld van een abstracte groepswerking is de al eerder genoemde *conjugatiewerking*. We zagen in 4.10 dat voor ieder groepselement $g \in G$ de conjugatieafbeelding $\sigma_g : x \mapsto gxg^{-1}$ een bijectie van G is, en dat de afbeelding $g \mapsto \sigma_g$ een homomorfisme $G \to \mathrm{Aut}(G) \subset S(G)$ is met als kern $Z(G)$, het centrum van G. In het bijzonder is dit een werking van G op zichzelf. Voor deze werking is er een specifieke terminologie voor banen en stabilisatoren. De stabilisator van $x \in G$ onder conjugatie heet de *normalisator*

$$N_x = \{g \in G : gxg^{-1} = x\}$$

van het element x. Het is de ondergroep bestaande uit de elementen die met x commuteren. De banen onder conjugatie in G heten de *conjugatieklassen* van G. De cardinaliteit $[G : N_x]$ van een conjugatieklasse deelt voor eindige groepen de orde van de groep. De dekpunten voor de conjugatie-actie zijn de elementen van het centrum $Z(G)$ van G.

5.11. Voorbeeld. Voor de symmetrische groep S_n is de bepaling van de conjugatieklassen relatief eenvoudig. Immers, om voor willekeurige $\sigma, \tau \in S_n$ de geconjugeerde $\tau\sigma\tau^{-1}$ van σ te krijgen moet men (opgave 2.46) iedere cykel $(x_1\ x_2\ \cdots\ x_k)$ in de disjuncte cykeldecompositie van σ vervangen door $(\tau(x_1)\ \tau(x_2)\ \cdots\ \tau(x_k))$. Elementen in S_n zijn daarom geconjugeerd precies wanneer hun voor 2.7 gedefinieerde *cykeltypes* overeenstemmen.

De groep S_3 van orde 6 bevat naast het eenheidselement twee 3-cykels en drie 2-cykels: dit geeft drie conjugatieklassen van orde respectievelijk 1, 2 en 3. Voor grotere n krijgen we een iets uitgebreidere telpartij. Merkt men eerst op dat het aantal k-cykels in de S_n gelijk aan $\binom{n}{k} \cdot (k-1)!$ is, dan kan men in concrete gevallen het aantal elementen van gegeven cykeltype betrekkelijk eenvoudig uitrekenen. Zo vindt men voor $n = 4$ en

$n = 5$ de volgende aantallen elementen in elk van de conjugatieklassen. Merk op dat deze aantallen inderdaad delers zijn van de groepsordes $\#S_4 = 24$ en $\#S_5 = 120$.

	(1)	(12)	(123)	(1234)	(12)(34)	(12345)	(12)(345)
S_4:	1	6	8	6	3	–	–
S_5:	1	10	20	30	15	24	20

De groep S_4 kwamen we al tegen als de draaiingsgroep K^+ van de kubus. De 5 conjugatieklassen in S_4 zijn precies de 5 'types' van draaiingen van de kubus.

Opgave 9. Bepaal de grootte van alle conjugatieklassen in de alternerende groepen A_4 en A_5.

Iedere groep werkt ook door conjugatie op de verzameling van zijn ondergroepen. De baan onder conjugatie van een ondergroep $H \subset G$ bestaat uit de verzameling van met H geconjugeerde ondergroepen $\{gHg^{-1} : g \in G\}$. Omdat iedere conjugatie een automorfisme van G geeft, zijn al deze ondergroepen isomorf met H. Ze hebben ook allen dezelfde index in G. De dekpunten voor deze conjugatie-actie zijn precies de normaaldelers van G. De stabilisator van een ondergroep $H \subset G$ onder conjugatie heet weer de *normalisator*

$$N_G(H) = \{g \in G : gHg^{-1} = H\} \tag{5.12}$$

van H in G. Er geldt $H \triangleleft N_G(H)$, en $N_G(H)$ is de grootste ondergroep van G waarin H normaal is. Voor $H \triangleleft G$ geldt $N_G(H) = G$, en voor willekeurige H is het aantal met H geconjugeerde ondergroepen in G wegens 5.3 gelijk aan de index $[G : N_G(H)]$.

Opgave 10. Laat zien dat een ondergroep van eindige index maar eindig veel geconjugeerden heeft.

▶ Stelling van Cauchy

Indien X eindig is kan men de orde van X schrijven als de som van de lengtes van de banen onder G. Met behulp van de formule in 5.3 voor de lengte van een baan geeft dit

$$\#X = \sum_{Gx \in G\backslash X} [G : G_x].$$

De stabilisator G_x in deze formule hangt af van de keuze van de *representant* x in elke baan, maar de index $[G : G_x]$ niet. Immers, voor verschillende keuzen van x binnen een baan zijn de stabilisatoren geconjugeerd, en geconjugeerde ondergroepen hebben dezelfde index in G. In plaats van over banen kan men ook sommeren over de elementen in een *representantensysteem* voor de G-banen van X; dit is een deelverzameling van X die uit elke G-baan precies 1 element bevat. Is $\mathcal{B}$ zo'n representantensysteem, dan geldt $X^G \subset \mathcal{B}$ omdat elk dekpunt de unieke representant in zijn G-baan is. Men kan de voorafgaande formule daarom herschrijven als

$$\#X = \#X^G + \sum_{x \in \mathcal{B}\backslash X^G} [G : G_x]. \tag{5.13}$$

Als toepassing hiervan bewijzen we een fundamentele stelling van Cauchy over eindige groepen. Het bewijs is een generalisatie van een eenvoudiger argument dat alleen voor $p = 2$ werkt (opgave 4.24).

5.14. Stelling van Cauchy. *Zij G een eindige groep en p een priemdeler van $\#G$. Dan bevat G een element van orde p.*

Bewijs. Laat $X \subset G^p$ de verzameling van p-tupels $(g_1, g_2, \ldots, g_p) \in G^p$ zijn waarvoor $g_1 g_2 g_3 \ldots g_p = e$ geldt. Conjugatie van $g_1 g_2 g_3 \ldots g_p$ met g_p laat zien dat dan ook $g_p g_1 g_2 g_3 \ldots g_{p-1} = e$ geldt, dus we kunnen de p-tupels in X 'cyclisch opschuiven'. Dit definieert een werking van de cyclische groep $\mathbf{Z}/p\mathbf{Z}$ op X gegeven door

$$\overline{k} \cdot (g_1, g_2, \ldots, g_p) = (g_{p-k+1}, g_{p-k+2}, \ldots, g_{p-1}, g_p, g_1, \ldots, g_{p-k}) \qquad (1 \leq k \leq p).$$

De lengte van iedere baan onder deze werking is wegens 5.3 een deler van $\#(\mathbf{Z}/p\mathbf{Z}) = p$, dus gelijk aan 1 of p. De banen van lengte 1 komen van de dekpunten onder de opschuifactie, en dit zijn precies de constante rijtjes $(x, x, \ldots, x) \in X$. Wegens de producteis op X is er één zo'n rijtje voor ieder element $x \in G$ met $x^p = e$.

Het aantal elementen van X is gelijk aan $(\#G)^{p-1}$. Immers, men kan $p-1$ coördinaten vrij kiezen, en de laatste coördinaat ligt dan vast door de producteis. Omdat de orde van X een p-voud is en alle banen lengte 1 of p hebben zien we (al dan niet met behulp van 5.13) dat het aantal $\#X^G$ van banen van lengte 1 een veelvoud is van p. Dit betekent dat het aantal constante rijtjes $(x, x, \ldots, x) \in X$ deelbaar is door p. Behalve het triviale rijtje $(e, e, \ldots, e)$ zijn er dus nog andere rijtjes in X^G, en deze corresponderen met elementen van orde p in G. □

Algemener volgt uit 5.13 dat als G een *p-groep* is, d.w.z. een eindige groep G waarvan de orde een macht van een priemgetal p is, voor iedere eindige G-verzameling X de congruentie

$$\#X \equiv \#X^G \bmod p \tag{5.15}$$

geldt. Net als in het bewijs van 5.14 zijn dan namelijk alle banen buiten X^G van lengte deelbaar door p.

In 10.6 en 10.7 zullen we 5.15 gebruiken om te laten zien dat iedere groep G van orde deelbaar door p^k een ondergroep H van orde p^k bevat. Voor $k = 1$ is dit de stelling van Cauchy, want een ondergroep van orde p is van de vorm $\langle x \rangle$ met x van orde p. In het geval dat p^k de hoogste p-macht is die $\#G$ deelt heet een ondergroep $H \subset G$ van orde p^k een *Sylow-p-ondergroep* van G. Voor $k > 1$ hoeft zo'n ondergroep niet *cyclisch* te zijn. Opgave 57 laat zien waarom Sylow-p-ondergroepen altijd bestaan.

OPGAVEN.

11. Laat $\phi, \phi' : K \to S_8$ twee inbeddingen van de kubusgroep in S_8 zijn verkregen door de hoekpunten van de kubus op twee verschillende manieren te nummeren. Bewijs: $\phi = \sigma \circ \phi'$ voor een inwendig automorfisme $\sigma \in \mathrm{Inn}(S_8)$.

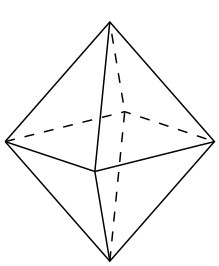
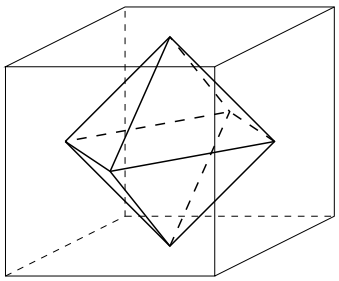
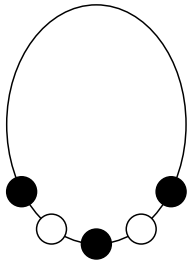
12. Laat zien dat de formule $r \circ z = z + r$ voor $r \in \mathbf{R}$ en $z \in \mathbf{C}$ een werking van de additieve groep $G = \mathbf{R}$ van reële getallen op de verzameling $X = \mathbf{C}$ van complexe getallen geeft. Beschrijf de banen onder deze werking.

13. Als de vorige opgave, voor $r \circ z = e^{ir}z$.

14. Een *octaëder* is de ruimtelijke figuur begrensd door 8 gelijkzijdige driehoeken. Laat Oct de groep van symmetrieën van de octaëder zijn. Bepaal de orde van de stabilisatoren van respectievelijk een hoekpunt en een zijvlak in Oct, en de orde van Oct zelf.

15. Laat zien dat de zes middens van de zijvlakken van een kubus de hoekpunten van een octaëder vormen. Leid hieruit af dat we een isomorfisme $K \xrightarrow{\sim}$ Oct hebben.

16. Bedenk wat een Hollandse octaëder is en bepaal het aantal 'echt verschillende' Hollandse octaëders. Hoe groot wordt dit aantal als we een octaëder en zijn spiegelbeeld ook als 'hetzelfde' opvatten?

17. Een *oranje-ketting* bestaat uit 5 bolvormige kralen aan een gesloten ketting die elk rood, wit, blauw of oranje zijn. De kralen kunnen vrij bewegen langs de ketting. Bepaal het aantal verschillende oranje-kettingen.

18. Een *magische achthoek* wordt verkregen door 8 gekleurde staafjes van gelijke lengtes tot een regelmatige achthoek te solderen. Hoeveel echt verschillende achthoeken kan men maken als er 10 kleuren staafjes beschikbaar zijn?

19. Een afbeelding $f : G \to G'$ van groepen heet een *anti-homomorfisme* als voor ieder tweetal elementen $x, y \in G$ de identiteit $f(xy) = f(y)f(x)$ geldt.
    a. Geef een voorbeeld van een anti-homomorfisme dat *geen* homomorfisme is.
    b. Gelden de uitspraken in 4.2 en 4.3 voor anti-homomorfismen?
    c. Bewijs: f is een anti-homomorfisme $\iff f^* : x \mapsto f(x^{-1})$ is een homomorfisme.

20. Een *rechtswerking* van een groep G op een verzameling X is een anti-homomorfisme $\phi : G \to S(X)$. We noteren in dit geval $\phi(g)(x)$ als $x \circ g$.
    a. Bewijs dat een afbeelding $X \times G \to X$, genoteerd als $(x, g) \mapsto x \circ g$, tot een rechtswerking aanleiding geeft dan en slechts dan als aan de volgende twee voorwaarden voldaan is:
    (RW1) $x \circ e = x$ voor alle $x \in X$;

(RW2) $x \circ gh = (x \circ g) \circ h$ voor alle $g, h \in G$ en $x \in X$.

b. Bewijs dat voor iedere rechtswerking $X \times G \to X$ de afbeelding $G \times X \to X$ gegeven door $(g, x) \mapsto x \circ g^{-1}$ een (links)werking is.

21. Laat zien dat de *modulaire groep*[15] $\mathrm{SL}_2(\mathbf{Z})$ van geheeltallige matrices van determinant 1 werkt op het complexe bovenhalfvlak $\mathcal{H} = \{z : \mathrm{Im}(z) > 0\}$ door $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(z) = \frac{az+b}{cz+d}$. Bepaal de isotropiegroepen van $z = i$, $z = 2i$ en $z = \zeta_3$ (de derde eenheidswortel in $\mathcal{H}$). Is de werking transitief?

22. Laat zien dat een matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ geen dekpunten heeft op het complexe bovenhalfvlak $\mathcal{H}$ als zijn spoor absolute waarde $|a + d| > 2$ heeft.

23. Zij $F = \mathrm{Map}(\mathcal{H}, \mathbf{C})$ de verzameling van complexwaardige functies op $\mathcal{H}$. Definieer voor $f \in F$ en $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ de functie $f \circ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ op $\mathcal{H}$ door $(f \circ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))(z) = f(\frac{az+b}{cz+d})$. Bewijs dat dit een rechtswerking van $\mathrm{SL}_2(\mathbf{Z})$ op F geeft.
[Als dekpunten onder deze werking vinden we de *modulaire functies*.]

24. Laat zien dat voor iedere G-verzameling X de verzameling $\mathrm{Map}(X, \mathbf{C})$ van complexwaardige functies op X een natuurlijke rechtswerking van G heeft.

25. Definieer de natuurlijke translatiewerking van $\mathbf{Z}$ op het complexe vlak $\mathbf{C}$ door $k \circ z = z + k$, en laat Ω de banenruimte zijn. De *afstand* tussen twee banen $B_1, B_2 \in \Omega$ is $d(B_1, B_2) = \min\{|z_1 - z_2| : z_1 \in B_1, z_2 \in B_2\}$.
   a. Laat zien dat Ω geïdentificeerd kan worden met de factorgroep $\mathbf{C}/\mathbf{Z}$.
   b. Laat zien dat voor iedere $z_0 \in \mathbf{C}$ de natuurlijke afbeelding $\pi : \mathbf{C} \to \Omega$ gegeven door $z \mapsto \mathbf{Z} + z$ injectief en afstand bewarend is op een schijfje rond z_0. Concludeer dat de groep Ω er 'locaal uitziet als het platte vlak'. [Men noemt π een *locale isometrie*.]
   c. Leg uit waarom de groep Ω 'topologisch een cylinder is'.
   [De *topologie*[16] maakt deze vraag precies: $\mathbf{C}/\mathbf{Z}$ is *homeomorf* met de cylinder.]

*26. Formuleer en maak het analogon van de vorige opgave, met $\mathbf{Z}$ vervangen door de groep $\mathbf{Z}[i] = \{a + bi \in \mathbf{C} : a, b \in \mathbf{Z}\}$ van *gehele getallen van Gauss*.
[Je krijgt als banenruimte het fietsbandoppervlak dat *torus* genoemd wordt.]

27. Zij X een G-verzameling. Laat zien dat een deelverzameling $Y \subset X$ *stabiel* is onder G (d.w.z. er geldt $gy \in Y$ voor $g \in G$ en $y \in Y$) dan en slechts dan als Y een vereniging van banen is. Concludeer: een ondergroep $H \subset G$ is normaal dan en slechts dan als H een vereniging van conjugatieklassen is.

28. Laat zien dat de enige normaaldelers van de alternerende groep A_5 de triviale normaaldelers $N = 1$ en $N = A_5$ zijn.

29. Zij G een eindige groep die transitief werkt op een verzameling X en N een normaaldeler van G. Bewijs dat alle banen van X onder N even lang zijn. Laat zien dat de voorwaarde dat N normaal is niet weggelaten kan worden.

30. Voor G-verzamelingen X en Y geven we met $\mathrm{Map}(X, Y)$ de verzameling van afbeeldingen van X naar Y aan. Bewijs dat $\mathrm{Map}(X, Y)$ een G-verzameling wordt met de definitie
$$(gf)(x) = gf(g^{-1}x) \qquad (g \in G, \quad f \in \mathrm{Map}(X, Y), \quad x \in X).$$

31. Een afbeelding $f : X \to Y$ van G-verzamelingen heet *G-equivariant* als hij voldoet aan $f(gx) = g(f(x))$ voor $g \in G$ en $x \in X$. Bewijs dat de dekpunten van G in $\mathrm{Map}(X, Y)$ precies de G-equivariante afbeeldingen van X naar Y zijn.

32. Definieer een isomorfiebegrip voor G-verzamelingen, en laat zien dat de bijectie $G/G_x \longrightarrow Gx$ uit 5.3 een isomorfisme van G-verzamelingen is.

33. Zij G een eindige groep. Bewijs dat er een n bestaat waarvoor G isomorf is met een ondergroep van $\mathrm{GL}_n(\mathbf{R})$.

34. Zij G een eindige groep van orde n en $G \to S(G) \cong S_n$ de Cayley-afbeelding uit 5.8. Bewijs dat het beeld van een element $g \in G$ van orde k een product van n/k disjuncte k-cykels in $S(G)$ is. Wanneer bevat het beeld van G in $S(G)$ oneven permutaties?

35. Zij G een eindige groep van orde $2u$ met u oneven. Bewijs dat de elementen van oneven orde een ondergroep van orde u in G vormen. [Hint: gebruik de vorige opgave.]

36. Laat zien dat de elementen van oneven orde geen ondergroep vormen in S_n voor $n > 3$.

37. Zij G een eindige groep van orde $2^n u$ met u oneven, en stel dat G een element van orde 2^n bevat. Bewijs dat de elementen van oneven orde een ondergroep van index 2^n in G vormen.

38. Zij $H \subset D_{10}$ de deelverzameling van elementen van oneven orde in D_{10}. Is H een ondergroep? Zo ja, bepaal de index $[D_{10} : H]$.

39. Bewijs dat iedere groep van orde 6 isomorf is met C_6 of S_3.

40. Zij $I(n)$ het aantal isomorfieklassen van groepen van orde n. Laat zien $I(n)$ eindig is voor alle $n \geq 1$, en bereken $I(n)$ voor $n \leq 7$.

41. Laat zien dat voor de waarde $I(n)$ in de vorige opgave $I(n) \leq ((n-1)!)^{n-1}$ geldt. *Kun je een betere bovengrens vinden?[17]

42. Zij $\mathcal{C}$ een representantensysteem voor de conjugatieklassen van G en geef met N_x de normalisator van $x \in G$ aan. Bewijs de *klassenformule*

$$\#G = \#Z(G) + \sum_{x \in \mathcal{C} \setminus Z(G)} [G : N_x].$$

43. Zij G een eindige groep met precies twee conjugatieklassen. Bewijs dat G de cyclische groep van orde 2 is.
[Er bestaan oneindige groepen met precies twee conjugatieklassen.[18]]

*44. Zij $n \geq 1$ een geheel getal. Bewijs dat er (op isomorfie na) maar *eindig* veel eindige groepen met precies n conjugatieklassen zijn.
[Hint: gebruik het jaarwisselingspuzzeltje aan het einde van §1.]

45. Zij G een groep van priemmachtorde $p^k > 1$. Bewijs: $Z(G) \neq 1$.

46. Zij p een priemgetal. Bewijs dat iedere groep van orde p^2 abels is.

47. Stel dat G een ondergroep H van eindige index $[G : H] > 1$ bevat. Bewijs dat G een normaaldeler N van eindige index $[G : N] > 1$ bevat.

48. Zij $H \subset \mathbf{R}$ een ondergroep van eindige index in de optelgroep $\mathbf{R}$ van de reële getallen. Bewijs: $H = \mathbf{R}$. Geldt de analoge uitspraak voor ondergroepen van de optelgroep $\mathbf{Q}$ van de rationale getallen?

49. Zij G een eindige groep die transitief werkt op een verzameling X met $\#X > 1$. Bewijs: er is een element $g \in G$ dat geen enkel element van X vasthoudt, d.w.z. $gx \neq x$ voor alle $x \in X$.

50. Zij $\mathcal{C}$ een verzameling van representanten voor de conjugatieklassen van een eindige groep G. Bewijs dat G voortgebracht wordt door $\mathcal{C}$.

51. Bepaal de normalisator van $H = \langle(1\ 2\ 3)\rangle$ in A_4 en in S_4.

52. Bepaal de normalisator van $H = \langle(1\ 2\ 3\ 4\ 5)\rangle$ in A_5 en in S_5.

53. Zij C de conjugatieklasse van een even permutatie $\sigma \in S_n$. Bewijs dat C een conjugatieklasse is in A_n als de normalisator van σ in de S_n een oneven permutatie bevat, en een vereniging van twee conjugatieklassen in A_n van dezelfde orde als dit niet het geval is.

*54. Stel dat het element $\sigma \in A_n$ in de vorige opgave een disjuncte cykeldecompositie heeft corresponderend met de partitie $n = a_1 + a_2 + \ldots + a_t$. Bewijs: C is een conjugatieklasse in A_n dan en slechts dan als twee a_i's gelijk zijn of er een even waarde a_i voorkomt.

55. Zij G een eindige groep en p een priemgetal dat de orde van G deelt. Zij t het aantal elementen van orde p in G, en h het aantal ondergroepen van orde p in G. Bewijs: $t = h(p-1)$ en $h - 1$ is deelbaar door p.

*56. Laat zien dat elke ondergroep van S_n kan worden voortgebracht met ten hoogste $n-1$ elementen.
[Hint: bewijs met inductie naar n de *sterkere* uitspraak dat $n - t$ elementen voldoende zijn, met t het aantal banen van $\{1, 2, 3, \ldots, n\}$ onder de werking van de ondergroep.]

57. Zij G groep van orde $n = p^k m$ met p priem en $p \nmid m$. Een *Sylow-p-ondergroep* van G is een ondergroep $H \subset G$ van orde p^k. Neem om te bewijzen dat zo'n H bestaat X gelijk aan de collectie van *deelverzamelingen* van G van orde p^k, en laat G werken op de verzamelingen in X door linksvermenigvuldiging: $gV = \{gv : v \in V\}$ voor $g \in G$ en $V \in X$.
    a. Bewijs: $\#X = \binom{n}{p^k} \equiv m \bmod p$.
    b. Bewijs dat er $V \in X$ bestaat waarvoor de baan GV lengte copriem met p heeft.
    c. Laat zien dat de stabilisator $H = G_V$ van een verzameling V als in b een Sylow-p-ondergroep van G is.

58. Zij $p \geq 3$ een priemgetal, en n een positief geheel getal.
    a. Laat zien dat de zijden van een regelmatige p-hoek op $(n^p + (p-1)n)/p$ echt verschillende manieren gekleurd kunnen worden, indien iedere zijde 1 van n mogelijke kleuren krijgt.
    b. Concludeer dat $n^p - n$ deelbaar is door p. (Vergelijk met stelling 6.18.)

59. Zij G een eindige groep, en H een ondergroep van G. Kan het aantal conjugatieklassen van H groter zijn dan dat van G?

6 Gehele getallen

In deze paragraaf bestuderen we wiskundige objecten die zo fundamenteel zijn dat ze in alle ontwikkelde culturen voorkomen: *gehele getallen*. Men krijgt de verzameling $\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ van gehele getallen door het toevoegen van negatieve getallen aan de verzameling $\mathbf{N} = \{0, 1, 2, \ldots\}$ van niet-negatieve of *natuurlijke* getallen. Sommigen rekenen 0 niet tot de natuurlijke getallen, en het getal 0 is niet-natuurlijk in de zin dat het net als de negatieve getallen een vinding van later datum is die bijvoorbeeld bij de oude Grieken nog niet voorkomt. We gaan hier niet in op de axiomatische beschrijvingen[19] van $\mathbf{N}$ die door de Italiaan Peano (1858–1932) gegeven zijn. Dergelijke axioma's formaliseren in de logica de intuïtief duidelijke eigenschappen van de natuurlijke getallen, waaronder de door ons al gebruikte bewijsmethode van de *volledige inductie* en het feit dat iedere niet-lege verzameling van positieve getallen een *kleinste element* bevat.

De uitbreiding van $\mathbf{N}$ tot $\mathbf{Z}$ behoeft geen rechtvaardiging voor wie wel eens een kasboek of een thermometer gezien heeft; vanuit groepentheoretisch perspectief kan men zeggen dat $\mathbf{Z}$, anders dan $\mathbf{N}$, een *groep* is onder de optelling. Het is een *oneindige cyclische groep* met 1 (of -1) als voortbrenger. Iedere cyclische groep voortgebracht door een element x van oneindige orde is isomorf met $\mathbf{Z}$ onder de bijectie $x^k \leftrightarrow k$.

Iedere eindige cyclische groep is een quotiënt van $\mathbf{Z}$. Immers, als $G = \langle x \rangle$ voortgebracht wordt door een element x van orde n, dan is de afbeelding $\mathbf{Z} \to G$ gegeven door $k \mapsto x^k$ een surjectie met kern $n\mathbf{Z} = \{nk : k \in \mathbf{Z}\}$. Wegens de isomorfiestelling krijgen we $G \cong \mathbf{Z}/n\mathbf{Z}$. Dit is de 'additieve notatie' voor de cyclische groep C_n uit 3.8.

▶ Deling met rest

De cyclische groepen $\mathbf{Z}/n\mathbf{Z}$ van *restklassen modulo* n zijn de enige quotiënten van $\mathbf{Z}$. Het bewijs hiervan berust op het nuttige begrip *deling met rest*.

6.1. Deling met rest. *Laat a en $b > 0$ natuurlijke getallen zijn. Dan bestaan er natuurlijke getallen q en r met*

$$a = qb + r \qquad en \qquad 0 \leq r < b.$$

Bewijs. De verzameling $S = \{a, a - b, a - 2b, a - 3b, \ldots\}$ bevat natuurlijke getallen, zoals $a \in S$, en dus een *kleinste* natuurlijk getal $r = a - qb$. Nu is het getal $r - b \in S$ kleiner dan r, dus negatief. Dit geeft zoals verlangd $0 \leq r < b$. □

Opgave 1. Formuleer en bewijs een analoge stelling voor a en $b \neq 0$ geheel.

Wat 6.1 zegt is niet meer dan het bekende feit dat je b 'net zo vaak van a af kunt trekken tot het niet meer gaat'. Het getal r in 6.1 heet de *rest* van a bij deling door b. Voor $b = n$ laat 6.1 zien dat we de elementen van $\mathbf{Z}/n\mathbf{Z}$ aan kunnen geven met $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$. Een gelijkheid $\overline{x} = \overline{y} \in \mathbf{Z}/n\mathbf{Z}$ voor $x, y \in \mathbf{Z}$ heet een *congruentie* en wordt sinds Gauss (1777–1855) als $x \equiv y \bmod n$ genoteerd.

6.2. Gevolg. *Iedere ondergroep van* $\mathbf{Z}$ *is van de vorm* $n\mathbf{Z}$ *voor een natuurlijk getal* n*.*

Bewijs. Zij $H \subset \mathbf{Z}$ een ondergroep. Als H de triviale groep is hebben we $n = 0$. Als H niet-triviaal is bevat H positieve getallen, immers met $x \in H$ geldt $-x \in H$. Zij dan n het kleinste positieve getal in H. Dan hebben we $H \supset n\mathbf{Z}$, en we laten zien dat gelijkheid geldt. Voor $a \in H$ willekeurig schrijven we $a = qn + r$ als in 6.1. Dan is $r = a - qn$ een niet-negatief getal kleiner dan n, en als verschil van elementen in H is het bevat in H. Er volgt $r = 0$ en $a = qn \in n\mathbf{Z}$, dus $H = n\mathbf{Z}$. □

▶ Ggd en kgv

Met behulp van 6.2 kan men deelbaarheidseigenschappen van gehele getallen uitdrukken in termen van ondergroepen van $\mathbf{Z}$. We schrijven $a\mathbf{Z} + b\mathbf{Z}$ voor de ondergroep van $\mathbf{Z}$ voortgebracht door a en b. Hij bestaat uit de elementen $xa + yb$ met $x, y \in \mathbf{Z}$.

6.3. Definitie. *Voor gehele getallen* a *en* b *gebruiken we de volgende terminologie.*

1. *Als* $a\mathbf{Z} \supset b\mathbf{Z}$ *geldt, dan heet* a *een deler van* b *en* b *een veelvoud van* a*.*
2. *Als* $a\mathbf{Z} + b\mathbf{Z} = \mathbf{Z}$ *geldt, dan heten* a *en* b *onderling ondeelbaar of copriem.*
3. *De niet-negatieve voortbrengers van* $a\mathbf{Z} + b\mathbf{Z}$ *en* $a\mathbf{Z} \cap b\mathbf{Z}$ *heten de grootste gemene deler* $\gcd(a, b)$ *en het kleinste gemene veelvoud* $\mathrm{kgv}(a, b)$ *van* a *en* b*.*

Merk op dat 6.3.1 equivalent is met een andere gebruikelijke formulering: een getal a deelt b als er een $x \in \mathbf{Z}$ bestaat met $ax = b$. We noteren 'a deelt b' als $a|b$. We zien dat ieder getal een deler is van 0, want de triviale ondergroep $0\mathbf{Z}$ is in iedere andere ondergroep $a\mathbf{Z}$ van $\mathbf{Z}$ bevat. Een getal $b \neq 0$ heeft maar eindig veel delers, want voor iedere deler $a|b$ geldt $|a| \leq |b|$.

Een getal $d \geq 0$ met $d\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z}$ is een deler van zowel a als b. Omgekeerd geldt voor iedere gemeenschappelijke deler n van a en b de inclusie $n\mathbf{Z} \supset a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$, dus n deelt d. Behalve in het geval $d = 0 = \gcd(0, 0)$ is d dus inderdaad de *grootste* gemeenschappelijke deler. Analoge opmerkingen verklaren de naam van het kleinste gemene veelvoud.

Uit de definitie van $\gcd(a, b)$ volgt dat er getallen $x, y \in \mathbf{Z}$ bestaan met

$$xa + yb = \gcd(a, b). \tag{6.4}$$

In het bijzonder zijn a en b onderling ondeelbaar dan en slechts dan als de vergelijking $xa + yb = 1$ een oplossing in gehele getallen heeft. We zullen in 6.13 en 6.14 aangeven hoe men, gegeven a en b, de getallen x, y en $\gcd(a, b)$ snel kan berekenen.

Opgave 2. Definieer de getallen $\gcd(a_1, a_2, \ldots, a_n)$ en $\mathrm{kgv}(a_1, a_2, \ldots, a_n)$ voor $n \geq 2$.

▶ Priemgetallen

De *triviale delers* van een getal $a \neq 0$ zijn de delers ± 1 en $\pm a$. Een getal $a > 1$ met alleen triviale delers heet een *priemgetal*. Een getal $a > 1$ dat niet priem is heet *samengesteld*. Per definitie is 1 niet priem, en de verzameling van priemgetallen $\mathcal{P}$ ziet er uit als

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\}.$$

Veel elementaire vragen met betrekking tot $\mathcal{P}$ zijn nog steeds onopgelost[20]. Een positief resultaat is de volgende klassieke stelling van Euclides[21] ($\pm$300 v.C.).

6.5. Stelling. *Er zijn oneindig veel priemgetallen.*

Bewijs. Stel dat $\mathcal{P} = \{p_1, p_2, p_3, \ldots, p_n\}$ eindig is, en zij p de kleinste deler > 1 van $N = p_1p_2p_3 \ldots p_n + 1$. Dan is p een priemgetal, want iedere deler van p is ook een deler van N. Vanwege onze aanname geldt $p = p_i \in \mathcal{P}$ voor zekere i. Nu is $p = p_i$ een deler van N en van $p_1p_2p_3 \ldots p_n$, dus ook van $N - p_1p_2p_3 \ldots p_n = 1$. Tegenspraak. □

Opgave 3. Zijn de getallen $p_1p_2p_3 \ldots p_n + 1$, met $p_1, p_2, \ldots, p_n$ de eerste n priemgetallen, alle priem?

Een priemgetal in $\mathbf{Z}$ is gedefinieerd door een *irreducibiliteitseigenschap*: er zijn geen niet-triviale delers. Veel nuttiger is de volgende *priemeigenschap* van priemgetallen.

6.6. Lemma. *Laat a en b geheel zijn en p priem. Dan geldt: $p|ab \Longrightarrow p|a$ of $p|b$.*

Bewijs. Stel dat p een deler is van ab maar niet van b. Dan is $\text{ggd}(p, b)$ een positieve deler van p die niet gelijk is aan p, dus we hebben $\text{ggd}(p, b) = 1$. Als in 6.4 hebben we $x, y \in \mathbf{Z}$ met $xp + yb = 1$. Schrijf nu $a = (xp + yb)a = axp + yab$, dan deelt p zowel axp als yab, en dus a. □

Opgave 4. Laat a en b onderling ondeelbaar zijn, en c deelbaar door a en b. Bewijs: $ab|c$.

Uit 6.6 volgt met inductie gemakkelijk dat een priemgetal p dat een product $a_1a_2 \ldots a_n$ deelt, ten minste één van de getallen a_i deelt.

▶ Eenduidige priemfactorisatie

De priemgetallen zijn de 'multiplicatieve bouwstenen' van de gehele getallen, als volgt.

6.7. Eenduidige factorisatie. *Ieder positief getal n is uniek te ontbinden als een product*

$$n = \prod_{p \in \mathcal{P}} p^{n_p},$$

van priemgetallen. Hierbij zijn de exponenten n_p natuurlijke getallen die voor slechts eindig veel priemgetallen p verschillend van 0 zijn.

Bewijs. We bewijzen eerst met inductie dat ieder geheel getal $n \geq 1$ een ontbinding in priemgetallen heeft. Voor $n = 1$ kunnen we het lege product nemen. Zij nu $n > 1$ willekeurig en neem aan dat alle getallen kleiner dan n producten van priemen zijn. Als n alleen triviale delers heeft, dan is n priem en zijn we direct klaar. Als n een niet-triviale deler $n_1 > 1$ heeft, dan schrijven we $n = n_1n_2$. Wegens de inductiehypothese hebben n_1 en n_2 een ontbinding, en door deze te combineren krijgen we een ontbinding van n. Dit bewijst de *existentie* van een priemfactorontbinding voor alle n.

We moeten nog laten zien dat ontbindingen eenduidig zijn. Stel hiertoe dat we twee ontbindingen

$$p_1p_2 \ldots p_s = q_1q_2 \ldots q_t$$

van een getal in priemfactoren hebben. We willen bewijzen dat de priemgetallen in beide ontbindingen op volgorde na dezelfde zijn. We voeren het bewijs met inductie naar de lengte s van de eerste ontbinding. Voor $s = 0$ is er niets te bewijzen. Voor $s \geq 1$ is p_1 een deler van $q_1 q_2 \dots q_t$, dus we hebben $p | q_i$ voor zekere i. Uit de primaliteit van q_i volgt $p_1 = q_i$. Als we de factoren p_1 en q_i wegdelen uit bovenstaande gelijkheid krijgen we gelijke ontbindingen met links $s-1$ en rechts $t-1$ priemfactoren. Wegens de inductiehypothese geldt $s - 1 = t - 1$ en zijn de factoren op volgorde na aan elkaar gelijk. Voor de oorspronkelijke ontbindingen gold dit dus ook. Dit bewijst de *uniciteit* van de ontbinding. □

De exponent n_p van p in de factorisatie van n wordt wel de *orde* van n bij p genoemd en met $\mathrm{ord}_p(n)$ aangegeven. De functie $\mathrm{ord}_p : \mathbf{Z}_{>0} \to \mathbf{Z}_{\geq 0}$ voldoet aan de 'homomorfie-achtige' eigenschap $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$ voor $x, y \in \mathbf{Z}_{>0}$.

Opgave 5. Laat zien dat er een uniek homomorfisme $\mathrm{ord}_p : \mathbf{Q}^* \to \mathbf{Z}$ bestaat waarvan de beperking tot $\mathbf{Z}_{>0}$ gelijk is aan de zojuist gedefinieerde functie.

Het vinden van de *priemfactorontbinding* of *factorisatie* in 6.7 is in principe elementair. Een effectieve maar vaak nogal tijdrovende manier om een getal $n > 1$ te ontbinden bestaat uit het domweg proberen ('*trial division*') van $d = 2, 3, 4, \dots$ als delers van n. De kleinste deler $p > 1$ van n is een priemgetal. Heeft men $p < n$, dan schrijft men $n = p \cdot m$ en gaat door met het ontbinden van m. In het geval $p = n$ is n zelf een priemgetal.

Opgave 6. Bewijs dat een getal $n > 1$ een priemgetal is als het geen delers d bezit met $1 < d \leq \sqrt{n}$.

▶ Ringen

Stelling 6.7 is geen groepentheoretische stelling voor $\mathbf{Z}$. Hij heeft betrekking op de *vermenigvuldiging* in $\mathbf{Z}$, en we zagen in §4 al dat $\mathbf{Z}$ geen multiplicatieve groep is omdat niet alle elementen een inverse hebben. Omdat in een multiplicatieve groep alle elementen delers van elkaar zijn is deelbaarheid alleen van belang in multiplicatieve structuren die *geen* groep zijn. Om de combinatie van 'optelstructuur' en 'vermenigvuldigstructuur' op $\mathbf{Z}$ te axiomatiseren verlaten we het te eng geworden kader van de groepentheorie en introduceren het begrip *ring*.

6.8. Definitie. *Een ring is een additief geschreven abelse groep A voorzien van een multiplicatief geschreven bewerking $A \times A \to A$ die aan de volgende drie voorwaarden voldoet.*

(R1) *A bevat een eenheidselement 1 voor de vermenigvuldiging;*

(R2) *Voor elk drietal elementen $a, b, c \in A$ geldt de associatieve eigenschap*

$$a(bc) = (ab)c;$$

(R3) *Voor elk drietal elementen $a, b, c \in A$ gelden de distributieve eigenschappen*

$$a(b + c) = ab + ac \qquad \text{en} \qquad (a + b)c = ac + bc.$$

Geldt bovendien $ab = ba$ voor alle $a, b \in A$, dan heet A een commutatieve ring.

De onderliggende optelgroep van een ring A wordt per definitie abels genomen. Dit is geen beperking, want deze eigenschap volgt uit de overige ringaxioma's (opgave 50). De voorwaarden (R1) en (R2) zijn gelijk aan de voorwaarden (G1) en (G2) in 2.1. We eisen echter niet dat ieder element van A een multiplicatieve inverse heeft, en de multiplicatieve structuur van een ring is daarom veel minder 'mooi' dan we voor groepen gewend zijn. De verzameling van *eenheden*

$$A^* = \{a \in A : \text{ er bestaat } a^\dagger \in A \text{ met } aa^\dagger = a^\dagger a = 1\}$$

in A voldoet (opgave 7) wel aan de groepsaxioma's onder de vermenigvuldiging en heet de *eenhedengroep* van A. In het geval van $\mathbf{Z}$ is de eenhedengroep $\mathbf{Z}^* = \{\pm 1\}$ beduidend kleiner dan $\mathbf{Z}$.

Opgave 7. Laat zien dat het product van twee eenheden in een ring A een eenheid is.

Commutatieve ringen A waarvoor $A^* = A \setminus \{0\}$ geldt heten *lichamen*. In een lichaam is ieder element verschillend van 0 een eenheid. De bekendste voorbeelden van lichamen zijn $\mathbf{Q}$, $\mathbf{R}$ en $\mathbf{C}$.

De keuze van de algemene ringaxioma's is deels ingegeven door het bestaan van de ring van gehele getallen $\mathbf{Z}$; deze ring is het 'standaardvoorbeeld' van een commutatieve ring. Andere bekende voorbeelden van commutatieve ringen zijn de ringen $\mathbf{R}[X]$ en $\mathbf{C}[X]$ van polynomen met coëfficiënten in $\mathbf{R}$ of $\mathbf{C}$. Deze polynomen worden op de uit de analyse bekende wijze opgeteld en vermenigvuldigd, en het is welbekend dat hiervoor de ringaxioma's gelden. We komen hier nog uitgebreid op terug in het college algebra 2.

Opgave 8. Definieer de polynoomring $A[X]$ over een willekeurige commutatieve ring A, en ga na dat $A[X]$ een commutatieve ring is.

▶ De ring $\mathbf{Z}/n\mathbf{Z}$

We zagen in §1 al dat we modulo n ook kunnen vermenigvuldigen, en deze ontdekking betekent in formele termen dat de groep $\mathbf{Z}/n\mathbf{Z}$ van restklassen modulo n net als $\mathbf{Z}$ een ring 'is'.

6.9. Stelling. *Zij n geheel en $\pi : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ het natuurlijke groepshomomorfisme. Dan maakt de vermenigvuldiging $\pi(x)\pi(y) = \pi(xy)$ de groep $\mathbf{Z}/n\mathbf{Z}$ tot een ring.*

Bewijs. We moeten laten zien dat de natuurlijke vermenigvuldiging op $\mathbf{Z}/n\mathbf{Z}$ welgedefinieerd is, alle ringeigenschappen volgen dan uit die voor $\mathbf{Z}$. Geldt $x \equiv x' \bmod n$ en $y \equiv y' \bmod n$, dan hebben we

$$xy - x'y' = x(y - y') + (x - x')y'. \tag{6.10}$$

Het rechterlid is een element van $n\mathbf{Z}$, immers $x - x'$ en $y - y'$ zijn elementen van $n\mathbf{Z}$. We vinden $xy \equiv x'y' \bmod n$, zoals gewenst. □

Een afbeelding $f : A \to A'$ tussen ringen heet een *ringhomomorfisme* als het een homomorfisme van de additieve groepen is dat bovendien voldoet aan

(1) $f(1_A) = 1_{A'}$;
(2) $f(xy) = f(x)f(y)$ voor $x, y \in A$.

Is f bovendien bijectief, dan heet f een *ringisomorfisme*.

Opgave 9. Laat aan de hand van een voorbeeld zien dat, anders dan voor groepen, eis (1) hier geen gevolg is van eis (2).

Stelling 6.9 is het 'ringenequivalent' voor $G = \mathbf{Z}$ van 4.13. Hij zegt dat met het gegeven product op $\mathbf{Z}/n\mathbf{Z}$ de quotiëntafbeelding $\pi : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ een ringhomomorfisme is.

De *restklassenring* $\mathbf{Z}/n\mathbf{Z}$ is voor $n \neq 0$ een eindige ring met $|n|$ elementen. Zijn eenhedengroep $(\mathbf{Z}/n\mathbf{Z})^*$ is de groep van *inverteerbare restklassen modulo* n. Een restklasse $\bar{a} \in \mathbf{Z}/n\mathbf{Z}$ is inverteerbaar als er een element $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$ bestaat met $\bar{a}\bar{x} = \bar{1}$, en dit betekent dat de vergelijking $ax = 1 + ny$ een oplossing in gehele getallen toelaat. We zagen na 6.4 dat dit mogelijk is precies wanneer a en n copriem zijn, en we vinden

$$(\mathbf{Z}/n\mathbf{Z})^* = \{\bar{a} \in \mathbf{Z}/n\mathbf{Z} : \mathrm{ggd}(a, n) = 1\}. \tag{6.11}$$

De orde van de groep $(\mathbf{Z}/n\mathbf{Z})^*$ wordt aangegeven met $\varphi(n)$, en de functie $\varphi : \mathbf{Z}_{\geq 1} \to \mathbf{Z}$ heet de *φ-functie van Euler*.

Opgave 10. Bereken $\varphi(n)$ voor $n \leq 20$.

Als *alle* restklassen verschillend van $\bar{0}$ eenheden zijn in $\mathbf{Z}/n\mathbf{Z}$ is n copriem met alle getallen 1, 2, 3, $\ldots$, $n-1$, en dit betekent dat n priem is.

6.12. Stelling. *De ring $\mathbf{Z}/n\mathbf{Z}$ is een lichaam dan en slechts dan als n priem is.* □

De eindige lichamen $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ voor de priemgetallen p lijken in een aantal opzichten op bekendere lichamen als $\mathbf{R}$ en $\mathbf{C}$. Veel stellingen uit de lineaire algebra over matrices, determinanten en dimensies gelden bijvoorbeeld voor willekeurige grondlichamen, zodat men hierin voor $\mathbf{R}$ of $\mathbf{C}$ ook $\mathbf{F}_p$ kan nemen. De lineaire algebra over $\mathbf{F}_p$ mist echter het natuurlijke afstandsbegrip, dat afhangt van de positiviteit van een inproduct $\langle x, x\rangle$. In $\mathbf{F}_p$ zijn er helemaal geen positieve en negatieve getallen, en men kan ook niet praten over 'grote' en 'kleine' elementen in de zin van een absolute waarde. Hier staat tegenover dat alle eindig-dimensionale vectorruimtes over $\mathbf{F}_p$ maar eindig veel elementen hebben, zodat men anders dan voor $\mathbf{R}$ of $\mathbf{C}$ vaak *telargumenten* kan gebruiken. Men spreekt in dit kader wel van *eindige meetkundes.*

Er zijn over $\mathbf{F}_p$ maar eindig veel matrices van gegeven dimensie, en dit betekent dat de groepen $\mathrm{GL}_n(\mathbf{F}_p)$ van inverteerbare $n \times n$-matrices met coëfficiënten in $\mathbf{F}_p$ allemaal eindig zijn. Dergelijke *eindige groepen van Lie-type* komen veelvuldig voor.

Opgave 11. Laat zien dat $\mathrm{GL}_2(\mathbf{F}_2)$ isomorf is met S_3.

De ringen $\mathbf{Z}/n\mathbf{Z}$ voor samengestelde getallen n gedragen zich in veel opzichten anders dan de lichamen $\mathbf{R}$ en $\mathbf{C}$. Een identiteit als $\bar{2}\cdot\bar{2} = \bar{0} \in \mathbf{Z}/4\mathbf{Z}$ laat zien dat een product van elementen verschillend van nul gelijk aan nul kan zijn, en dat een lineaire vergelijking

als $\bar{2} \cdot \bar{x} = \bar{0} \in \mathbf{Z}/4\mathbf{Z}$ twee verschillende oplossingen $\bar{x} = \bar{2}$ en $\bar{x} = \bar{0}$ kan hebben. In feite hebben we zoiets al in §1 gezien: de kwadratische vergelijking $\bar{x}^2 = \bar{1}$ heeft *vier* oplossingen $\bar{1}$, $\bar{3}$, $\bar{5}$ en $\bar{7}$ in $\mathbf{Z}/8\mathbf{Z}$. Dit laat zien dat 'bekende feiten' over aantallen nulpunten van polynomen niet altijd waar zijn als we met coëfficiënten uit willekeurige commutatieve ringen rekenen.

▶ Rekenen modulo n

Bij het rekenen in de groepen $(\mathbf{Z}/n\mathbf{Z})^*$ is het handig om over een manier te beschikken om inversen expliciet uit te rekenen. Dit wil zeggen dat we een methode moeten vinden om ggd's te berekenen en vergelijking 6.4 expliciet op te lossen.

6.13. Euclidische algoritme. *Definieer voor gehele getallen a en b de rij van niet-negatieve gehele getallen $r_0, r_1, r_2, \ldots$ door $r_0 = |a|$, $r_1 = |b|$ en*

$$r_{i+1} = (\textit{rest van } r_{i-1} \textit{ bij deling door } r_i) \quad \textit{als } r_i \neq 0.$$

Dan bestaat er een index $k > 0$ met $r_k = 0$, en er geldt $\gcd(a, b) = r_{k-1}$.

Bewijs. Omdat de getallen in de rij $r_1, r_2, \ldots$ steeds kleiner worden, maar nooit negatief, moet $r_k = 0$ optreden voor zekere $k > 0$. Dan geldt $r_{k-1} = \gcd(r_{k-1}, 0) = \gcd(r_{k-1}, r_k)$, en omdat duidelijk $\gcd(a, b) = \gcd(r_0, r_1)$ geldt is het nu voldoende de gelijkheden $\gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{k-1}, r_k)$ te bewijzen.

Genoemde gelijkheden zeggen dat, voor a en $b \neq 0$ natuurlijke getallen en r de rest van a bij deling door b, steeds $\gcd(a, b) = \gcd(b, r)$ geldt. Dit is equivalent met de gelijkheid

$$a\mathbf{Z} + b\mathbf{Z} = b\mathbf{Z} + r\mathbf{Z}$$

van ondergroepen van $\mathbf{Z}$. Voor het bewijs hiervan merkt men op dat $a = qb + r$ in het rechterlid bevat is en $r = a - qb$ in het linkerlid. □

De *uitgebreide Euclidische algoritme* is een berekening als in 6.13 die niet alleen de ggd van a en b geeft, maar ook een oplossing van de vergelijking 6.4. We kiezen hiervoor $x_0 = \pm 1$ en $y_0 = 0$ alsmede $x_1 = 0$ en $y_1 = \pm 1$ zodanig dat de vergelijkingen

$$x_0 a + y_0 b = r_0 \ (= |a|)$$
$$x_1 a + y_1 b = r_1 \ (= |b|)$$

gelden. De deling met rest in 6.13 geeft ons getallen q_i zodat $r_{i-1} = q_i r_i + r_{i+1}$ geldt. Dit betekent dat we uit bovenstaande twee vergelijkingen een rij vergelijkingen

$$x_i a + y_i b = r_i \qquad \text{voor } i = 0, 1, 2, \ldots$$

kunnen maken waarin de $(i+1)$-de vergelijking ontstaat door de i-de q_i maal van de $(i-1)$-de af te trekken. Anders gezegd: de getallen x_i en y_i voldoen net als r_i aan de betrekkingen $x_{i-1} = q_i x_i + x_{i+1}$ en $y_{i-1} = q_i y_i + y_{i+1}$. Is k de index in 6.13 waarvoor $r_k = 0$ optreedt, dan geeft $x_{k-1} a + y_{k-1} b = r_{k-1} = \gcd(a, b)$ een oplossing van 6.4.

Opgave 12. Bewijs: als a en b positief zijn geldt $x_i y_{i+1} - x_{i+1} y_i = (-1)^i$ voor $i = 0, 1, \ldots, k-1$.

Het berekenen van ggd's met de Euclidische algoritme is meestal veel efficiënter dan de in opgave 20 voorkomende berekening via de priemfactorisatie. De onderliggende gedachte blijkt ook in andere situaties toepasbaar, en varianten van de algoritme komen dan ook in talloze computerimplementaties voor.

6.14. Voorbeeld. Voor $b = 12345$ en $a = 56789$ vinden we achtereenvolgens:

$$\begin{aligned}
1 \cdot 56789 - \quad 0 \cdot 12345 &= 56789 \\
-0 \cdot 56789 + \quad 1 \cdot 12345 &= 12345 \qquad (q_1 = 4) \\
1 \cdot 56789 - \quad 4 \cdot 12345 &= 7409 \qquad (q_2 = 1) \\
-1 \cdot 56789 + \quad 5 \cdot 12345 &= 4936 \qquad (q_3 = 1) \\
2 \cdot 56789 - \quad 9 \cdot 12345 &= 2473 \qquad (q_4 = 1) \\
-3 \cdot 56789 + \quad 14 \cdot 12345 &= 2463 \qquad (q_5 = 1) \\
5 \cdot 56789 - \quad 23 \cdot 12345 &= 10 \qquad (q_6 = 246) \\
-1233 \cdot 56789 + \quad 5672 \cdot 12345 &= 3 \qquad (q_7 = 3) \\
3704 \cdot 56789 - 17039 \cdot 12345 &= 1.
\end{aligned}$$

Deze berekening laat zien dat 12345 en 56789 copriem zijn, en hoe we hun ggd als 'lineaire combinatie' van 12345 en 56789 kunnen schrijven. De tekenkeuze '-0' in het begin benadrukt het alternerende karakter van de tekens van x_i en y_i.

Willen we alleen de ggd bepalen, dan is het voldoende om in 6.14 alleen de berekening rechts van de gelijkheidstekens uit te voeren. De gegeven berekening heet wel een 'uitgebreide ggd-berekening'. Is de ggd van a en b gelijk aan 1, dan geven de 'slotwaarden' x_{k-1} en y_{k-1} de inverse van a modulo b en van b modulo a. (Hebben we slechts één van beide inversen nodig, dan kunnen we in de hele berekening de 'overbodige' kolom achterwege laten.) In ons voorbeeld krijgen we

$$\begin{aligned}
\overline{56789}^{-1} &= \overline{3704} \in (\mathbf{Z}/12345\mathbf{Z})^* \\
\overline{12345}^{-1} &= \overline{-17039} = \overline{39750} \in (\mathbf{Z}/56789\mathbf{Z})^*.
\end{aligned}$$

Merk op dat we met onze berekening wel $\mathrm{ggd}(12345, 56789) = 1$ vinden, maar *geen* informatie krijgen over de priemfactoren van de beide getallen.

Opgave 13. Bepaal de ggd van $a =$ je telefoonnummer (zonder netnummer) en $b =$ je geboortedatum (schrijf 920301 voor 1 maart 1992) en vind $x, y \in \mathbf{Z}$ waarvoor $xa + yb$ gelijk is aan deze ggd.

Om de structuur van de ring $\mathbf{Z}/n\mathbf{Z}$ en zijn eenhedengroep $(\mathbf{Z}/n\mathbf{Z})^*$ te begrijpen is er een klassieke stelling om de ring $\mathbf{Z}/n\mathbf{Z}$ in een product van ringen te 'ontbinden'. Een *product* $A_1 \times A_2$ van ringen A_1 en A_2 wordt net als voor groepen (opgave 4.17) op de voor de hand liggende manier gedefinieerd; op de productverzameling $A_1 \times A_2$ definieert men optelling en vermenigvuldiging coördinaatsgewijs als

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \qquad \text{en} \qquad (x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2).$$

Men gaat gemakkelijk na dat dit aanleiding geeft tot een ringstructuur op $A_1 \times A_2$. Op soortgelijke wijze kan men producten van meer dan 2 ringen definiëren.

6.15. Chinese reststelling. *Laat m en n onderling ondeelbare gehele getallen zijn. Dan is de natuurlijke afbeelding*

$$\begin{array}{rccc} \psi: & \mathbf{Z}/mn\mathbf{Z} & \xrightarrow{\sim} & \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \\ & (x \bmod mn) & \longmapsto & (x \bmod m, x \bmod n) \end{array}$$

een ringisomorfisme. De afbeelding ψ induceert een isomorfisme van eenhedengroepen

$$\psi_* : (\mathbf{Z}/mn\mathbf{Z})^* \xrightarrow{\sim} (\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*,$$

en de Euler-φ-functie voldoet aan $\varphi(mn) = \varphi(m)\varphi(n)$.

Bewijs. We merken eerst op dat ψ een welgedefinieerd ringhomomorfisme is: voldoen $x, x' \in \mathbf{Z}$ aan $x \equiv x' \bmod mn$, dan geldt $(x \bmod m, x \bmod n) = (x' \bmod m, x' \bmod n)$.

Omdat m en n copriem zijn, bestaan er $r, s \in \mathbf{Z}$ met $rm + sn = 1$. De restklassen van $rm = 1 - sn$ en $sn = 1 - rm$ worden door ψ op respectievelijk $(\bar{0}, \bar{1})$ en $(\bar{1}, \bar{0})$ afgebeeld. Deze elementen brengen de additieve groep $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ voort, dus ψ is surjectief. Omdat $\mathbf{Z}/mn\mathbf{Z}$ en $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ beide mn elementen hebben, is ψ ook injectief. We concluderen dat ψ een ringisomorfisme is.

Onder ψ wordt $(\mathbf{Z}/mn\mathbf{Z})^*$ isomorf op de eenhedengroep van $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ afgebeeld, en deze is gelijk aan $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$. Vergelijken van de ordes geeft de relatie $\varphi(mn) = \varphi(m)\varphi(n)$. □

Het bewijs van 6.15 laat zien hoe men uitgaande van een oplossing van de vergelijking $rm + sn = 1$ een element $x \in \mathbf{Z}$ kan vinden met $\psi(x) = (a \bmod m, b \bmod n)$. Immers, wegens $\psi(sn) = (\bar{1}, \bar{0})$ en $\psi(rm) = (\bar{0}, \bar{1})$ geldt $\psi(asn + brm) = (\bar{a}, \bar{0}) + (\bar{0}, \bar{b}) = (\bar{a}, \bar{b})$.

Opgave 14. Bepaal een getal $x \in \mathbf{Z}$ dat voldoet aan de congruenties $x \equiv 12 \bmod 34$ en $x \equiv 45 \bmod 67$.

Door 6.15 herhaald toe te passen kunnen we uit de priemfactorisatie van n een 'ontbinding' van de ring $\mathbf{Z}/n\mathbf{Z}$ in ringen van de vorm $\mathbf{Z}/p^k\mathbf{Z}$ met p een priemgetal afleiden.

6.16. Gevolg. *Voor ieder positief geheel getal n is er een natuurlijk ringisomorfisme*

$$\mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} \textstyle\prod_{p|n} (\mathbf{Z}/p^{\mathrm{ord}_p(n)}\mathbf{Z}).$$

Voor de Euler-φ-functie geldt dienovereenkomstig

$$\varphi(n) = \prod_{p|n} \varphi(p^{\mathrm{ord}_p(n)}) = \prod_{p|n} (p-1)p^{\mathrm{ord}_p(n)-1} = n \cdot \prod_{p|n} (1 - \frac{1}{p}).$$

Bewijs. De eerste uitspraak volgt door herhaald toepassen van 6.15. Door vergelijking van de ordes van de eenhedengroepen vinden we $\varphi(n) = \prod_{p|n} \varphi(p^{\mathrm{ord}_p(n)})$. De inverteerbare restklassen $\bar{a} \in \mathbf{Z}/p^k\mathbf{Z}$ voor $k \geq 1$ zijn wegens 6.11 de restklassen met $p \nmid a$. Er zijn $\frac{1}{p} \cdot p^k$ restklassen $\bar{a}$ met $p|a$, en dit geeft $\varphi(p^k) = (1 - \frac{1}{p}) \cdot p^k = (p-1)p^{k-1}$. □

▶ Stellingen van Euler en Fermat

Uit de stelling van Lagrange hebben we in 4.8 afgeleid dat de orde van een groepselement in een eindige groep altijd de groepsorde deelt. Passen we dit toe op de groepen $(\mathbf{Z}/n\mathbf{Z})^*$, dan krijgen we een rond 1750 door Euler ontdekte stelling.

6.17. Stelling. *Voor a en $n \geq 1$ onderling ondeelbaar geldt $a^{\varphi(n)} \equiv 1 \bmod n$.* □

Het geval dat n een priemgetal is was al bestudeerd door Fermat (1601–1665), die rond 1640 het volgende speciale geval van 6.17 formuleerde.

6.18. Kleine stelling van Fermat. *Voor p een priemgetal en a een geheel getal geldt*

$$a^p \equiv a \bmod p.$$

Bewijs. Voor $a \equiv 0 \bmod p$ is de uitspraak duidelijk. Voor $a \not\equiv 0 \bmod p$ is a onderling ondeelbaar met p en geldt $\bar{a}^{p-1} = \bar{1} \in (\mathbf{Z}/p\mathbf{Z})^*$ wegens 6.17. Vermenigvuldigen we links en rechts met $\bar{a}$, dan volgt het gewenste resultaat. □

De naam van stelling 6.18 is bedoeld om het onderscheid aan te geven met de beroemde 'grote' of 'laatste' stelling van Fermat, die zegt dat de vergelijking $x^n + y^n = z^n$ voor $n > 2$ geen gehele oplossingen heeft buiten de triviale oplossingen met $xyz = 0$. Deze laatste stelling werd in 1995 bewezen door de Britse wiskundige Andrew Wiles[22]. Het bewijs geldt als een hoogtepunt van de twintigste-eeuwse getaltheorie.

De ringen $\mathbf{Z}/n\mathbf{Z}$ kunnen vaak gebruikt worden om te laten zien dat vergelijkingen in $\mathbf{Z}$ geen oplossingen hebben. In (1.2) zagen we dit voor de vergelijking $3x^2+2 = y^2$, en in opgave 1.25 voor de vergelijking $55x^3+3 = y^3$. Voor gegeven n is de oplosbaarheid in $\mathbf{Z}/n\mathbf{Z}$ in eindig veel stappen te bepalen, en als men de ringstructuur van $\mathbf{Z}/n\mathbf{Z}$ efficiënt gebruikt is dit berekening vaak erg eenvoudig. In de meeste gevallen kiest men met het oog op 6.16 voor n een priemgetal of een macht daarvan. Een moeilijke vraag hier is wat we kunnen besluiten uit het feit dat een vergelijking modulo alle priemmachten oplossingen heeft. In sommige gevallen kan men uit het bestaan van al deze zogenaamde 'locale oplossingen' besluiten dat er een 'globale oplossing' in $\mathbf{Z}$ bestaat. De Fransman Legendre (1752–1833) vond bijvoorbeeld al in 1785 dat voor ieder drietal paarsgewijs onderling ondeelbare positieve gehele getallen a, b, c de kwadratische vergelijking

$$ax^2 + by^2 = cz^2$$

een geheeltallige oplossing $(x, y, z) \neq 0$ heeft dan en slechts dan als dit modulo alle priemgetallen p het geval is. Voor hogeregraads-vergelijkingen is de situatie beduidend gecompliceerder, en pas in de 20e eeuw is hier substantiële vooruitgang geboekt. De obstructies die hier optreden tegen het zogenaamde *locaal-globaal-principe* hebben aanleiding gegeven tot diverse nog onopgeloste problemen in de getaltheorie[23]

OPGAVEN.

15. Laat a en b geheel zijn met $d = \gcd(a, b) \neq 0$. Bewijs: a/d en b/d zijn copriem.

16. Laat zien dat het 'quotiënt' q en de rest r in 6.1 eenduidig bepaald zijn door a en b.

17. Zij $b > 1$ een geheel getal. Bewijs dat ieder positief geheel getal a een eenduidige representatie
$$a = c_t b^t + c_{t-1} b^{t-1} + \ldots + c_1 b + c_0$$
heeft met t een niet-negatief getal dat van a afhangt, 'cijfers' $c_i \in \{0, 1, 2, \ldots, b-1\}$ en $c_t \neq 0$. [Dit heet de representatie in het *b-tallig stelsel*.]

18. Bewijs dat ieder geheel getal $a \neq 0$ een eenduidige representatie
$$a = 3^t c_t + 3^{t-1} c_{t-1} + \ldots + 3c_1 + c_0$$
heeft met t een niet-negatief getal dat van a afhangt, 'cijfers' $c_i \in \{-1, 0, 1\}$ en $c_t \neq 0$. Laat hetzelfde zien voor de representaties
$$a = 2^t c_t + 2^{t-1} c_{t-1} + \ldots + 2c_1 + c_0$$
met 'cijfers' $c_i \in \{-1, 0, 1\}$ die voldoen aan $c_t \neq 0$ en $c_i c_{i+1} = 0$ voor $i = 0, 1, \ldots, t-1$.

19. De rij 1, 1, 2, 3, 5, 8, 13, ... van *Fibonacci-getallen* is recursief gedefinieerd door $x_1 = x_2 = 1$ en $x_{n+2} = x_{n+1} + x_n$ voor $n \geq 1$. Bewijs dat twee opvolgende Fibonacci-getallen copriem zijn. Geldt ook altijd $\gcd(x_n, x_{n+2}) = 1$?

20. Laat zien dat de ggd en kgv van de getallen $a = \prod_{p \in \mathcal{P}} p^{m_p}$ en $b = \prod_{p \in \mathcal{P}} p^{n_p}$ gelijk zijn aan respectievelijk
$$\prod_{p \in \mathcal{P}} p^{\min(m_p, n_p)} \qquad \text{en} \qquad \prod_{p \in \mathcal{P}} p^{\max(m_p, n_p)}.$$
Concludeer: voor a en b geheel geldt $|ab| = \gcd(a, b) \cdot \mathrm{kgv}(a, b)$.

21. Kan men $\mathrm{kgv}(a, b)$ berekenen zonder a en b expliciet in factoren te ontbinden?

22. Bereken de ggd en de kgv van $a = 10000010$ en $b = 10000020$.

23. Laat zien dat ieder rationaal getal $q \in \mathbf{Q}^*$ uniek te schrijven is als $\varepsilon \prod_{p \in \mathcal{P}} p^{n_p}$ met $\varepsilon \in \{\pm 1\}$ en getallen $n_p \in \mathbf{Z}$ die voor slechts eindig veel p verschillend zijn van 0.

24. Laat zien dat er oneindig veel priemgetallen $p \equiv 3 \bmod 4$ bestaan.
[Hint: imiteer het bewijs van Euclides van 6.5.]

25. Zij n een geheel getal van de vorm $n = x^2 + 1$ met $x \in \mathbf{Z}$, en p een oneven priemdeler van n. Bewijs: $p \equiv 1 \bmod 4$.

26. Laat zien dat er oneindig veel priemgetallen $p \equiv 1 \bmod 4$ bestaan.

27. Laat zien dat er oneindig veel priemgetallen $p \equiv 2 \bmod 3$ bestaan, en ook dat er oneindig veel priemgetallen $p \equiv 1 \bmod 3$ bestaan[24].

28. Laat $a > 1$ en $k > 1$ getallen zijn waarvoor $a^k - 1$ priem is. Bewijs: $a = 2$ en k is priem. Zijn alle getallen van de vorm $2^p - 1$ met p een priemgetal priem?
[Priemgetallen van de vorm $2^p - 1$ heten *Mersenne-priemen*[25].]

29. Laat a en $b \neq 0$ natuurlijke getallen zijn, en r de rest van a bij deling door b. Bewijs dat voor ieder geheel getal $t > 1$ de rest van $t^a - 1$ bij deling door $t^b - 1$ gelijk is aan $t^r - 1$. Concludeer: $\text{ggd}(t^a - 1, t^b - 1) = t^{\text{ggd}(a,b)} - 1$.

30. Laat $k \geq 1$ een geheel getal zijn waarvoor $2^k + 1$ priem is. Bewijs: $k = 2^n$ voor zekere n. Zijn alle getallen van de vorm $2^{2^n} + 1$ priem?
[Het getal $F_n = 2^{2^n} + 1$ wordt het n-de *Fermat-getal* genoemd[26].]

31. Zij n positief en p een priemdeler van het getal $F_n = 2^{2^n} + 1$. Bewijs dat $\bar{2} \in (\mathbf{Z}/F_n\mathbf{Z})^*$ een element van orde 2^{n+1} is. Leid hieruit af: $p \equiv 1 \bmod 2^{n+1}$.

32. Neem $n > 1$ en p en F_n als in de vorige opgave, en definieer $u = 2^{2^{n-2}} \bmod F_n$. Bewijs dat u orde 8 heeft in $(\mathbf{Z}/F_n\mathbf{Z})^*$, en $u - u^3$ orde 2^{n+2}. Leid hieruit af: $p \equiv 1 \bmod 2^{n+2}$.
[Voor $n = 5$ volgt $p \equiv 1 \bmod 128$. De twee kleinste waarden zijn $p = 257$ en $p = 641$.]

33. Bepaal voor alle $n \geq 1$ de orde van $F_{n-1} \bmod F_n$ in $(\mathbf{Z}/F_n\mathbf{Z})^*$.

34. Zij p een priemgetal en q een priemdeler van het Mersennegetal $M_p = 2^p - 1$. Bewijs: $q \equiv 1 \bmod p$.
[Voorbeeld: $M_{11} = 2047 = 23 \cdot 89$ heeft alleen priemdelers 1 mod 11.]

35. Bewijs dat voor ieder geheel getal a de congruentie $a^{13} \equiv a \bmod 2730$ geldt.

36. Laat zien dat voor ieder element $x \in (\mathbf{Z}/7161\mathbf{Z})^*$ de orde van x een deler is van 30. Bestaat er een element $x \in (\mathbf{Z}/7161\mathbf{Z})^*$ van orde 30?

37. Bewijs: $\varphi(5186) = \varphi(5187) = \varphi(5188)$. Geldt $\lim_{n\to\infty} \varphi(n) = \infty$?

38. Bepaal alle $n > 0$ met $\varphi(n) = 8$. Idem voor $\varphi(n) = 14$.

39. Laat $m, n > 0$ voldoen aan $\frac{\varphi(m)}{m} = \frac{\varphi(n)}{n}$. Bewijs dat m en n dezelfde priemdelers hebben.

40. Bepaal alle $n > 0$ waarvoor $\frac{n}{\varphi(n)}$ geheel is.

41. Bepaal een geheel getal x dat voldoet aan de congruenties

$$x \equiv 1 \bmod 7$$
$$x \equiv 5 \bmod 11$$
$$x \equiv 1 \bmod 13.$$

In hoeverre is het gevonden antwoord uniek bepaald?

42. Zij G cyclisch van orde n. Laat zien dat het aantal elementen in G dat de groep voortbrengt gelijk is aan $\varphi(n)$. Leid hieruit af: $\text{Aut}(G) \cong (\mathbf{Z}/n\mathbf{Z})^*$.

43. Laat zien dat een cyclische groep van orde n voor iedere deler $d|n$ precies $\varphi(d)$ elementen van orde d bevat. Bewijs hiermee de *formule van Gauss*: $\sum_{d|n} \varphi(d) = n$.

44. Bepaal voor welke priemgetallen $p < 20$ de groep $(\mathbf{Z}/p\mathbf{Z})^*$ cyclisch is.

45. Zij p een priemgetal. Bewijs dat de binomiaalcoëfficiënten $\binom{p}{i}$ voor $1 \leq i \leq p-1$ deelbaar zijn door p, en leid hieruit voor $x, y \in \mathbf{Z}$ de congruentie $(x + y)^p \equiv x^p + y^p \bmod p$ af. Neem nu $y = 1$, en bewijs de congruentie $x^p \equiv x \bmod p$ uit 6.18 door inductie naar x toe te passen.

46. Bepaal het kleinste samengestelde getal n waarvoor de congruentie $2^n \equiv 2 \bmod n$ geldt. [Wie kan programmeren is snel klaar...]

47. Laat zien dat $\mathrm{GL}_n(\mathbf{F}_p)$ een groep van orde $(p^n-1)(p^n-p)(p^n-p^2)\dots(p^n-p^{n-1})$ is.

48. (Sterretjesloze opgave 2.21.) Laat zien dat de ondergroep $G \subset \mathrm{GL}_3(\mathbf{F}_3)$ gegeven door

$$G = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in \mathbf{F}_3\}$$

een niet-abelse groep van orde 27 is, en dat $x^3 = \mathrm{id}$ geldt voor alle $x \in G$.

49. Laat m en n positieve getallen zijn met $d = \mathrm{ggd}(m,n)$ en $k = \mathrm{kgv}(m,n)$. Bewijs dat de ringen $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ en $\mathbf{Z}/d\mathbf{Z} \times \mathbf{Z}/k\mathbf{Z}$ isomorf zijn.

50. Laat zien dat het abels zijn van de optelgroep van een ring R een gevolg is van de ringaxioma's (R1)–(R3).
[Hint: kijk naar $(1+1)(a+b)$.]

51. Zij A een ring en $H \subset A$ een ondergroep van de optelgroep van A. Laat zien dat A/H tot een ring en de quotiëntafbeelding $\pi : A \to A/H$ tot een ringhomomorfisme gemaakt kunnen worden als H voldoet aan de eigenschap

$(*)$ voor $a \in A$ en $h \in H$ geldt $ah \in H$ en $ha \in H$.

[Hint: kijk naar 6.10. De ondergroepen in kwestie heten *idealen* van A.]

52. Formuleer en bewijs het analogon van de isomorfiestelling 4.9 voor ringen.

53. Zij $A = \mathbf{R}[X]$ de ring van polynomen met coëfficiënten in $\mathbf{R}$. Bewijs: $A^* = \mathbf{R}^*$.

54. Zij $A = (\mathbf{Z}/4\mathbf{Z})[X]$ de ring van polynomen met coëfficiënten in $\mathbf{Z}/4\mathbf{Z}$. Bewijs: voor alle $f \in A$ geldt $1 + 2f \in A^*$. Concludeer dat A^* een oneindige groep is, en dus niet gelijk is aan $(\mathbf{Z}/4\mathbf{Z})^*$.

55. Laat zien dat voor elementen x en y in een lichaam geldt: $xy = 0 \Rightarrow x = 0$ of $y = 0$.

*56. Zij $A = K[X]$ de polynoomring over een lichaam K. Laat $f, g \in A$ polynomen zijn met $g \neq 0$. Bewijs dat er polynomen $q, r \in A$ bestaan met

$$f = qg + r \qquad \text{en} \qquad r = 0 \quad \text{of} \quad \mathrm{graad}(r) < \mathrm{graad}(g).$$

Leid hieruit af dat er voor ieder tweetal polynomen $a, b \in A$ een polynoom $d \in A$ bestaat zo dat $aA + bA = \{ax + by : x, y \in A\}$ gelijk is aan $dA = \{dx : x \in A\}$.

*57. Zij K een lichaam. Een niet-constant polynoom $f \in A = K[X]$ heet *irreducibel* als het niet als een product van twee niet-constante polynomen geschreven kan worden. Bewijs dat een irreducibel polynoom $p \in A$ de *priemeigenschap* heeft: $p|ab \Rightarrow p|a$ of $p|b$. Hier is deelbaarheid van polynomen op de gebruikelijke manier gedefinieerd.

*58. Zij K een lichaam. Bewijs dat ieder niet-constant polynoom $f \in K[X]$ geschreven kan worden als een product van irreducibele polynomen, en dat dit product op volgorde van de factoren en vermenigvuldiging met constanten na uniek is.

59. Laat $n \in \mathbf{Z}$ een kwadraat zijn, en stel dat de vier eindcijfers van n in decimale notatie gelijk zijn. Bewijs dat n op vier nullen eindigt. Geldt hetzelfde met 'vier' beide malen door 'drie' vervangen?

60. Laat zien voor iedere $m \in \mathbf{Z}_{>0}$ de vergelijking $\varphi(n) = m!$ een oplossing $n \in \mathbf{Z}_{>0}$ heeft.

7 Factorisatie en cryptografie.

In deze paragraaf, die een iets ander karakter draagt dan de andere paragrafen in deze syllabus, geven we een aantal toepassingen van de in 6.17 en 6.18 gegeven stellingen van Euler en Fermat. Deze toepassingen maken gebruik van het bestaan van rekenapparatuur om snel elementaire operaties op grote getallen te verrichten. Sommige van de opgaven veronderstellen dat de lezer de beschikking heeft over een enigszins geavanceerd rekenprogramma, zoals Maple, Mathematica, Magma of SAGE, om routinematig met grote gehele getallen of modulo een getal n te kunnen rekenen.

▶ Primaliteit van grote getallen

We beginnen met een toepassing van de kleine stelling van Fermat op het herkennen van grote priemgetallen. Deze vaardigheid zal later goed van pas komen.

Stelling 6.18 impliceert dat als een getal n priem is, voor alle positieve getallen $a < n$ de congruentie $a^{n-1} \equiv 1 \bmod n$ geldt. Deze congruentie is 'snel' te testen *zonder* dat men eerst het vaak onopschrijfbaar grote getal a^{n-1} uitrekent. Men kan namelijk de exponent $n-1$ binair schrijven als een som $n-1 = \sum_{k=0}^{N} c_k 2^k$ met cijfers $c_k \in \{0,1\}$. De machten $\bar{a}^{2^k}$ kan men voor $k = 0, 1, \ldots, N$ uitrekenen door *herhaald kwadrateren* van $\bar{a}$. Omdat na iedere kwadratering het antwoord modulo n gereduceerd mag worden treden hierbij geen getallen op die groter zijn dan n^2. Uit de binaire representatie van $n-1$ ziet men welke machten $\bar{a}^{2^k}$ vermenigvuldigd moeten worden om $\bar{a}^{n-1}$ te krijgen. Dit zijn niet meer dan $N+1$ machten, en na elke vermenigvuldiging kan men reduceren modulo n. We concluderen dat ten hoogste $2N+2$ vermenigvuldigingen modulo n nodig zijn. Omdat N niet groter is dan ${}^2\log n$ groeit het aantal vermenigvuldigingen slechts logaritmisch met n. In de *complexiteitstheorie*, een vak op de grens van wiskunde en informatica dat het gedrag van algoritmen bestudeert, noemt men berekeningen voor waarvan de 'duur' begrensd wordt door een polynomiale uitdrukking in de lengte van de invoer kortweg *polynomiaal*. Dit begrip correspondeert redelijk met 'in de praktijk efficiënt'. Het testen van een 'Fermatcongruentie', waarvoor de lengte van de invoer (a, n) (in decimale of binaire representatie) orde van grootte $\log n$ heeft, is in deze terminologie polynomiaal.

7.1. Voorbeeld. We willen testen of $n = 250093$ een priemgetal is. Het getal heeft geen heel kleine priemfactoren, dus we gaan kijken of $3^{250092} \equiv 1 \bmod n$ geldt. Hiertoe schrijven we de exponent 250092 als 18-cijferig binair getal

$$250092 = 111101000011101100_2.$$

Door herhaald kwadrateren van 3 mod 250093 vinden we de machten 3^{2^k} mod 250093 voor $k = 0, 1, 2, \ldots, 17$. We hebben de 10 waarden corresponderend met $k = 2$, 3, 5, 6, 7, 12, 14, 15, 16 en 17 nodig. Dit zijn de restklassen van respectievelijk

81, 6561, 174643, 85634, 205103, 39836, 49857, 46122, 197919, 114064.

Deze vermenigvuldigen we, waarbij we na iedere vermenigvuldiging het antwoord reduceren modulo n. Het resultaat is 187705 mod 250093. We concluderen dat n niet priem is. We vinden echter op deze manier geen factor van n.

Opgave 1. Ga na dat 3^{250092} meer dan 100 000 decimale cijfers heeft.

Als men voor een getal n voor een paar willekeurig gekozen waarden van a vindt dat $\bar{a}^{n-1} \equiv 1 \bmod n$ geldt, dan is dit een sterke aanwijzing dat n priem is. Het geeft echter geen *bewijs* dat n priem is. Sterker nog, er zijn samengestelde getallen n, de zogenaamde *Carmichael-getallen*, die de eigenschap hebben dat voor alle $a \in \mathbf{Z}$ de Fermatcongruentie $a^n \equiv a \bmod n$ uit 6.18 geldt. Voor dergelijke n geldt $\bar{a}^{n-1} = \bar{1}$ voor alle $\bar{a} \in (\mathbf{Z}/n\mathbf{Z})^*$. Carmichael-getallen zijn tamelijk zeldzaam, maar we weten sinds 1992 dat er oneindig veel zijn[27].

Opgave 2. Ga na dat $n = 3 \cdot 11 \cdot 17 = 561$ en $1729 = 7 \cdot 13 \cdot 19$ Carmichael-getallen zijn.

Nog afgezien van de problemen met een eventuele omkering van 6.18 is het testen van welke congruentie dan ook voor *alle* $a \bmod n$ evenveel werk als het proberen van alle delers van n, en dus niet praktisch. We kunnen daarom via de Fermatcongruentie wel vaak bewijzen dat bepaalde getallen samengesteld zijn, maar vrijwel nooit dat ze priem zijn. Om te bewijzen dat een getal p priem is moet men namelijk laten zien dat $(\mathbf{Z}/p\mathbf{Z})^*$ echt orde $p-1$ heeft, niet alleen dat er veel elementen in $(\mathbf{Z}/p\mathbf{Z})^*$ zijn met een orde die $p-1$ deelt. Men past in de praktijk daarom varianten van de Fermatcongruentie toe die leiden tot wat wel een *pseudo-priemtest* heet. Voor deze iets subtielere congruenties kan men bewijzen dat indien n niet priem is, voor minstens de helft van alle $a < n$ de testcongruentie *niet* geldt. Dit geeft een *probabilistische methode* om primaliteit van n te testen. Immers, de kans om als n samengesteld is k keer achter elkaar een a te treffen die aan de congruentie voldoet is kleiner dan 2^{-k}. Neemt men bijvoorbeeld $k = 10$, dan is de kans dat een samengestelde n door de test komt kleiner dan 1 op 1000. Wil men heel zeker zijn, dan neemt men $k = 50$; de kans op vergissing door een fout in de hardware is dan meestal groter dan de kans op 50 achtereenvolgende ongelukkige keuzes voor a. De kans is echter voor dergelijke algoritmen nooit 0.

Er zijn priemtests die wat meer tijd vragen, maar als resultaat dan ook een echt *primaliteitsbewijs* voor n geven ingeval n priem is. De vraag of zoiets in polynomiale tijd kan, is lang open gebleven. Pas in 2002 vonden de Indiase informatici Agrawal, Kayal en Saxena een deterministische methode, naar hun initialen de AKS-primaliteitstest genoemd, waarvan zij bewezen dat hij polynomiaal was. Oudere methoden, die tamelijk geavanceerde wiskunde als *elliptische krommen* en *cyclotomische lichamen* gebruiken, waren al zo snel dat primaliteit van getallen van enige duizenden cijfers ermee bewezen kan worden[28].

Grote priemgetallen zijn niet alleen gemakkelijk te herkennen, ze zijn in de praktijk ook gemakkelijk te *maken*. Er is namelijk de volgende kwantitatieve versie van Euclides' stelling 6.5.

7.2. Priemgetalstelling. *Zij $\pi(x)$ het aantal priemgetallen kleiner dan $x \in \mathbf{R}$. Dan geldt*

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

Deze beroemde stelling, die al voor 1800 vermoed werd door Gauss, werd pas in 1896 bewezen door de Franse wiskundigen Hadamard (1865–1963) en de la Vallée-Poussin (1866–1962). Het bewijs past complex-analytische argumenten toe op de *Riemann-zeta-functie*, die voor $s > 1$ gedefinieerd is door $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ en een natuurlijke voortzetting heeft tot $\mathbf{C} \setminus \{1\}$. Het valt buiten het bestek van dit college[29].

De priemgetalstelling wordt vaak geschreven als $\pi(x) \sim x/\log x$, waarbij het symbool $\sim$ betekent dat het quotiënt van beide functies voor $x \to \infty$ tot 1 nadert. Op grond van deze stelling verwachten we dat in de buurt van een groot getal x ongeveer 1 op de $\log x$ getallen een priemgetal is. Voor $x = 10^{100}$ is dit 1 op $100\log(10) \approx 230$. Er is geen stelling die ons garandeert dat de priemgetallen niet af en toe onverwacht ver uit elkaar liggen, zodat het in principe mogelijk zou zijn dat er na 10^{100} een groot 'gat' in de priemgetallen valt. Praktisch zijn er echter nooit problemen. Zo zijn de eerste 10 priemgetallen na 10^{100} de getallen $10^{100} + k$ met $k = 267$, 949, 1243, 1293, 1983, 2773, 2809, 2911, 2967 en 3469, op onderlinge afstanden variërend van 790 tot 36. We vatten het bovenstaande op de volgende informele manier samen.

7.3. Feit. *Grote priemgetallen zijn gemakkelijk te maken.*

▶ Factorisatie van grote getallen

Het feit dat we van een groot getal gemakkelijk kunnen bepalen of het een priemgetal is betekent niet dat we, in het geval we vinden dat het getal samengesteld is, zo'n getal gemakkelijk in factoren kunnen ontbinden. Zo heeft het getal in voorbeeld 7.1 een ontbinding $250093 = 449 \cdot 557$, maar die volgt niet uit ons 'samengesteldheidsbewijs'. In dit geval zijn de priemdelers zo klein dat ze met de na 6.7 geschetste methode van *trial division* gemakkelijk te vinden zijn. Deze methode is echter niet polynomiaal in de zin van de complexiteitstheorie, maar voor getallen zonder kleine priemfactoren *exponentieel*. In het ongunstigste geval moet men namelijk alle delers $d \leq \sqrt{n}$ van n testen. In de praktijk is trial division daarom vaak totaal ondoenlijk. Heeft men bijvoorbeeld een getal n van 100 cijfers dat een product van twee ongeveer even grote priemgetallen is en een snelle computer die een biljoen delers per seconde kan testen, dan duurt deze methode ongeveer $10^{50}/10^{12} = 10^{38}$ seconden. Om een idee te krijgen van grote getallen: er gaan ongeveer $3 \cdot 10^7$ seconden in een jaar, een mensenleven duurt gemiddeld ruim $2 \cdot 10^9$ seconden en de geschatte leeftijd van het heelal is om en nabij de 10^{18} seconden. Dit laat zien dat trial division voor getallen zonder kleine priemfactoren geen praktische waarde heeft.

De cryptografische toepassing van de stelling van Euler die we nu gaan geven is in zekere zin een negatieve toepassing. Hij berust erop dat we vooralsnog *niet* goed kunnen factoriseren, en bij de ontdekking van een efficiënte factorisatiealgoritme houdt hij op te bestaan.

7.4. Timmermanswijsheid. *Het ontbinden van grote gehele getallen is moeilijk.*

In wiskundiger termen betekent bovenstaande wijsheid dat de beste algoritmen die we op dit moment hebben om getallen n te factoriseren voor 'veel' n een looptijd hebben

die verre van polynomiaal is. In praktische bewoordingen betekent het dat niemand samengestelde getallen van een paar honderd cijfers zonder 'makkelijke' priemfactoren kan ontbinden. Makkelijke priemfactoren zijn factoren p die klein genoeg zijn om snel met trial division of andere exponentiële methoden gevonden te kunnen worden.

▶ Cryptografie

De *cryptografie* dankt haar bestaansrecht aan het feit dat er behoefte bestaat aan het zodanig versturen van boodschappen dat anderen dan de geadresseerde de inhoud van de boodschap niet kunnen begrijpen als zij er op een of andere manier in slagen deze in handen te krijgen. Met andere woorden: de boodschap moet in *geheimschrift* worden verzonden, en niemand behalve de geadresseerde moet dit kunnen ontcijferen. De oudste toepassingen van de cryptografie zijn militair, maar inmiddels is het toepassingsgebied drastisch uitgebreid. Moderne communicatietechnieken als mobiel telefoneren, bankieren per modem of bestellen via internet vragen om grootschalige routinematige versleuteling van informatie die langs min of meer publieke kanalen verstuurd wordt. Het *RSA-cryptosysteem*, genoemd naar de ontdekkers Rivest, Shamir en Adleman die de methode in 1976 voorstelden, is hierbij een standaardmethode. Het is wat in het Engels een *public key cryptosystem* heet. Dit betekent dat, anders dan in meer traditionele cryptosystemen, de sleutel en de methode voor het coderen van boodschappen publiek bekend worden gemaakt, Dit heeft het zeker in veel moderne toepassingen uiterst praktische voordeel dat er *niet* van te voren een geheime sleutel tussen zender en ontvanger hoeft te worden afgesproken, met alle veiligheidsproblemen die dit met zich meebrengt. Het verbazende is dat er bij dit ogenschijnlijke gebrek aan geheimen *toch* informatie verstuurd kan worden die voor derden nagenoeg onleesbaar is.

▶ Het RSA-cryptosysteem

In het RSA-systeem gaan we ervanuit dat de te versturen boodschap uit één of meer getallen bestaat van een vaste grootte, zeg 300 cijfers. Voor 'letterboodschappen' kan men bijvoorbeeld alle woorden 'vercijferen' door een eenvoudige substitutie ($a = 01$, $b = 02$, $c = 03$, tot en met spatie $= 27$, er is zelfs ruimte voor 100 karakters) toe te passen en vervolgens het verkregen lange getal in blokjes van 300 cijfers op te hakken. Iedereen die alleen door hem te lezen boodschappen wil ontvangen kiest 2 getallen die hij publiek bekend maakt, bijvoorbeeld door ze te adverteren of op zijn internethomepage op te nemen. Het eerste getal is zijn persoonlijke *modulus* n. Dit is een getal $n \approx 10^{300}$ dat de ontvanger zelf maakt door twee grote priemgetallen, zeg van zo'n 150 cijfers elk, te vermenigvuldigen. De factorisatie $n = pq$ houdt hij geheim, en mits de keuze van p en q niet extreem onhandig is betekent dit met de huidige stand van zaken dat niemand anders dan hij achter de waarde van p en q kan komen.

Opgave 3. Waarom is de keuze $n = (10^{150}+67)(10^{150}+427)$, het product van de twee kleinste priemen van 151 cijfers, niet veilig? Is algemener een keus van twee opeenvolgende priemen verstandig?

Het tweede getal dat de ontvanger bekend maakt is zijn *publieke exponent*. Dit is een getal $e > 1$ waarvan de belangrijkste eigenschap is dat het onderling ondeelbaar is met $(p-1)(q-1)$. Men kan het kleinste priemgetal nemen dat $(p-1)(q-1)$ niet deelt, maar in principe is ieder ander getal waarvoor de Euclidische algoritme uitwijst dat het onderling ondeelbaar is met $(p-1)(q-1)$ ook goed[30]. We maken nu gebruik van onderstaand gevolg van Euler's stelling 6.17.

7.5. Stelling. *Laat $n = pq$ een product van twee verschillende priemgetallen p en q zijn, en $e > 1$ een getal dat onderling ondeelbaar is met $(p-1)(q-1)$. Dan bestaat er een getal $f > 0$ met $ef \equiv 1 \bmod (p-1)(q-1)$, en voor dergelijke f geldt*

$$a^{ef} \equiv a \bmod n$$

voor alle $a \in \mathbf{Z}$.

Bewijs. Omdat e inverteerbaar is modulo $(p-1)(q-1)$ bestaan er positieve getallen f met de genoemde eigenschap. Voor dergelijke f kunnen we $ef = 1 + r(p-1)(q-1)$ schrijven met $r \in \mathbf{Z}$. Wegens 6.16 geldt $\varphi(pq) = (p-1)(q-1)$. Met behulp van 6.17, toegepast op $n = pq$, vinden we nu $a^{ef} = a \cdot a^{r(p-1)(q-1)} \equiv a \bmod n$ voor alle a die onderling ondeelbaar zijn met $n = pq$. Is a deelbaar door p of q, dan ziet men als in het bewijs van 6.18 gemakkelijk dat de congruentie eveneens vervuld is. □

Opgave 4. Laat zien dat 7.5 ook geldt als we $ef \equiv 1 \bmod \mathrm{kgv}(p-1, q-1)$ eisen.

Om nu een geheime boodschap N van 300 cijfers te sturen aan een ontvanger met modulus n en publieke exponent e berekent men het getal $N^e \bmod n$. Zoals we zagen kan dit efficiënt door herhaalde kwadrateringen modulo n, en is het niet nodig een groot getal als N^e ooit uit te rekenen. Wil het systeem nu werken, dan dient het zo te zijn dat behalve de ontvanger niemand anders uit de waarde van $N^e \bmod n$ de waarde van $N \bmod n$ af kan leiden. (Merk op dat we met $N \bmod n$ ook N zelf hebben omdat we $0 < N < n$ kiezen.) Dit berust op het feit dat de enige bekende manier waarmee men in de praktijk de waarde van $N \bmod n$ uit de waarde van N^e af kan leiden bestaat uit het vinden van een 'inverse exponent' f als in stelling 7.5. Met de inverse exponent f krijgt men namelijk door een tweede machtsverheffing de oorspronkelijke boodschap $N < n$ terug: $(N^e)^f \equiv N \bmod n$. Andere mogelijke methodes, zoals het proberen van exponenten, kosten veel te veel tijd.

Het vinden van de inverse exponent f in 7.5 bestaat uit het vinden van de inverse van e modulo $(p-1)(q-1)$, en dit kan niemand anders dan de ontvanger, die de waarden p en q kent. Zelfs de afzender van een bericht, die niet alleen N^e maar ook N kent, kan de inverse exponent f niet vinden. We zien dat de ontvanger de 'onleesbaarheid' van alle aan hem gerichte berichten kan garanderen door zorgvuldig de waarden van p, q en zijn 'geheime exponent' f geheim te houden.

Opgave 5. Laat zien hoe we uit $n = pq$ en $m = (p-1)(q-1)$ de factoren p en q kunnen bepalen. Factoriseer $250093 = pq$ met gebruik van de waarde $249088 = (p-1)(q-1)$.

7.6. Voorbeeld. Stel dat we de boodschap 'OK' willen versturen aan een ontvanger met publieke exponent 23 en (onrealistisch kleine) modulus 250093. We vernummeren

de boodschap zoals aangegeven als 1511 en berekenen $1511^{23} \equiv 141886 \bmod 250093$. Het getal 141886 wordt nu verstuurd. De ontvanger, die de factorisatie $250093 = 449 \cdot 557$ bezit, kent de inverse van 23 modulo $448 \cdot 556 = 249088$, die $f = 129959$ is. Hij berekent gemakkelijk $141886^{129959} \equiv 1511 \bmod 250093$ en vindt zo het originele bericht $1511 = \text{OK}$ terug.

Opgave 6. Stel dat de ontvanger publieke modulus 1111 en exponent 29 heeft. Decodeer de aan hem gerichte boodschap 198.

▶ Digitale handtekeningen

Er is een verfijning van het boven beschreven *RSA-protocol* waarbij de afzender A tevens *bewijst* dat hij degene is die de boodschap verstuurd heeft, en niet een bedrieger die probeert zich voor A uit te geven. Men kan hierbij denken aan de situatie dat de ontvanger B een bank is en A een persoon die betalingsopdrachten verstuurt. De bank wil dan graag een 'digitale handtekening' van A onder de betalingsopdrachten zien staan.

Voor deze verfijning hebben we niet alleen de publieke exponent e_B en de modulus n_B van de ontvanger B nodig, maar eveneens soortgelijke door A gekozen waarden e_A en n_A. Hierbij is B de enige persoon die n_B kan ontbinden en A de enige persoon die n_A kan ontbinden. Stel dat we een bericht $N < n_A < n_B$ willen versturen. Wat A doet om een geheime boodschap N te vercijferen is eerst N vervangen door een getal $M < n_A$ met $M \equiv N^{f_A} \bmod n_A$. Hierbij is f_A de geheime exponent van A, die aan niemand anders dan A bekend is. De afzender A zendt nu M over als voorheen. Dit wil zeggen dat hij de waarde $M^{e_B} \bmod n_B$ naar B stuurt. Hier kan B door een machtsverheffing tot zijn eigen geheime exponent de waarde van M uit afleiden, en dus kent hij het getal $N^{f_A} \bmod n_A$. Om nu de originele boodschap te verkrijgen neemt B de publieke exponent e_A en rekent modulo de modulus n_A de e_A-de macht van $N^{f_A} \bmod n_A$ uit. Dit is $N^{e_A f_A} = N \bmod n_A$, en dit geeft hem N. Bovendien weet B nu dat de boodschap van A komt, want niemand anders dan A zelf is in staat een boodschap tot de geheime exponent f_A te verheffen modulo n_A.

Opgave 7. Is de aanname $n_A < n_B$ essentieel?

▶ Veiligheid van RSA

De veiligheid van het RSA-protocol berust op de aanname dat niemand een welgekozen modulus van 300 cijfers zonder aanvullende kennis kan factoriseren. Bij de introductie van het RSA-systeem, in 1976, gaf Rivest een gecodeerde boodschap als uitdaging mee. Hij gebruikte hiervoor het 'veilige' getal

$$\begin{aligned}\text{RSA}_{129} =& 114381625757888867669235779976146612010218296721242362562561842\backslash\\ & 9357069352457338978305971235639587050589890751475992900268795435 41\end{aligned}$$

van 129 cijfers en zei te verwachten dat de vele miljoenen jaren rekentijd die nodig zouden zijn voor het factoriseren van dit getal de code praktisch onkraakbaar maakten.

Voorspellingen doen blijkt hier niet gemakkelijk, en de methoden om grote gehele getallen te ontbinden zijn in de afgelopen 30 jaar dramatisch verbeterd.

In 1994 werd het getal met een als de *kwadratische zeef* bekend staande methode gefactoriseerd als

$$\begin{aligned}\mathrm{RSA}_{129} = 34905295108476509491478496199038981334177646384933878439908205 77\cdot \\ 32769132993266709549961988190834461413177642967992942539798288533.\end{aligned}$$

Deze methode maakt gebruik van vele duizenden door computerbezitters via e-mail aangedragen 'hulpfactorisaties'. Met behulp van de in de vroege jaren 90 ontwikkelde 'getallenlichamenzeef' werd in 1996 de volgende 'RSA-challenge', de RSA-sleutel RSA_{130} van 130 cijfers gekraakt[31]. De getallenlichamenzeef is een wat ingewikkelder algoritme, dat gebruik maakt van de arithmetiek van getallenlichamen. De optimalisatie heeft enige tijd gekost, maar het is nu de methode die alle records vestigt. In december 2009 werd een mijlpaal bereikt met het kraken van de eerste 768-bits sleutel (232 decimale cijfers). De 1024-bits sleutels (309 decimale cijfers) bij de banken zijn al door 2048-bits sleutels vervangen; hoe lang dit als veilig zal gelden, moet de toekomst leren. De nog geen 35 jaar lange historie van RSA laat zien dat het doen van voorspellingen over de ontwikkeling van factorisatie-methoden tot dusver een hachelijke onderneming gebleken is.

▶ Discrete logaritmen

Als op een dag een efficiënte factorisatiealgoritme gevonden wordt die RSA als cryptosysteem onbruikbaar maakt, dan zijn er diverse andere public key cryptosystemen die nog wel gebruikt kunnen worden. Wat men om zulke systemen te maken nodig heeft is een wiskundige procedure die in één richting eenvoudig uit te voeren is, maar waarvoor de 'omkering' onevenredig veel moeilijker is. Het vermenigvuldigen van priemgetallen p en q tot een groot getal n is voor RSA een dergelijke procedure, daar de omkering, het ontbinden van n in p en q, niet iets is waarvoor we snelle algoritmen hebben.

In de groepentheorie is er een soortgelijk probleem dat geheel binnen het kader van deze syllabus valt, het bepalen van *discrete logaritmen*. In sommige groepen lijkt dit een erg moeilijk probleem te zijn, maar net als in het geval van factorisatie ontbreekt steeds een *stelling* dat een snelle algoritme niet bestaat: misschien zijn we onhandig en ligt een slimme algoritme om de hoek voor wie voldoende wiskunde op zak heeft!

Laat G een cyclische groep van orde n zijn, en g een voortbrenger van G. Dan is het isomorfisme

$$\begin{aligned} f: \quad \mathbf{Z}/n\mathbf{Z} &\xrightarrow{\sim} G \\ k &\longmapsto g^k \end{aligned}$$

een afbeelding waarvoor de input k lengte $\log n$ heeft, en waarvoor de output g^a voor veel groepen G in tijd polynomiaal in $\log n$ berekend kan worden. Het discrete-logaritme-probleem in de groep G bestaat eruit de *inverse* van f te berekenen. Met andere woorden: gegeven een element $h \in G$, vind een exponent $k = f^{-1}(h) \in \mathbf{Z}/n\mathbf{Z}$

zodat $g^k = h$ geldt. Men noemt $k = f^{-1}(h)$ de *discrete logaritme* van $h \in G$ met betrekking tot de basis g, en schrijft

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

De moeilijkheid van het berekenen van f^{-1} hangt er sterk van af welke keuze er gemaakt wordt voor G. Neemt men bijvoorbeeld $G = \mathbf{Z}/n\mathbf{Z}$ en $g = 1 \bmod n$, dan is f de identiteit en is er helemaal geen probleem. Kiest men een andere voortbrenger x voor de additieve groep $G = \mathbf{Z}/n\mathbf{Z}$, dan is het discrete-logaritme-probleem voor $h \in \mathbf{Z}/n\mathbf{Z}$ niets anders dan het oplossen van k uit de vergelijking $kx = h$. Hiervoor is het voldoende beide leden te vermenigvuldigen met de *multiplicatieve* inverse x^{-1} van x modulo n, en deze inverse kan berekend worden met de Euclidische algoritme, als in 6.14. In dit geval kan het discrete-logaritme-probleem in tijd polynomiaal in $\log n$ opgelost worden.

Opgave 8. Laat g_1 en g_2 voortbrengers zijn van G. Bewijs: $\log_{g_2}(h) = \log_{g_1}(h) \log_{g_2}(g_1)$.

Een interessantere keuze voor G is de multiplicatieve groep $G = (\mathbf{Z}/p\mathbf{Z})^*$ modulo een priemgetal p, die orde $n = p - 1$ heeft.

7.7. Stelling. *Voor een priemgetal p is $(\mathbf{Z}/p\mathbf{Z})^*$ een cyclische groep van orde $p - 1$.*

Het bewijs van 7.7 berust op een feit dat meer met ringen dan met groepen te maken heeft. We zullen het in 12.3 en 12.4 nogmaals tegenkomen.

7.8. Lemma. *Zij $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ een polynoom van graad $n \geq 1$ met coëfficiënten in $\mathbf{Z}/p\mathbf{Z}$. Dan heeft f niet meer dan n nulpunten in $\mathbf{Z}/p\mathbf{Z}$.*

Bewijs. We voeren het bewijs met inductie naar de graad van f. Voor $n = 1$ en $f = X + a_0$ is $-a_0$ het enige nulpunt: inversen in de optelgroep $\mathbf{Z}/p\mathbf{Z}$ zijn uniek!

Zij nu f van graad $n > 1$ en $x \in \mathbf{Z}/p\mathbf{Z}$ een nulpunt van f. Dan kunnen we f schrijven als $f = (X - x)g$ voor een polynoom g van graad $\leq n - 1$. Immers, omdat $X^k - x^k$ deelbaar is door $X - x$ voor $k \geq 1$ hebben we heel expliciet

$$f(X) = f(X) - f(x) = \textstyle\sum_{k=0}^{n} a_k(X^k - x^k) = (X - x) \cdot \sum_{k=1}^{n} a_k \sum_{j=0}^{k-1} x^{k-1-j}X^j.$$

Is nu $y \neq x$ een tweede nulpunt van f in $\mathbf{Z}/p\mathbf{Z}$, dan geldt hiervoor $(y - x)g(y) = 0$. Wegens de priemeigenschap 6.6 is een product van twee elementen in $\mathbf{Z}/p\mathbf{Z}$ alleen 0 als één van beide elementen het is. Wegens $x - y \neq 0$ moet $g(y) = 0$ gelden, dus de nulpunten van f verschillend van x zijn de nulpunten van g. Wegens de inductiehypothese heeft g ten hoogste $n - 1$ nulpunten, en we zijn klaar. □

Merk op dat de aanname dat p priem is essentieel is: in $\mathbf{Z}/24\mathbf{Z}$ heeft het polynoom $X^2 - 1$ de *acht* nulpunten $\pm 1, \pm 5, \pm 7, \pm 11$.

Bewijs van 7.7. We brengen in herinnering dat een *cyclische* groep $C = \langle y \rangle$ van orde n voor iedere positieve deler $d|n$ precies één ondergroep van orde d bevat, voortgebracht door $x = y^{n/d}$, en dat de elementen van orde d in C de machten x^i van x zijn met exponent $i \in \{1, 2, \ldots, d\}$ onderling ondeelbaar met d. In het bijzonder bevat C voor

iedere $d|n$ precies $\varphi(d)$ elementen van orde d, met φ de Euler-φ-functie. Sommatie over alle $d|n$ geeft $\sum_{d|n}\varphi(d) = \#C = n$, de *formule van Gauss*.

Geef nu met $\psi(d)$ het aantal elementen van orde d aan in $(\mathbf{Z}/p\mathbf{Z})^*$. Als $x \in (\mathbf{Z}/p\mathbf{Z})^*$ orde d heeft, dan zijn de d verschillende machten $x, x^2, x^3, \ldots, x^d = 1$ van x nulpunten van $X^d - 1$ in $\mathbf{Z}/p\mathbf{Z}$. Wegens 7.8 zijn er geen verdere nulpunten van $X^d - 1$ in $\mathbf{Z}/p\mathbf{Z}$, dus de elementen van orde d in $(\mathbf{Z}/p\mathbf{Z})^*$ zijn precies de $\varphi(d)$ machten x^i van x met exponent i copriem met d. We concluderen dat $\psi(d)$ gelijk is aan $\varphi(d)$ als $(\mathbf{Z}/p\mathbf{Z})^*$ een element van orde d bevat, en gelijk aan 0 als dat niet het geval is. Nu geldt

$$p - 1 = \#(\mathbf{Z}/p\mathbf{Z})^* = \textstyle\sum_{d|p-1}\psi(d) \leq \sum_{d|p-1}\varphi(d) = p - 1,$$

en er volgt $\psi(d) = \varphi(d)$ voor alle $d|p-1$. In het bijzonder geldt $\psi(p-1) = \varphi(p-1) > 0$, dus $(\mathbf{Z}/p\mathbf{Z})^*$ bevat een element van orde $p-1$ en is cyclisch. □

Zie opgave 16 voor een bewijs van 7.7 dat niet berust op de formule van Gauss.

Een getal $a \in \mathbf{Z}$ waarvoor $a \bmod p$ een voortbrenger van $(\mathbf{Z}/p\mathbf{Z})^*$ is, heet een *primitieve wortel* modulo p. Merk op dat een getal a niet deelbaar door p een primitieve wortel is modulo p dan en slechts dan als $a^d \not\equiv 1 \bmod p$ geldt voor alle delers $d < p-1$ van $p-1$.

Opgave 9. Laat zien dat a een primitieve wortel is modulo p als p geen deler is van a en $a^d \not\equiv 1 \bmod p$ geldt voor alle exponenten $d = (p-1)/\ell$, met ℓ lopend over de priemdelers van $p-1$.

Is p een groot priemgetal en a een primitieve wortel modulo p, dan is het isomorfisme

$$\begin{aligned} f: \quad \mathbf{Z}/(p-1)\mathbf{Z} &\xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^* \\ k &\longmapsto a^k \end{aligned} \tag{7.9}$$

voor gegeven k efficiënt te berekenen als in 7.1, door herhaald kwadrateren. Het bepalen van de inverse van f is echter een lastig probleem, dat aan diverse cryptografische routines ten grondslag ligt. Er zijn betere methoden dan het domweg proberen van alle mogelijke waarden van k voor $f^{-1}(b)$, maar voor grote priemen blijven deze methoden nog veel te langzaam. De huidige records (van 2014) liggen bij priemen van 180 cijfers.

Er zijn diverse cyclische groepen verschillend van $(\mathbf{Z}/p\mathbf{Z})^*$ waarin men wel 'snel' kan machtsverheffen, maar waarin het bepalen van discrete logaritmen moeilijk lijkt. Cyclische groepen voortgebracht door een punt van grote orde op *elliptische krommen* over $\mathbf{Z}/p\mathbf{Z}$ worden al gebruikt in de cryptografie, en de arithmetische algebraïsche meetkunde heeft nog meer groepen in petto waarvan de cryptografische merites nog onderwerp van onderzoek zijn.

▶ Diffie-Hellman protocol

Ter afsluiting geven we een protocol dat twee partijen A en B in staat stelt om over een *publiek* kanaal af te spreken welke *geheime* sleutel zij gaan gebruiken om boodschappen aan elkaar te versleutelen. De voor de hand liggende gedachte dat zoiets helemaal niet mogelijk is blijkt ook hier niet juist te zijn, en de reden is van eenzelfde soort als in het

geval van RSA: het berekenen van $a^k \in (\mathbf{Z}/p\mathbf{Z})^*$ voor gegeven $a \in (\mathbf{Z}/p\mathbf{Z})^*$ en $k \in \mathbf{Z}$ is gemakkelijk, maar het terugvinden van $k \in \mathbf{Z}/(p-1)\mathbf{Z}$ uit a en $a^k \in (\mathbf{Z}/p\mathbf{Z})^*$ is een discrete-logaritme-probleem, dat voor grote p te moeilijk is om in de praktijk te doen. Preciezer gezegd: het eerste kunnen we in polynomiale tijd doen, voor het tweede zijn geen polynomiale algoritmen bekend. Men zegt daarom wel dat het isomorfisme f in 7.9 voor grote p een *one way function* is.

Het *Diffie-Hellman protocol* gebruikt de 'onomkeerbaarheid' van 7.9 om A en B over een publieke lijn een geheime sleutel af te laten spreken. Hiertoe kiezen zij 'in het openbaar' samen een groot priemgetal p en een primitieve wortel g mod p. Vervolgens kiest elk van beide partijen een strikt persoonlijke geheime exponent. Als A de exponent a kiest, dan stuurt hij g^a naar B. Evenzo stuurt B naar A het element g^b, met b zijn eigen geheime exponent. Nu berekent A, die niet b maar wel a kent, de a-de macht g^{ab} van het van B ontvangen bericht g^b. Evenzo berekent B, die niet a maar wel b kent, de b-de macht g^{ab} van het van A ontvangen bericht g^a. We zien dat g^{ab} een element is dat zowel A als B gemakkelijk kan berekenen, en dit kiezen A en B als geheime sleutel.

Een argeloze afluisteraar van het publieke kanaal kan nu echter de sleutel g^{ab} *niet* berekenen. Immers, deze persoon kent behalve p en g de machten g^a en g^b, maar *geen van beide* geheime exponenten a en b. Immers, dit zijn de discrete logaritmen van g^a en g^b met betrekking tot de basis g, en die kan hij niet berekenen als p voldoende groot gekozen wordt. Voor zover ons nu bekend is, is er geen efficiënte methode om g^{ab} te berekenen uit g^a en g^b zonder eerst a of b te berekenen, en dit geeft ons vertrouwen dat dit zogenaamde *Diffie-Hellman-protocol* een veilige methode is om een geheime sleutel te kiezen.

Opgaven.

10. Zij $n = n_0$ een natuurlijk getal, en definieer voor $k \geq 0$ en $n_k \neq 0$ inductief gehele getallen $r_k \in \{0, 1\}$ en $n_{k+1} \in \mathbf{Z}$ door $n_k = 2n_{k+1} + r_k$, waar $r_k \equiv n_k \bmod 2$. Bereken de getallenrij $(r_k)_k$ voor het getal $n_0 = 250092$, en bewijs algemeen dat de getallenrij $\ldots r_2 r_1 r_0$ de binaire representatie van n geeft.

11. Zij a geheel en $p \nmid a$ een oneven priemgetal. Bewijs: $a^{(p-1)/2} \equiv \pm 1 \bmod p$.

12. *(Pseudo-priemtests.)* Bepaal een oneven getal n dat samengesteld is en waarvoor aan de congruenties $2^{(n-1)/2} \equiv \pm 1 \bmod n$ en $3^{(n-1)/2} \equiv \pm 1 \bmod n$ voldaan is.
[Ik zou deze pseudo-priemtest maar programmeren. Er zijn 2 oplossingen $n < 10000$.]

13. Decodeer de boodschap 99099932142 gericht aan een ontvanger met publieke exponent 13 en modulus 246790125209.
[Hint: het laatste priemjaar van de 20e eeuw is in de modulus gebruikt....]

*14. (Voor de serieuze factorisator....) Hier is een laatste bericht, gecodeerd met exponent $e = 31$ modulo $n = 152415787532388367515775036651577063184899559529738 21$:

$$57578028973406421763606857604395192250102736353887 24.$$

15. Laat A een abelse groep zijn, en stel dat A elementen van eindige ordes a en b bevat. Bewijs dat A een element van orde $\mathrm{kgv}(a, b)$ bevat.
[Hint: kijk eerst naar het geval dat a en b onderling ondeelbaar zijn.]

16. Zij A een abelse groep van orde n. Definieer de *exponent* van A als het kleinste positieve getal e met de eigenschap dat $a^e = 1$ geldt voor alle $a \in A$.
    a. Bewijs: e is een deler van n, en gelijk aan n dan en slechts dan als A cyclisch is.
    b. Leid uit 7.8 af dat de exponent van $A = (\mathbf{Z}/p\mathbf{Z})^*$ gelijk is aan $p-1$, en dat $(\mathbf{Z}/p\mathbf{Z})^*$ *dus* cyclisch is.

17. Bepaal primitieve wortels modulo 11, 31, 41 en 71.

18. Bepaal de kleinste 6 priemgetallen $p > 2$ waarvoor 5 mod p een primitieve wortel is. Wat valt je op aan de eindcijfers van deze priemgetallen?[32] *Zijn er oneindig veel priemgetallen p waarvoor 5 mod p een primitieve wortel is?[33]

19. Laat zien dat 2 een primitieve wortel is modulo 101, en bereken $\log_2(3)$, $\log_2(5)$ en $\log_2(7)$ in de groep $(\mathbf{Z}/101\mathbf{Z})^*$.

8 Quotiënten en producten.

Met de constructie van de quotiëntafbeelding $G \to G/N$ uit 4.13 wordt het mogelijk om allerlei 'abstracte groepentheorie' te doen. We beginnen met een aantal algemene stellingen over quotiëntgroepen, die in feite directe gevolgen zijn van de definities of de isomorfiestelling 4.9.

▶ Ondergroepen onder quotiëntafbeeldingen

De factorgroep G/N van een groep G modulo een normaaldeler N is in principe 'eenvoudiger' dan G; we hebben immers informatie 'vergeten'. De vraag wat de ondergroepen, normaaldelers en quotiënten van G/N zijn kunnen we dan ook direct beantwoorden in termen van G.

8.1. Stelling. *De ondergroepen van de quotiëntgroep $\overline{G} = G/N$ zijn van de vorm $\overline{H} = H/N$, met $H \subset G$ een ondergroep van G die N bevat. Voor dergelijke H is*

$$\begin{aligned} f : G/H &\longrightarrow \overline{G}/\overline{H} \\ gH &\longmapsto \overline{g}\overline{H} \end{aligned}$$

een bijectieve afbeelding tussen de verzamelingen van linkernevenklassen. In het bijzonder geldt $[G : H] = [\overline{G} : \overline{H}]$, en is H normaal in G dan en slechts dan als $\overline{H}$ normaal is in $\overline{G}$. In het normale geval is f een groepsisomorfisme.

Bewijs. Als $X \subset G/N$ een ondergroep is en $\pi : G \to G/N$ de quotiëntafbeelding, dan is $H = \pi^{-1}[X]$ een ondergroep van G die $N = \ker \pi$ omvat. Omdat π surjectief is geldt $X = \pi[H] = H/N$, dus X is van de vereiste vorm.

Voor $H \supset N$ als boven is $f : G/H \to \overline{G}/\overline{H}$ welgedefinieerd en surjectief. Voldoen $g_1, g_2 \in G$ aan $\overline{g}_1\overline{H} = \overline{g}_2\overline{H}$, dan hebben we $\overline{g}_1 = \overline{g}_2\overline{h} = \overline{g_2 h}$ en $g_1 = g_2 hn$ voor zekere $h \in H$ en $n \in N \subset H$. Wegens $hn \in H$ krijgen we $g_1 H = g_2 H$, dus f is ook injectief. De verkregen bijectie geeft direct de gelijkheid $[G : H] = [\overline{G} : \overline{H}]$ van indices.

Als H normaal is in G of $\overline{H}$ normaal in $\overline{G}$, dan erven G/H en $\overline{G}/\overline{H}$ een groepsstructuur van G. In dit geval is f een isomorfisme. □

Opgave 1. Leid voor $H \supset N$ normaaldelers van G het isomorfisme in 8.1 af door de isomorfiestelling op de natuurlijke afbeelding $G/N \to G/H$ toe te passen.

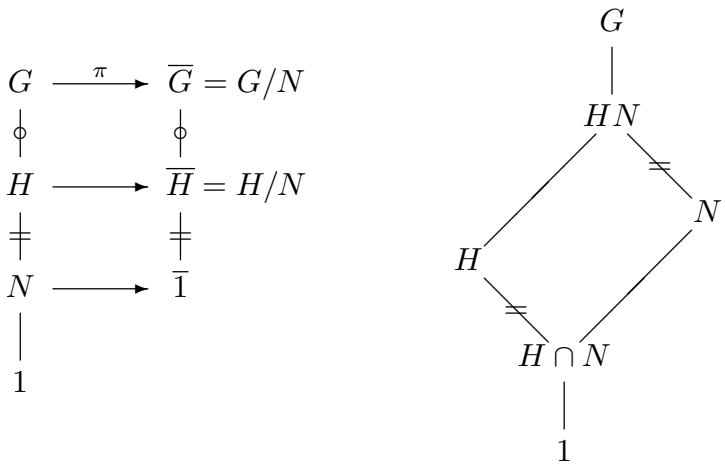
Men kan zich afvragen wat er onder de quotiëntafbeelding $\pi : G \to G/N$ gebeurt met een willekeurige ondergroep $H \subset G$. Het beeld $\pi[H]$ is de ondergroep van G/N bestaande uit de restklassen hN met $h \in H$. Onder 8.1 correspondeert dit met een ondergroep van G die N omvat, te weten $HN = \{hn : h \in H, n \in N\}$.

8.2. Stelling. *Zij $N \triangleleft G$ een normaaldeler en $H \subset G$ een ondergroep. Dan is er een natuurlijk isomorfisme*

$$H/(H \cap N) \xrightarrow{\sim} HN/N.$$

Bewijs. De beperking van de quotiëntafbeelding $\pi : G \to G/N$ tot H geeft een homomorfisme $H \to G/N$ met kern $H \cap N$ en beeld HN/N. De isomorfiestelling 4.9 geeft nu een isomorfisme $H/(H \cap N) \xrightarrow{\sim} HN/N$. □

De uitspraken van de stellingen 8.1 en 8.2 kan men visualiseren aan de hand van *diagrammen* die de diverse pijlen en inclusies aangeven. De conventie hierbij is dat men alle inclusies aangeeft met recht of schuin omhooglopende verbindingslijnen. In onderstaande diagrammen zijn door markering met '=' paren inclusies aangegeven die tot isomorfe quotiënten aanleiding geven. De met '$\circ$' gemarkeerde inclusies zijn het onderwerp van stelling 8.1.



8.3. Voorbeelden. 1. Laat a en b positieve getallen zijn, en neem $H = a\mathbf{Z}$ en $N = b\mathbf{Z}$ in 8.2. Wegens definitie 6.3.3 zijn $H+N$ (het additieve equivalent van HN) en $H \cap N$ de ondergroepen van de additieve groep $\mathbf{Z}$ voortgebracht door respectievelijk $\gcd(a,b)$ en $\mathrm{kgv}(a,b)$. De quotiëntgroepen $a\mathbf{Z}/\mathrm{kgv}(a,b)\mathbf{Z}$ en $\gcd(a,b)\mathbf{Z}/b\mathbf{Z}$ zijn wegens 8.2 isomorf. Hun ordes $\mathrm{kgv}(a,b)/a$ en $b/\gcd(a,b)$ zijn dus hetzelfde, en we vinden hieruit de uit opgave 6.20 bekende gelijkheid

$$\gcd(a,b) \cdot \mathrm{kgv}(a,b) = ab.$$

2. De symmetrische groep $G = S_4$ van orde 24 heeft een normale ondergroep $N = V_4$ bestaande uit (1) en de drie producten van twee disjuncte 2-cykels. Passen we hiervoor 8.2 toe op de niet-normale ondergroep $H = S_3$ van permutaties die het element 4 als dekpunt hebben, dan geldt $H \cap N = 1$ en vinden we een isomorfisme $S_3 \xrightarrow{\sim} S_3V_4/V_4$. Omdat S_3 orde 6 en V_4 orde 4 heeft, is S_3V_4 van orde 24 en dus gelijk aan S_4. We krijgen een isomorfisme $S_3 \xrightarrow{\sim} S_4/V_4$. Dit is de inverse van het isomorfisme $S_4/V_4 \xrightarrow{\sim} S_3$ geïnduceerd door het 'tetraëderhomomorfisme' $T = S_4 \to S_3$ uit §5.

De symmetrische groep S_3 bevat een normale ondergroep A_3 van index 2 en drie niet-normale ondergroepen van index 3. Passen we 8.1 toe op de quotiëntafbeelding $\pi : S_4 \to S_4/V_4 \cong S_3$, dan volgt dat S_4 een normale ondergroep van index 2 en drie niet-normale ondergroepen $H_1, H_2, H_3 \subset S_4$ van index 3 bevat. De ondergroep van index 2 is A_4. De drie niet-normale ondergroepen H_i, die orde 8 hebben, bevatten elk V_4 als ondergroep. Iedere ondergroep van S_4 voortgebracht door V_4 en een 2-cykel is gelijk aan één van de H_i.

Opgave 2. Laat zien dat de drie ondergroepen $H_i \subset S_4$ isomorf zijn met D_4 en door inwendige automorfismen van S_4 in elkaar worden overgevoerd.

Voorbeeld 8.3.2 laat zien dat de stellingen 8.1 en 8.2, die verbanden geven tussen de groepen G en G/N, ons in staat stellen informatie in elk van beide richtingen over te dragen. In bovenstaand voorbeeld gebruikten we eerst een ondergroep $H = S_3$ van $G = S_4$ om het quotiënt $G/N = S_4/V_4$ te begrijpen, en daarna onze expliciete kennis van dit quotiënt om ondergroepen van orde 8 in S_4 te ontdekken.

▶ Homomorfiestelling

De homomorfiestelling vertelt ons wanneer een homomorfisme $f : G \to G'$ *factoriseert* via de quotiëntgroep G/N. Hiermee bedoelen we dat f te schrijven is als een 'product' $f = \overline{f}\pi$ van de quotiëntafbeelding $\pi : G \to G/N$ met een homomorfisme $\overline{f} : G/N \to G'$. Uit het bestaan van zo'n factorisatie volgt dat N bevat is in $\ker(f)$.

8.4. Homomorfiestelling. *Zij $f : G \to G'$ een homomorfisme en N een normaaldeler van G die in $\ker(f)$ bevat is. Dan bestaat er een uniek homomorfisme $\overline{f} : G/N \to G'$ zodat f verkregen wordt als samenstelling*

$$G \xrightarrow{\pi} G/N \xrightarrow{\overline{f}} G'$$

van de quotiëntafbeelding $\pi : G \to G/N$ met $\overline{f}$.

Bewijs. Een afbeelding $\overline{f} : G/N \to G'$ met de genoemde eigenschap wordt noodzakelijk gegeven door $gN \mapsto f(g)$, dus we moeten laten zien dat $\overline{f}$ met deze definitie een welgedefinieerd homomorfisme is.

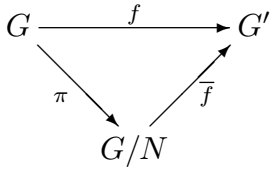
Geldt $g_1N = g_2N$, dan hebben we $g_1 = g_2n$ voor zekere $n \in N \subset \ker(f)$. Wegens $f(n) = e'$ krijgen we $f(g_1) = f(g_2n) = f(g_2)f(n) = f(g_2)$, dus $\overline{f}$ is welgedefinieerd. De homomorfie-eigenschap van $\overline{f}$ volgt direct uit die van f:

$$\overline{f}(g_1N \cdot g_2N) = \overline{f}(g_1g_2N) = f(g_1g_2) = f(g_1)f(g_2) = \overline{f}(g_1N)\overline{f}(g_2N). \qquad \square$$

Opgave 3. Bewijs: $\ker(\overline{f}) = \ker(f)/N$. Hoe volgt 4.9 hieruit?

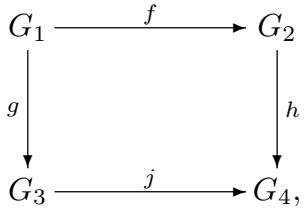
Kort gezegd is de karakterisering van de quotiëntafbeelding $\pi : G \to G/N$ gegeven door 8.4: alle homomorfismen op G die op N triviaal zijn, lopen via het quotiënt G/N.

De homomorfiestelling 8.4 wordt vaak geformuleerd door te zeggen dat er een uniek homomorfisme $\overline{f} : G/N \to G'$ is waarvoor het diagram



commuteert of *commutatief is*. In het algemeen bedoelt men met het commutatief zijn van een diagram van groepen en homomorfismen dat, indien men op twee manieren langs de pijlen van het diagram van een groep naar een andere groep kan lopen, de

bijbehorende samenstellingen van homomorfismen gelijk zijn. Zo betekent bijvoorbeeld het commutatief zijn van een rechthoekig diagram



dat de samenstellingen hf en jg *hetzelfde* homomorfisme $G_1 \to G_4$ geven. De zogenaamde *commutatieve algebra*, een onderdeel van de algebra waar we later kennis mee zullen maken, drukt zich veelvuldig in termen van zulke diagrammen uit.

▶ Commutatorondergroep

Als toepassing van 8.4 beschouwen we het geval dat N de *commutatorondergroep* $[G,G] \subset G$ is. Dit is per definitie de ondergroep van G voortgebracht door alle *commutatoren*

$$[x,y] = xyx^{-1}y^{-1}$$

van elementen $x, y \in G$. De identiteit $[\sigma(x),\sigma(y)] = \sigma([x,y])$ voor $\sigma \in \mathrm{Aut}(G)$ laat zien dat een automorfisme van G de commutatoren permuteert. De commutatorondergroep blijft dus onder automorfismen op zijn plaats, en is daarmee een *karakteristieke ondergroep* van G. Omdat $[G,G]$ in het bijzonder onder alle inwendige automorfismen $\sigma \in \mathrm{Inn}(G)$ op zijn plaats wordt gelaten is het een normale ondergroep van G.

Het quotiënt $G_{\mathrm{ab}} = G/[G,G]$ heet de *abels gemaakte* G. Immers, per definitie van de commutatorondergroep geldt voor ieder tweetal elementen $\overline{x}, \overline{y} \in G_{\mathrm{ab}}$ de relatie $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \overline{e}$, en dus $\bar{x}\bar{y} = \bar{y}\bar{x}$. Men noemt G_{ab} ook wel het *maximale abelse quotiënt* van G. Is G zelf abels, dan geldt $[G,G] = \{e\}$ en $G_{\mathrm{ab}} = G$.

Opgave 4. Laat zien dat G/N abels is dan en slechts dan als $N \supset [G,G]$ geldt.

Ieder homomorfisme $f : G \to A$ naar een *abelse* groep A stuurt de commutatoren van G naar het eenheidselement $e_A \in A$:

$$f([x,y]) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = f(x)f(x)^{-1}f(y)f(y)^{-1} = e_A.$$

Er volgt dat $[G,G]$ bevat is in $\ker(f)$, en 8.4 geeft de volgende uitspraak.

8.5. Stelling. *Zij $f : G \to A$ een homomorfisme naar een abelse groep A. Dan bestaat er een homomorfisme $f_{\mathrm{ab}} : G_{\mathrm{ab}} = G/[G,G] \to A$ zodat f verkregen wordt als samenstelling*

$$G \xrightarrow{\pi} G_{\mathrm{ab}} \xrightarrow{f_{\mathrm{ab}}} A$$

van de natuurlijke afbeelding $\pi : G \to G_{\mathrm{ab}}$ met f_{ab}. □

Uit 8.5 volgt dat het geven van een homomorfisme $G \to A$ naar een abelse groep 'hetzelfde' is als het geven van een homomorfisme $G_{\mathrm{ab}} \to A$: de afbeelding $f_{\mathrm{ab}} \mapsto f_{\mathrm{ab}}\pi$ geeft een bijectie $\mathrm{Hom}(G_{\mathrm{ab}}, A) \longleftrightarrow \mathrm{Hom}(G, A)$.

8.6. Gevolg. *Ieder homomorfisme $f : S_n \to A$ naar een abelse groep A is de samenstelling*

$$S_n \xrightarrow{\varepsilon} \{\pm 1\} \xrightarrow{\overline{f}} A$$

van de tekenafbeelding ε met een homomorfisme $\overline{f} : \{\pm 1\} \to A$. □

Bewijs. Met het oog op 8.5 is het voldoende te bewijzen dat de alternerende groep $A_n = \ker \varepsilon$ gelijk is aan de commutatorondergroep van S_n. Omdat iedere commutator $xyx^{-1}y^{-1}$ in S_n een even permutatie is geldt $[S_n, S_n] \subset A_n$. Voor de andere inclusie is het wegens 2.10 voldoende iedere 3-cykel als commutator te schrijven. Voor $n \leq 2$ is er niets te bewijzen, voor $n \geq 3$ laat de identiteit

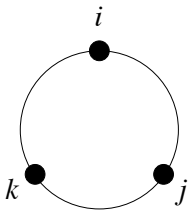
$$[(a\ b), (a\ c)] = (a\ b)(a\ c)(a\ b)(a\ c) = (a\ b\ c)$$

zien dat iedere 3-cykel een commutator is. Dit geeft $A_n = [S_n, S_n]$. □

8.7. Voorbeeld. De *quaternionengroep* Q van Hamilton, genoemd naar de Ier William Rowan Hamilton (1805–1865), bestaat uit de acht elementen ± 1, $\pm i$, $\pm j$ en $\pm k$ en heeft een groepsstructuur die vastgelegd wordt door de identiteiten

$$i^2 = j^2 = k^2 = ijk = -1 \quad \text{en} \quad (-1)^2 = 1.$$

De rekenregel die men hieruit voor de elementen i, j en k van orde 4 kan distilleren is dat het product van twee van hen, langs onderstaande cirkel 'met de klok mee' genomen, de derde geeft. Dus: $jk = i$ en $ki = j$. Tegen de klok in krijgen we tegengestelde uitkomsten: $kj = -i$ en $ik = -j$.



Het element -1, dat een macht van zowel i als j is, commuteert met alle elementen van $Q = \langle i, j \rangle$. Het is een voortbrenger van het centrum $Z(Q) = \{\pm 1\}$ van Q.

Ook de commutatorondergroep $[Q, Q]$ is gelijk aan $\{\pm 1\}$, want ieder tweetal niet-commuterende elementen van Q heeft commutator -1. In de quotiëntgroep $Q/[Q, Q]$ hebben de drie niet-triviale elementen $\overline{i}$, $\overline{j}$ en $\overline{k}$ elk orde 2, en het product van twee van hen is gelijk aan de derde. Kennelijk is de abels gemaakte quaternionengroep Q^{ab} isomorf met de viergroep van Klein V_4.

***Opgave 5.** Laat zien dat Q precies 24 verschillende automorfismen heeft. Welke groep is $\mathrm{Aut}(Q)$?

Op de 4-dimensionale reële vectorruimte $\mathbf{H} = \mathbf{R} \cdot 1 + \mathbf{R} \cdot i + \mathbf{R} \cdot j + \mathbf{R} \cdot k$ ligt behalve de bekende vectoroptelling een natuurlijke *niet-commutatieve* ringstructuur. Vermenigvuldiging in deze *quaternionenalgebra* van Hamilton, die het lichaam van de complexe getallen $\mathbf{C} = \mathbf{R} \cdot 1 + \mathbf{R} \cdot i$ als deelring bevat, verloopt door systematisch toepassen van

de distributieve eigenschap (R3) uit 6.8 en de vermenigvuldigingsregels voor i, j en k:

$$\begin{aligned}(a+bi+cj+dk)\cdot(a'+b'i+c'j+d'k) = \\ (aa'-bb'-cc'-dd') \ +(ab'+a'b+cd'-c'd)i+ \\ (ac'+a'c+db'-d'b)j+(ad'+a'd+bc'-b'c)k.\end{aligned}$$

In het kader van deze syllabus gaan we niet verder op deze ring in.

▶ Direct product

De voorafgaande stellingen in deze paragraaf illustreren het bekende groepentheoretische feit dat men een groep G vaak kan bestuderen via zijn quotiënten G/N voor geschikte normaaldelers $N \triangleleft G$. In de meeste gevallen zijn N en G/N elk van beide 'kleiner' en dus 'makkelijker' dan G zelf. We gaan in de rest van de paragraaf in op de belangrijke vraag in hoeverre men G kan 'reconstrueren' uit een normaaldeler N en het bijbehorende quotiënt G/N. In sommige gevallen kan men G terugkrijgen als 'product' van N en G/N. We bekijken eerst algemene producten van groepen.

De eenvoudigste manier om uit twee groepen G_1 en G_2 een product-groep te maken wordt gegeven door de constructie van het *directe product* $G_1 \times G_2$. Deze constructie zijn we al eerder tegengekomen in de Chinese reststelling 6.15. Dit laat al zien dat de vorming van producten niet alleen voor groepen mogelijk is, maar ook voor andere categorieën van objecten.

Als verzameling is de groep $G_1 \times G_2$ het cartesisch product

$$G_1 \times G_2 = \{(x_1, x_2) : \ x_1 \in G_1, x_2 \in G_2\},$$

en men neemt hierop als bewerking de coördinaatsgewijze vermenigvuldiging

$$(x_1, x_2)\cdot(y_1, y_2) = (x_1y_1, x_2y_2).$$

Dit geeft een groep met als eenheidselement (e_1, e_2). De inverse van (x_1, x_2) is het element (x_1^{-1}, x_2^{-1}). Op soortgelijke manier kan men producten

$$\textstyle\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n$$

van n groepen definiëren: men neemt het cartesisch product van de verzamelingen en voert groepsoperaties coördinaatsgewijs uit. De *projectie*: $\pi_i : G_1 \times G_2 \times \ldots \times G_n \to G_i$ op de i-de coördinaat is voor alle i een surjectief groepshomomorfisme. Het n-voudig product van een groep met zichzelf wordt vaak als G^n genoteerd. Zo is bijvoorbeeld het product $C_2^2 = C_2 \times C_2$ van de cyclische groep van orde 2 met zichzelf een abelse groep van orde 4 waarin alle elementen voldoen aan $x^2 = e$. Uit §1 weten we dat dit betekent dat $C_2 \times C_2$ isomorf is met de viergroep van Klein V_4.

Voor additief genoteerde abelse groepen A_1 en A_2 noemt men het directe product liever de *directe som* en schrijft $A_1 \oplus A_2$. De optelgroep van de vectorruimte $\mathbf{R}^n$ is een directe som van n exemplaren van de optelgroep $\mathbf{R}$ met zichzelf. Iedere basiskeuze

in een reële vectorruimte V van dimensie n is in feite de keuze van een isomorfisme $\mathbf{R}^n \xrightarrow{\sim} V$. Een vectorruimte is dan ook op vele manieren isomorf met een directe som van 1-dimensionale deelruimtes.

De productgroep $G_1 \times G_2$ bevat ondergroepen $G_1 \times 1$ en $1 \times G_2$ die isomorf zijn met G_1 en G_2, en vaak met G_1 en G_2 geïdentificeerd worden. Om een groep G als een product van kleinere groepen te schrijven moet men dus ondergroepen $H_1, H_2 \subset G$ vinden waarvoor er een isomorfisme $H_1 \times H_2 \xrightarrow{\sim} G$ is gegeven door 'uitvermenigvuldigen van coördinaten': $(x, y) \mapsto xy$. Is bijvoorbeeld $G = V_4 = \{e, a, b, c\}$ de viergroep van Klein, dan zijn $H_1 = \langle a \rangle$ en $H_2 = \langle b \rangle$ cyclische ondergroepen van orde 2, en men kan het isomorfisme $C_2 \times C_2 \xrightarrow{\sim} V_4$ expliciet maken door

$$\langle a \rangle \times \langle b \rangle \xrightarrow{\sim} V_4$$

te definiëren door $(x, y) \mapsto xy$. Om algemener te kunnen constateren dat een groep verkregen kan worden als direct product van twee ondergroepen is de volgende stelling nuttig.

8.8. Stelling. *Laat H_1 en H_2 ondergroepen van G zijn waarvoor het volgende geldt:*

1. $H_1 \cap H_2 = 1$;
2. $H_1 H_2 = \{h_1 h_2 : \ h_1 \in H_1 \text{ en } h_2 \in H_2\} = G$;
3. *voor $h_1 \in H_1$ en $h_2 \in H_2$ geldt $h_1 h_2 = h_2 h_1$.*

Dan definieert de afbeelding $(h_1, h_2) \mapsto h_1 h_2$ een groepsisomorfisme

$$H_1 \times H_2 \xrightarrow{\sim} G.$$

Er zijn surjecties $\pi_1 : G \to H_1$ en $\pi_2 : G \to H_2$ met $\ker \pi_1 = H_2$ en $\ker \pi_2 = H_1$.

Bewijs. Laat $f : H_1 \times H_2 \to G$ de aangegeven afbeelding zijn. Eigenschap (3) impliceert dat f een homomorfisme is:

$$f((h_1, h_2)(\tilde{h}_1, \tilde{h}_2)) = f(h_1\tilde{h}_1, h_2\tilde{h}_2) = h_1\tilde{h}_1 \cdot h_2\tilde{h}_2 = h_1 h_2 \cdot \tilde{h}_1\tilde{h}_2 = f((h_1, h_2))f((\tilde{h}_1, \tilde{h}_2)).$$

Voor $(h_1, h_2) \in \ker(f)$ geldt $h_1 h_2 = e$, dus $h_1 = h_2^{-1} \in H_1 \cap H_2 = 1$. Dit geeft $(h_1, h_2) = (e, e)$, en f is injectief wegens 4.4. Wegens (2) is f tevens surjectief, dus een isomorfisme. De genoemde surjecties zijn de 'projecties op de coördinaten' gegeven door $\pi_1 : h_1 h_2 \mapsto h_1$ en $\pi_2 : h_1 h_2 \mapsto h_2$. □

Opgave 6. Laat zien dat we conditie 3 in stelling 8.8 kunnen vervangen door 'H_1 en H_2 zijn normaal in G'.

Opgave 7. Generaliseer 8.8 voor isomorfismen $H_1 \times H_2 \times \ldots \times H_n \xrightarrow{\sim} G$.

8.9. Voorbeelden. 1. De multiplicatieve groep $\mathbf{R}^*$ bevat een tekenondergroep $\{\pm 1\}$ en een ondergroep $\mathbf{R}_{>0}$ van positieve reële getallen die aan de eisen in 8.8 voldoen. Dit geeft een isomorfisme $\{\pm 1\} \times \mathbf{R}_{>0} \xrightarrow{\sim} \mathbf{R}^*$.

2. Op soortgelijke manier is de multiplicatieve groep van de complexe getallen $\mathbf{C}^*$ te krijgen als een product $\mathbf{C}^* \cong \mathbf{T} \times \mathbf{R}_{>0}$ van de cirkelgroep $\mathbf{T} = \{z \in \mathbf{C}^* : |z| = 1\}$ met $\mathbf{R}_{>0}$. Het isomorfisme voor $\mathbf{R}^*$ wordt hieruit door beperking verkregen.

3. De groep K van symmetrieën van de kubus heeft een ondergroep K^+ van draaiingssymmetrieën en een ondergroep $\langle -1\rangle$ voortgebracht door de centrale puntspiegeling -1. We zagen al in §5 dat deze ondergroepen van K voldoen aan de eisen 8.8.1 en 8.8.2. Om te laten zien dat ook 8.8.3 geldt vatten we de draaiingssymmetrieën op als lineaire afbeeldingen $\mathbf{R}^3 \to \mathbf{R}^3$ door het middelpunt van de kubus als oorsprong in $\mathbf{R}^3$ te kiezen. De centrale puntspiegeling wordt dan de scalaire vermenigvuldiging met -1, die met *alle* lineaire afbeeldingen commuteert. Voor de kubusgroep geldt dus

$$K \cong \langle -1\rangle \times K^+ \cong C_2 \times S_4.$$

4. Zij A een abelse groep van orde mn, met $m, n \in \mathbf{Z}_{>0}$ *onderling ondeelbare* getallen. Omdat A abels is, zijn

$$A_m = \{a \in A : a^m = 1\} \qquad \text{en} \qquad A_n = \{a \in A : a^n = 1\}$$

ondergroepen van A. Er geldt $A_m \cap A_n = 1$, want een element waarvan de orde zowel m als n deelt heeft orde $\gcd(m, n) = 1$. Kiezen we $x, y \in \mathbf{Z}$ met $nx + my = 1$, dan laat een element $a \in A$ zich schrijven als $a = a^{nx+my} = a^{nx} \cdot a^{my}$. Nu geldt $a^{nx} \in A_m$, immers $(a^{nx})^m = a^{mnx} = 1$, en evenzo $a^{my} \in A_n$. Er volgt dat A_m en A_n voldoen aan de eisen van stelling 8.8, en we vinden $A \cong A_m \times A_n$. Omdat de orde van A_m copriem is met n (waarom?) en die van A_n copriem met m volgt door het vergelijken van ordes $\#A_m = m$ en $\#A_n = n$.

Passen we de 'ontbinding' van A in voorbeeld 8.9.4 herhaald toe, dan vinden we dat iedere eindige abelse groep van orde $n = \prod_p p^{n_p}$ het product is van abelse groepen van orde p^{n_p}. In termen van de aan het einde van §5 geïntroduceerde Sylow-p-ondergroepen luidt de conclusie als volgt.

8.10. Stelling. *Iedere eindige abelse groep is het directe product van zijn Sylow-p-ondergroepen.* □

▶ Semi-direct product

De ondergroepen H_1 en H_2 in 8.8 zijn als kernen van de projectieafbeeldingen π_1 en π_2 beide normaal in G. Grof gezegd komt stelling 8.8 er op neer dat als we $G/H_1 = H_2$ en $G/H_2 = H_1$ hebben de groep G een direct product van H_1 en H_2 is.

In veel situaties is de eis dat H_1 en H_2 beide normaal zijn in G niet vervuld, en is slechts één van beide groepen het quotiënt van G modulo de ander. In deze asymmetrische situatie hebben we een normaaldeler $N \subset G$ en een ondergroep $H \subset G$ waarvoor de natuurlijke afbeelding $H \to G/N$ een isomorfisme is. In dit geval kan men G beschrijven als *semi-direct product* van N en H.

De definitie van het semi-directe product ziet er bij eerste kennismaking enigszins ingewikkeld uit, en daarom kijken we eerst eens naar het voorbeeld van de groep $I_2(\mathbf{R})$ van vlakke isometrieën uit §3. Deze groep bevat een ondergroep T van translaties en een orthogonale ondergroep $O_2(\mathbf{R})$ van lineaire isometrieën. De identiteit is het enige element in de doorsnijding van deze ondergroepen, en in 3.3.1 bewezen we dat elk

element $\varphi \in I_2(\mathbf{R})$ op een unieke manier te schrijven is als een product $\varphi = \tau\psi$ van een translatie τ en een orthogonale afbeelding ψ. Aan de eisen (1) en (2) uit 8.8 is nu voldaan, maar niet aan (3). Het nemen van de lineaire component uit 3.9 induceert namelijk wel een 'projectieafbeelding' $L : I_2(\mathbf{R}) \to O_2(\mathbf{R})$ met kern T, maar de situatie is niet symmetrisch in T en $O_2(\mathbf{R})$ omdat uit 3.10 volgt dat T wel, maar $O_2(\mathbf{R})$ niet normaal is in I_2. Dat betekent dat de correspondentie $\tau\psi \leftrightarrow (\tau, \psi)$ weliswaar een bijectie

$$I_2(\mathbf{R}) \leftrightarrow T \times O_2(\mathbf{R})$$

oplevert, maar dat de groepsoperatie op $I_2(\mathbf{R})$ *niet* met de groepsoperatie op het directe product correspondeert. Om te kijken wat de 'goede' groepsoperatie op $T \times O_2(\mathbf{R})$ is kijken we wat beter naar de in (3.10) gegeven relatie

$$\psi\tau_x\psi^{-1} = \tau_{\psi(x)}.$$

Deze relatie zegt dat, indien we T op de voor de hand liggende manier met $\mathbf{R}^2$ identificeren, de *conjugatiewerking* van $O_2(\mathbf{R})$ op $T = \mathbf{R}^2$ 'hetzelfde' is als de *natuurlijke werking* van $O_2(\mathbf{R})$ op $\mathbf{R}^2$. Met behulp van deze kennis kunnen we toch expliciet producten van translaties en orthogonale afbeeldingen vermenigvuldigen:

$$\tau_{x_1}\psi_1 \cdot \tau_{x_2}\psi_2 = \tau_{x_1}(\psi_1\tau_{x_2}\psi_1^{-1}) \cdot \psi_1\psi_2 = \tau_{x_1}\tau_{\psi_1(x_2)} \cdot \psi_1\psi_2. \tag{8.11}$$

De vermenigvuldiging op de 'orthogonale component' is dus de gewone vermenigvuldiging, maar de vermenigvuldiging op de 'translatiecomponent' niet. De aanwezigheid van een niet-triviale conjugatiewerking van $O_2(\mathbf{R})$ op T maakt de groepsoperatie 8.11 op $T \times O_2(\mathbf{R})$ tot een voorbeeld van *semi-directe vermenigvuldiging.*

Men kan heel algemeen semi-directe producten maken door een groep H te laten 'werken' op een groep N. Hiermee bedoelen we dat we voor elk element $h \in H$ een automorfisme $\sigma_h \in \mathrm{Aut}(N)$ hebben, en dat, net als in het geval van conjugatiewerkingen, de identiteit $\sigma_{h_1}\sigma_{h_2} = \sigma_{h_1h_2}$ geldt. Dit laatste betekent niets anders dan dat de afbeelding $\sigma : H \to \mathrm{Aut}(N)$ gegeven door $h \mapsto \sigma_h$ een groepshomomorfisme is. Men brengt dit wel suggestief tot uitdrukking door de 'exponentiële notatie' $\sigma_h(n) = {}^h n$ te gebruiken met de rekenregel ${}^{h_1}({}^{h_2}n) = {}^{h_1h_2}n$.

8.12. Propositie. *Laat N en H groepen zijn, $\sigma : H \to \mathrm{Aut}(N)$ een homomorfisme en schrijf $\sigma(h)(n) = {}^h n$. Dan definieert de bewerking*

$$(n_1, h_1)(n_2, h_2) = ({n_1}^{h_1}n_2,\ h_1h_2)$$

een groepsbewerking op de productverzameling $N \times H$.

Bewijs. De definitie is zo gekozen dat hij een situatie zoals die in het geval van $I_2(\mathbf{R})$ optreedt precies imiteert. Als we N en H als deelverzamelingen van $N \times H$ opvatten via $n \mapsto (n, e_H)$ en $h \mapsto (e_N, h)$, dan induceert de gegeven bewerking de 'gewone' vermenigvuldiging op N en H, en ieder groepselement is te schrijven als een product

$(n,h) = (n,e_H)(e_N,h) = nh$. Het automorfisme $\sigma(h) \in \mathrm{Aut}(N)$ is nu letterlijk de conjugatie met h geworden:

$$hnh^{-1} = (e_N,h)(n,e_H)(e_N,h^{-1}) = ({}^h n, e_H) = {}^h n = \sigma(h)(n).$$

Dit betekent dat we producten van de vorm nh kunnen vermenigvuldigen door ze eerst gewoon achter elkaar te zetten en vervolgens met het 'conjugatiefoefje' 8.11 alle h's naar rechts te werken. Het eenheidselement is $e = (e_N, e_H)$, en men vindt de inverse van (n,h) uit $(nh)^{-1} = h^{-1}n^{-1} = {}^{h^{-1}}(n^{-1})h^{-1}$ als $({}^{h^{-1}}(n^{-1}), h^{-1})$. De lezer mag bij wijze van oefening zelf de associatieve eigenschap nagaan. □

De in 8.12 verkregen groep heet het *semi-directe product* van N en H met betrekking tot de afbeelding σ en wordt genoteerd als $N \rtimes_\sigma H$ of kortweg $N \rtimes H$. Is $\sigma : H \to \mathrm{Aut}(N)$ het triviale homomorfisme, dan geldt steeds ${}^h n = n$ en is het semi-directe product niets anders dan het directe product.

Men vat N en H als in het bewijs van 8.12 op als ondergroepen van $N \rtimes H$. De ondergroep N, die invariant is onder conjugatie met elementen uit zowel N als H, is normaal in $N \rtimes H$. Het symbool $\rtimes$, dat verband houdt met het symbool $\lhd$, brengt dit feit tot uitdrukking. Het analogon van 8.8 voor semi-directe producten luidt als volgt.

8.13. Stelling. *Laat N en H ondergroepen van G zijn waarvoor het volgende geldt:*

1. $N \cap H = 1$;
2. $NH = \{nh : \ n \in N \text{ en } h \in H\} = G$;
3. *N is normaal in G.*

Is nu $\sigma : H \to \mathrm{Aut}(N)$ de afbeelding die de conjugatiewerking van H op N beschrijft, dan definieert de afbeelding $(n,h) \mapsto nh$ een groepsisomorfisme

$$N \rtimes_\sigma H \xrightarrow{\sim} G.$$

De afbeelding $nh \mapsto h$ geeft een surjectie $G \to H$ met kern N.

Bewijs. Het semi-directe product is precies zo gedefinieerd dat de afbeelding in kwestie een homomorfisme is. Hij is injectief wegens (1) en surjectief wegens (2), dus een isomorfisme. Uit 8.12 volgt dat de projectie op de H-component een surjectief homomorfisme is, en de kern hiervan is duidelijk N. □

Opgave 8. Laat zien dat H in 8.13 alleen normaal is in G als σ triviaal is, en dat in dat geval G het directe product van N en H is.

Stelling 8.13 is veel algemener toepasbaar dan 8.8 omdat we alleen '$G/N = H$' eisen, en niet ook nog eens '$G/H = N$'. Het verkregen product $N \rtimes_\sigma H$ is echter daardoor niet 'symmetrisch' in N en H.

8.14. Voorbeelden. 1. De *affiene groep* $\mathrm{Aff}(\mathbf{R})$ is de ondergroep van $S(\mathbf{R})$ bestaande uit de bijecties

$$\{x \mapsto ax + b : \ a \in \mathbf{R}^*, b \in \mathbf{R}\}.$$

Men krijgt ondergroepen $H = \mathbf{R}^*$ en $N = \mathbf{R}$ door $a \in \mathbf{R}^*$ en $b \in \mathbf{R}$ te laten corresponderen met respectievelijk de afbeeldingen $\sigma_a : x \mapsto ax$ en $\tau_b : x \mapsto x+b$. De doorsnijding

van beide ondergroepen bevat slechts de identiteit, en iedere affiene afbeelding is de unieke samenstelling van een vermenigvuldiging $x \mapsto ax$ en een translatie $x \mapsto x + b$. De ondergroep $\mathbf{R}$ van translaties is normaal, en de conjugatiewerking van $\mathbf{R}^*$ op $\mathbf{R}$ in $\mathrm{Aff}(\mathbf{R})$ is de natuurlijke vermenigvuldiging:

$$(\sigma_a \tau_b \sigma_a^{-1})(x) = a(a^{-1}x + b) = x + ab = \tau_{ab}(x).$$

We concluderen dat $\mathrm{Aff}(\mathbf{R})$ een semi-direct product $\mathbf{R} \rtimes \mathbf{R}^*$ is met betrekking tot de afbeelding $\mathbf{R}^* \to \mathrm{Aut}(\mathbf{R})$ gegeven door $a \mapsto \sigma_a$.

2. De dihedrale groep D_n bevat een normale ondergroep $N = C_n$ van index 2 voortgebracht door een rotatie ρ van orde n en een ondergroep $H = C_2 = \langle \sigma \rangle$ van orde 2 voortgebracht door een spiegeling. Ieder element is een uniek product van een element uit C_n en een element uit C_2, en de conjugatiewerking van het niet-triviale element C_2 op C_n wordt wegens (3.6) beschreven door de identiteit $\sigma\rho\sigma = \rho^{-1}$. Dit laatste betekent dat de bijbehorende afbeelding $C_2 \to \mathrm{Aut}(C_n)$ de voortbrenger van C_2 naar het automorfisme van C_n stuurt dat alle elementen inverteert. We vinden dat

$$D_n \cong C_n \rtimes C_2$$

een semi-direct product is van een cyclische groep van orde n met een groep van orde 2 die werkt door *inversie*. Algemener kan men voor iedere abelse groep A een *gegeneraliseerde diëdergroep* $A \rtimes C_2$ construeren door C_2 via inversie op A te laten werken.

3. In 8.3.2 zagen we dat de symmetrische groep S_4 een normaaldeler $N = V_4$ en een ondergroep $H = S_3$ bevat die aan de voorwaarden van 8.13 voldoen. De conjugatieactie $\sigma : S_3 \to \mathrm{Aut}(V_4)$ van S_3 op V_4 is (cf. opgave 4.35) een isomorfisme. Het verkregen isomorfisme

$$S_4 \cong V_4 \rtimes S_3 \cong V_4 \rtimes \mathrm{Aut}(V_4)$$

laat zien dat S_4 uit V_4 geconstrueerd kan worden door het semi-directe product van V_4 te nemen met zijn eigen automorfismengroep.

4. Voor iedere groep G kan men het product $G \rtimes \mathrm{Aut}(G)$ met betrekking tot de natuurlijke actie van $\mathrm{Aut}(G)$ op G vormen.

Voor de cyclische groep $G = \mathbf{Z}/n\mathbf{Z}$ geldt

$$\mathrm{Aut}(G) = (\mathbf{Z}/n\mathbf{Z})^*. \tag{8.15}$$

Immers, een element $\sigma \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$ met $\sigma(\bar{1}) = \bar{a}$ wordt gegeven door $\sigma(\bar{x}) = \overline{ax}$. Alleen voor $\bar{a} \in (\mathbf{Z}/n\mathbf{Z})^*$ is σ een automorfisme, en dit geeft de identificatie $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) = (\mathbf{Z}/n\mathbf{Z})^*$. Het semidirecte product $G \rtimes \mathrm{Aut}(G) = \mathbf{Z}/n\mathbf{Z} \rtimes (\mathbf{Z}/n\mathbf{Z})^*$, dat het analogon van 8.14.1 is voor de *ring* $\mathbf{Z}/n\mathbf{Z}$ in de plaats van $\mathbf{R}$, heet de *affiene groep* $\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ over $\mathbf{Z}/n\mathbf{Z}$.

Opgave 9. Bewijs: er zijn isomorfismen $\mathrm{Aff}(\mathbf{Z}/3\mathbf{Z}) \cong S_3$ en $\mathrm{Aff}(\mathbf{Z}/4\mathbf{Z}) \cong D_4$.

Opgaven.

10. Zij $f : G \to G'$ een homomorfisme en $N' \lhd G'$ een normaaldeler. Bewijs: $N = f^{-1}[N']$ is normaal in G. Laat tevens zien dat een surjectief homomorfisme f een isomorfisme $G/N \xrightarrow{\sim} G'/N'$ induceert.

11. Bepaal alle ondergroepen van A_4, en ga na welke van deze ondergroepen normaal zijn.

12. Geef een voorbeeld van een groep G met ondergroepen H_1 en H_2 waarvoor $H_1 \lhd H_2$ en $H_2 \lhd G$ geldt, maar *niet* $H_1 \lhd G$.

13. Zij D_n de dihedrale groep van orde $2n$ uit §3, en $\rho \in D_n$ een rotatie van orde n. Bewijs dat $[D_n, D_n]$ wordt voortgebracht door ρ^2, en leid hieruit af

$$(D_n)_{\mathrm{ab}} \cong \begin{cases} \{\pm 1\} & \text{als } n \text{ oneven is;} \\ V_4 & \text{als } n \text{ even is.} \end{cases}$$

14. Bepaal de ondergroepen van index 2 in D_n voor $n \geq 1$.

15. Bepaal het aantal elementen in $\mathrm{Hom}(S_n, \mathbf{C})$, $\mathrm{Hom}(S_n, \mathbf{C}^*)$ en $\mathrm{Hom}(D_n, \mathbf{C}^*)$ voor $n \geq 1$.

16. Zij A een additief geschreven abelse groep en $n \geq 2$ geheel. Geef een expliciete bijectie aan tussen $\mathrm{Hom}(S_n, A)$ en de 2-torsieondergroep $A[2] = \{a \in A : 2a = 0\}$ van A.

17. Zij G een groep en $N \subset G$ de ondergroep voortgebracht door $S = \{g^2 : g \in G\}$. Bewijs: N is normaal in G en G/N is abels.

18. Bereken de commutator $[(1\ 2\ 3), (1\ 4\ 5)] \in A_5$, en bewijs dat voor $n \geq 5$ de commutatorondergroep $[A_n, A_n]$ gelijk is aan A_n.

19. Bepaal $[A_n, A_n]$ voor $n \leq 4$.

20. Bepaal het aantal elementen in $\mathrm{Hom}(A_n, \mathbf{C}^*)$ voor $n \geq 1$.

21. Zij $f : G \to G'$ een homomorfisme. Bewijs dat er een homomorfisme $f_{\mathrm{ab}} : G_{\mathrm{ab}} \to G'_{\mathrm{ab}}$ bestaat zo dat het diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow & & \downarrow \\ G_{\mathrm{ab}} & \xrightarrow{f_{\mathrm{ab}}} & G'_{\mathrm{ab}} \end{array}$$

met natuurlijke verticale pijlen commuteert.
[Men zegt wel dat het abels maken van een groep *functorieel* is: niet alleen de groepen kunnen abels gemaakt worden, maar ook de afbeeldingen ertussen.]

22. Laat H_1 en H_2 eindige ondergroepen van G zijn met $H_1 \cap H_2 = 1$. Bewijs dat het aantal elementen van de verzameling $H_1H_2 = \{h_1h_2 : h_1 \in H_1 \text{ en } h_2 \in H_2\}$ gelijk is aan $\#H_1 \cdot \#H_2$. Laat zien dat H_1H_2 een ondergroep van G is indien G abels is, en geef een niet-abels voorbeeld waarin dit niet zo is.

23. Laat N_1 en N_2 normaaldelers van G zijn met $N_1 \cap N_2 = 1$. Bewijs: voor $n_1 \in N_1$ en $n_2 \in N_2$ geldt $n_1n_2 = n_2n_1$. Leid hieruit af dat G een ondergroep bevat die isomorf is met $N_1 \times N_2$.

24. Laat N_1 en N_2 als in de vorige opgave zijn. Bewijs dat $G/N_1 \times G/N_2$ een ondergroep bevat die isomorf is met G.

25. Laat zien dat er een natuurlijke bijectie $\mathrm{Hom}(X, G_1 \times G_2) \leftrightarrow \mathrm{Hom}(X, G_1) \times \mathrm{Hom}(X, G_2)$ is voor ieder drietal groepen G_1, G_2, X. Geldt iets soortgelijks voor $\mathrm{Hom}(G_1 \times G_2, X)$?

26. Zij $\mathrm{SL}_3(\mathbf{R})$ de groep van matrices van determinant 1 in $\mathrm{GL}_3(\mathbf{R})$. Bewijs: er is een isomorfisme
$$\mathbf{R}^* \times \mathrm{SL}_3(\mathbf{R}) \xrightarrow{\sim} \mathrm{GL}_3(\mathbf{R}).$$
Is de dimensie 3 hiervoor van belang?

27. Bepaal het centrum $Z(K)$ van de kubusgroep.

28. Geef een voorbeeld van een groep G met
    a. isomorfe normaaldelers N_1 en N_2 waarvoor G/N_1 en G/N_2 niet isomorf zijn;
    b. niet-isomorfe normaaldelers N_1 en N_2 waarvoor G/N_1 en G/N_2 isomorf zijn.

29. Laat zien dat er voor $n > 2$ een injectief homomorfisme $D_n \to \mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ bestaat, en dat dit alleen een isomorfisme is voor $n \in \{3, 4, 6\}$.

30. Laat zien de affiene groep $\mathrm{Aff}(\mathbf{R})$ isomorf is met de matrixgroep
$$\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbf{R}^*, b \in \mathbf{R}\} \subset \mathrm{GL}_2(\mathbf{R}).$$

31. Laat zien dat de matrixgroep $\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) : a \in \mathbf{R}^*, b \in \mathbf{R}\} \subset \mathrm{GL}_2(\mathbf{R})$ isomorf is met een direct product $\mathbf{R}^* \times \mathbf{R}$.

*32. Laat zien dat $\mathrm{SL}_2(\mathbf{R})$ wordt voortgebracht door de matrices van de vorm $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ en $\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right)$ met $x \in \mathbf{R}$.

33. Bepaal $[\mathrm{GL}_2(\mathbf{R}), \mathrm{GL}_2(\mathbf{R})]$, en laat zien dat ieder homomorfisme $f : \mathrm{GL}_2(\mathbf{R}) \to A$ naar een abelse groep A factoriseert via de determinantafbeelding $\det : \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}^*$.
[Hint: bereken commutatoren als $[\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} y & 0 \\ 0 & y^{-1} \end{smallmatrix}\right)]$ en gebruik de vorige opgave.]

34. Laat zien dat S_n voor $n \geq 2$ isomorf is met een semi-direct product $A_n \rtimes C_2$, en dat de conjugatiewerking $\sigma : C_2 \to \mathrm{Aut}(A_n)$ afhangt van de keuze van de ondergroep $C_2 \subset S_n$.

35. Is in een semi-direct product $G = N \rtimes H$ iedere normaaldeler $N' \lhd N$ ook een normaaldeler van G?

36. Zij A een abelse groep en $G = A \rtimes C_2$ de corresponderende gegeneraliseerde diëdergroep uit 8.14.2.
    1. Laat zien dat iedere ondergroep $H \subset A$ normaal is in G.
    2. Bepaal het centrum $Z(G)$ van G.
    3. Bepaal de abels gemaakte groep G_{ab}.

37. *(Lemma van Goursat)*[34] Laat $H \subset G_1 \times G_2$ een ondergroep zijn, en neem aan dat het beeld van H onder de projecties op de coördinaten gelijk is aan respectievelijk G_1 en G_2. Definieer
$$N_1 = \{g_1 \in G_1 : (g_1, e_2) \in H\} \qquad \text{en} \qquad N_2 = \{g_2 \in G_2 : (e_1, g_2) \in H\}.$$
Bewijs dat N_1 en N_2 normaal zijn in respectievelijk G_1 en G_2, en dat H de 'grafiek' is van een isomorfisme $\phi : G_1/N_1 \xrightarrow{\sim} G_2/N_2$. Dit laatste betekent:
$$H = \{(g_1, g_2) \in G_1 \times G_2 : \ \phi(g_1 N_1) = g_2 N_2\}.$$

38. Bewijs dat alle ondergroepen van $C_5 \times S_4$ van de vorm $1 \times H$ en $C_5 \times H$ zijn, met H een ondergroep van S_4.

39. Bepaal het aantal ondergroepen van $C_5 \times C_5$ en van $C_5 \times C_{25}$.

40. Zij $f : S_m \to S_n$ een homomorfisme. Bewijs: $f[A_m] \subset A_n$.

41. Zij G^n het n-voudig product van G met zichzelf, en laat C_n als in het bewijs van 5.14 werken op G^n door cyclisch opschuiven. Laat zien dat dit aanleiding geeft tot een semi-direct product $G^n \rtimes C_n$, het *kransproduct* $G \wr C_n$ van G met C_n. Welke groep is $C_2 \wr C_2$?

9 Abelse groepen

De productconstructies uit de voorafgaande paragraaf stellen ons in staat groepen te construeren als (semi-)direct product van kleinere groepen. Lastiger is het om in te zien dat een gegeven groep G op deze manier uit kleinere groepen 'samengesteld' is. Het probleem komt neer op het vinden van een normaaldeler $N \lhd G$ en een 'complement' $H \cong G/N$ in G waarop stelling 8.13 van toepassing is. Een techniek die men hiervoor kan gebruiken is het zogenaamde *splitsen van exacte rijtjes*. Deze techniek[35], die voornamelijk een kwestie van efficient taalgebruik is, zal ook in de context van modulen en vectorruimtes een nuttige aanwinst blijken te zijn.

In deze paragraaf richten we ons voornamelijk op het eenvoudigere geval van *abelse* groepen. Voor *eindig voortgebrachte* abelse groepen zullen we een complete structuurstelling 9.11 bewijzen. Voor niet-abelse groepen is het vinden van normaaldelers een moeilijker probleem, dat in §10 aan de orde komt.

▶ Exacte rijtjes

Gegeven groepshomomorfismen $f : A \to B$ en $g : B \to C$ zeggen we dat het rijtje

$$A \xrightarrow{f} B \xrightarrow{g} C$$

exact is (bij B) als $\operatorname{im} f = \ker g$ geldt: het beeld van f is de kern van g. Langere rijtjes van groepen en homomorfismen als

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \xrightarrow{f_3} A_4 \xrightarrow{f_4} A_5$$

heten exact als $\operatorname{im} f_i = \ker f_{i+1}$ geldt voor $i = 1, 2, 3$. Is $A = 1$ de triviale groep, dan betekent exactheid van het rijtje $1 \longrightarrow B \xrightarrow{g} C$ niets anders dan dat $\ker g$ alleen uit het eenheidselement bestaat. Wegens 4.4 betekent dit dat g *injectief* is. Op soortgelijke manier betekent exactheid van het rijtje $A \xrightarrow{f} B \longrightarrow 1$ dat het homomorfisme f *surjectief* is. Merk op dat we de homomorfismen van en naar de triviale groep niet hoeven te specificeren—er is geen keus. Een *kort exact rijtje* is een exact rijtje van de vorm

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1. \tag{9.1}$$

Als de afbeeldingen f en g uit de context duidelijk zijn worden ze vaak niet in het rijtje aangegeven. Wegens de isomorfiestelling 4.9 induceert het homomorfisme g in 9.1 een isomorfisme $B/f[A] \cong C$. Men zegt wel dat B een *extensie* van C met A is. Vaak vat men de injectie f op als een inclusie die A tot een ondergroep van B maakt, en schrijft dan kortweg $B/A \cong C$. Merk op dat B eindig is dan en slechts dan als A en C het zijn, en dat in dat geval $\#B = \#A \cdot \#C$ geldt.

In plaats van groepen en groepshomomorfismen kan men in het voorafgaande ook vectorruimtes en lineaire afbeeldingen beschouwen. De nulruimte, kortweg met 0 aangegeven, speelt dan de rol van de triviale groep. Veel uit deze paragraaf doet sterk

denken aan wat men in de lineaire algebra tegenkomt. Dat is niet zo'n wonder, want in §16 zal blijken dat vectorruimtes en abelse groepen speciale voorbeelden zijn van *modulen* over een ring.

Is G een groep en $N \triangleleft G$ normaal, dan past de quotiëntafbeelding $\pi : G \to G/N$ in een kort exact rijtje

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} G/N \longrightarrow 1.$$

We proberen nu de structuur van G uit te drukken in die van de kleinere groepen N en G/N. Voor gelukkige keuzes van N kan men soms een isomorfisme $G \cong N \times G/N$ verkrijgen, waarmee G in twee kleinere groepen is 'gesplitst'.

Het algemene probleem waar we ons mee geconfronteerd zien is, gegeven een kort exact rijtje als in 9.1, het bepalen van de structuur van B uit die van A en C. Dit is niet zonder meer mogelijk. Heeft G bijvoorbeeld een normaaldeler N van orde 2 waarvoor G/N isomorf is met de viergroep van Klein $V_4 \cong C_2 \times C_2$, dan is G een groep van orde 8 die past in een korte exacte rij

$$1 \longrightarrow C_2 \longrightarrow G \longrightarrow V_4 \longrightarrow 1.$$

Zelfs als we weten dat G abels is legt dit de isomorfieklasse van G niet vast: zowel $C_2 \times V_4 = C_2 \times C_2 \times C_2$ als $C_4 \times C_2$ passen in een dergelijk rijtje. Er bestaan dus 'echt verschillende' extensies van V_4 met C_2.

Opgave 1. Laat zien dat de diëdergroep D_4 en de quaternionengroep Q óók in dit rijtje passen.

▶ Splitsen van exacte rijtjes

Alle groepen in de rest van deze paragraaf zullen abels zijn, en om de analogieën met de lineaire algebra beter uit te laten komen zullen we deze zo veel mogelijk additief noteren. We schrijven dus kx voor de som van $k \in \mathbf{Z}$ elementen x (voor $k < 0$ neemt men $|k|$ elementen $-x$) en geven de triviale groep aan met 0. In deze additieve context schrijven we meestal $A \oplus C$ in plaats van $A \times C$. De directe som $A \oplus C$ van twee abelse groepen A en C past op een natuurlijke manier in een kort exact rijtje

$$0 \longrightarrow A \xrightarrow{\varepsilon_A} A \oplus C \xrightarrow{\pi_C} C \longrightarrow 0.$$

Hier is ε_A de inbedding $a \mapsto (a, 0)$ op de eerste coördinaat en π_C de projectie $(a, c) \mapsto c$ op de tweede coördinaat. In termen van de in §8 geïntroduceerde terminologie van commutatieve diagrammen kunnen we nu zeggen wanneer het rijtje 9.1 'in feite' het bovenstaande eenvoudige rijtje is.

9.2. Definitie. *Een kort exact rijtje* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *van abelse groepen splitst (of: is gesplitst) als er een homomorfisme* $\phi : B \longrightarrow A \oplus C$ *bestaat zo dat het diagram van groepen en homomorfismen*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}_C} & & \\
0 & \longrightarrow & A & \xrightarrow{\varepsilon_A} & A \oplus C & \xrightarrow{\pi_C} & C & \longrightarrow & 0
\end{array}$$

commuteert.

In 9.2 wordt niet geeist dat ϕ een isomorfisme is, want dit is automatisch het geval. Immers, voor $b \in \ker \phi$ geldt $g(b) = \pi_C(\phi(b)) = 0$, dus wegens exactheid $b = f(a)$ met $a \in A$. Uit $(0,0) = \phi(b) = \phi(f(a)) = (a,0)$ zien we dat $a = 0$ geldt, dus $b = 0$ en ϕ is injectief. Het beeld van ϕ bevat de ondergroep $(\phi \circ f)[A] = \varepsilon_A[A] = A \oplus 0$. Bovendien is er wegens de surjectiviteit van $g = \pi_C \circ \phi$ voor iedere $c \in C$ een element $(a,c) \in \mathrm{im}(\phi)$. Er volgt $\mathrm{im}(\phi) = A \oplus C$, dus ϕ is een isomorfisme.

Argumenten van de bovenstaande soort vallen in de categorie 'diagrammen jagen'. Ze komen veelvuldig voor in de commutatieve algebra. Zie ook opgave 9.10.

De fundamentele vraag na 9.2 is hoe je ziet of een exact rijtje splitst.

9.3. Stelling. *Voor een korte exacte rij* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *van abelse groepen zijn de volgende uitspraken equivalent.*

1. *er bestaat een homomorfisme* $p : B \to A$ *zo dat* $p \circ f = \mathrm{id}_A$;
2. *er bestaat een homomorfisme* $s : C \to B$ *zo dat* $g \circ s = \mathrm{id}_C$;
3. *de exacte rij is gesplitst.*

De homomorfismen p en s, die in den regel niet uniek zijn, heten wel een *retractie* van de injectie f en een *sectie* van de surjectie g. Zij 'splitsen' of 'splijten' de extensie B van C met A.

Bewijs van 9.3. Zij $\phi : B \xrightarrow{\sim} A \oplus C$ een splitsing van de extensie. Dan geeft de samenstelling met de projectie op de eerste coördinaat een homomorfisme $p : B \to A$ waarvoor $p \circ f$ de identiteit op A is. Evenzo geeft de samenstelling van de natuurlijke inbedding $C \to A \oplus C$ met ϕ^{-1} een sectie $C \to B$ van g. Dit laat zien dat (1) en (2) geïmpliceerd worden door (3).

Gegeven een retractie p van f als in (1) definiëren we een homomorfisme $\phi : B \to A \oplus C$ door $\phi(b) = (p(b), g(b))$. Dan passen B en ϕ in het commutatieve diagram in 9.2, dus ϕ is een isomorfisme en de rij is gesplitst.

Zij ten slotte een sectie s van g gegeven als in (2). Voor $b \in B$ hebben b en $(s \circ g)(b)$ hetzelfde beeld onder g, dus er geldt $b - (s \circ g)(b) \in \ker g = \mathrm{im}\, f$. De afbeelding $p : B \to A$ die $b \in B$ naar het element $a \in A$ met $f(a) = b - (s \circ g)(b)$ stuurt is nu een homomorfisme. Voor $b \in \mathrm{im}\, f$ geldt $(s \circ g)(b) = s(0) = 0$, dus er geldt $p(f(a)) = a$ en p is een retractie van f als in (1). Als boven volgt dat de rij splitst. □

Opgave 2. Laat zien dat de afbeelding $(a,c) \mapsto f(a) + s(c)$ een isomorfisme $A \oplus C \xrightarrow{\sim} B$ geeft voor iedere sectie s van g.

In het veel voorkomende geval dat C *cyclisch* is geeft 9.3 het volgende resultaat.

9.4. Lemma. *Zij* C *een cyclische groep met voortbrenger* c*. Dan is de exacte rij van abelse groepen*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

gesplitst dan en slechts dan als aan één van de beide volgende voorwaarden voldaan is:

1. c *heeft oneindige orde;*
2. c *heeft eindige orde* n *en de vezel* $g^{-1}(c)$ *boven* c *bevat een element van orde* n*.*

Bewijs. Wegens 9.3 splitst de rij dan en slechts dan als er een sectie $s : C = \langle c \rangle \to B$ van g bestaat. Zo'n sectie ligt vast door de keuze van een element $b = s(c) \in B$, en de vraag is of er een geschikte b bestaat.

Als c eindige orde n heeft, dan geeft niet ieder element b in de vezel $g^{-1}(c)$ boven c aanleiding tot een sectie s met $s(c) = b$. Immers, voor zo'n sectie geldt $nb = s(nc) = s(0) = 0 \in B$, dus de orde van b deelt n. Omdat de ordes van de elementen in de vezel boven c altijd veelvouden zijn van de orde van c zelf (opgave 4.16) kan een sectie alleen bestaan als er een element $b \in g^{-1}(c)$ van orde precies n bestaat. Voor zo'n element b van orde n krijgen we inderdaad een sectie door $s(kc) = kb$ te definiëren. Conclusie: de rij splitst dan en slechts dan als $g^{-1}(c)$ een element van orde n bevat.

Voor c van oneindige orde hebben we $C \cong \mathbf{Z}$ en vervalt bovengenoemde restrictie: ieder element $b \in g^{-1}(c) \subset B$ geeft een sectie s van g met $s(c) = b$, en de rij splitst. □

Opgave 3. Laat zien dat ieder kort exact rijtje van abelse groepen $0 \to A \to B \to \mathbf{Z}^n \to 0$ splitst.

Men kan 9.4 gemakkelijk generaliseren tot het geval waarin C een directe som van cyclische groepen is. De rij splitst dan en slechts dan als we elk van de voortbrengers van deze cyclische stukken kunnen 'liften' naar een element uit de corresponderende vezel dat dezelfde orde heeft. Voortbrengers van oneindige orde kan men als in voorgaande opgave altijd liften, voor voortbrengers van eindige orde kan zich het probleem voordoen dat *alle* elementen uit de vezel een te grote orde hebben. De rij splitst dan niet.

9.5. Voorbeeld. Het natuurlijke homomorfisme $g : \mathbf{Z}/6\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z}$ gegeven door $g(x \bmod 6) = x \bmod 3$ is surjectief met kern $\{0 \bmod 6, 3 \bmod 6\} \cong \mathbf{Z}/2\mathbf{Z}$ van orde 2. Om een sectie $s : \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/6\mathbf{Z}$ van g te krijgen moeten we een beeld $s(1 \bmod 3) \in \mathbf{Z}/6\mathbf{Z}$ aangeven. De elementen in de vezel $g^{-1}(1 \bmod 3) = \{1 \bmod 6, 4 \bmod 6\}$ hebben orde respectievelijk 6 en 3. Alleen $4 \bmod 6$ komt dus in aanmerking als beeld van $1 \bmod 3$, en de bijbehorende sectie $s : \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/6\mathbf{Z}$ gegeven door $s(x \bmod 3) = 4x \bmod 6$ geeft een splitsing van het exacte rijtje

$$0 \to \mathbf{Z}/2\mathbf{Z} \longrightarrow \mathbf{Z}/6\mathbf{Z} \xrightarrow{g} \mathbf{Z}/3\mathbf{Z} \to 0.$$

Het resulterende isomorfisme $\mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ is een speciaal geval van 6.15.

In de analoge situatie met $g : \mathbf{Z}/8\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}$ gegeven door $g(x \bmod 8) = x \bmod 4$ bevat de vezel $g^{-1}(1 \bmod 4) = \{1 \bmod 8, 5 \bmod 8\}$ boven $1 \bmod 4$ twee elementen van orde 8, dus *geen* element van de gezochte orde 4. In dit geval heeft g geen sectie, en met $\ker(g) = \{0 \bmod 8, 4 \bmod 8\} \cong \mathbf{Z}/2\mathbf{Z}$ krijgen we een rijtje

$$0 \to \mathbf{Z}/2\mathbf{Z} \longrightarrow \mathbf{Z}/8\mathbf{Z} \xrightarrow{g} \mathbf{Z}/4\mathbf{Z} \to 0$$

dat *niet* splitst. De groep $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ is inderdaad niet cyclisch van orde 8.

9.6. Lemma. *Een kort exact rijtje* $0 \to A \xrightarrow{(} f)B \xrightarrow{g} C \to 0$ *van eindige abelse groepen splitst als de ordes van* A *en* C *copriem zijn.*

Bewijs. Wegens 6.4 en de aanname bestaat er een veelvoud m van $\#A$ waarvoor $m \equiv 1 \bmod \#C$ geldt. Neem nu $c \in C$, en kies een willekeurig element $b \in g^{-1}(c)$ in de

vezel van g boven c. We beweren dat mb ook een element in de vezel boven c is, en dat het onafhankelijk is van de keuze van het element $b \in g^{-1}(c)$. Voor de eerste bewering merken we op dat $g(mb)-g(b) = (m-1)g(b) = (m-1)c = 0$ geldt omdat $m-1$ deelbaar is door de orde van C. Voor de tweede kiezen we twee elementen $b, b' \in g^{-1}(c)$. Dan geldt $b - b' \in \ker(g) = f[A]$, en omdat het m-voud van ieder element in $f[A]$ het nulelement is geldt $m(b - b') = 0$, en dus $mb = mb'$.

Nu we weten dat het m-voud mb van een willekeurig element $b \in g^{-1}(c)$ een uniek element in $g^{-1}(c)$ levert, volgt direct dat de afbeelding $s : C \to B$ gegeven door $s(c) = mb$ een homomorfisme is. Immers, voor b_1 en b_2 in de vezels van respectievelijk c_1 en c_2 ligt $b_1 + b_2$ in de vezel boven $c_1 + c_2$. Dit geeft $s(c_1) + s(c_2) = mb_1 + mb_2 = m(b_1 + b_2) = s(c_1 + c_2)$.

We concluderen dat s een sectie van g is, en wegens 9.3 splitst de rij. □

▶ Vrije abelse groepen

Als in 2.8 zeggen we dat een deelverzameling S van een abelse groep A de groep A *voortbrengt* indien ieder element $x \in A$ geschreven kan worden als een som $x = \sum_{s\in S} c_s s$ met getallen $c_s \in \mathbf{Z}$ die voor slechts eindig veel s verschillen van 0. Een dergelijke representatie is meestal niet uniek. Zijn alle $x \in A$ wel uniek te schrijven als zo'n som, dan heet A een *vrije abelse groep* en S een *basis* voor A. In zo'n geval betekent de uniciteit van de representatie van $x = 0$ dat de elementen van een basis S *lineair onafhankelijk* zijn, d.w.z. we hebben $\sum_{s\in S} c_s s = 0$ dan en slechts dan als $c_s = 0$ geldt voor alle $s \in S$. De cardinaliteit van een basis voor A noemt men de *vrije rang* of kortweg *rang* van A. Deze kan oneindig zijn. Voor $S = \emptyset$ is $A = 0$ de triviale groep van rang 0.

Opgave 4. Laat zien dat de verzameling $\mathcal{P}$ van priemgetallen een basis vormt voor de multiplicatieve groep $\mathbf{Q}_{>0}$ van positieve rationale getallen.

Voor een vrije abelse groep met *eindige* basis $S = \{s_1, s_2, \ldots, s_n\}$ van cardinaliteit n is de afbeelding

$$\begin{aligned} \mathbf{Z}^n &\longrightarrow A \\ (c_i)_{i=1}^n &\longmapsto \textstyle\sum_{i=1}^n c_i s_i \end{aligned}$$

een isomorfisme. Het geïnduceerde isomorfisme $A/2A \cong (\mathbf{Z}/2\mathbf{Z})^n$ nu laat zien dat $A/2A$ orde 2^n heeft, en we concluderen hieruit dat de rang van A kennelijk niet afhangt van de keuze van een basis voor A.

De gegeven definities lijken sterk op soortgelijke in de lineaire algebra. Zo is de rang van een abelse groep het analogon van de dimensie van een vectorruimte. Het belangrijke verschil is dat de 'scalairen' hier niet in een lichaam, maar in de ring $\mathbf{Z}$ liggen. De theorie van de abelse groepen, die men als 'lineaire algebra over $\mathbf{Z}$' kan bestempelen, wijkt daarom enigszins af van de 'klassieke' lineaire algebra. Ons argument voor de basisonafhankelijkheid van de rang werkt bijvoorbeeld niet voor dimensies van vectorruimtes. Anderzijds heeft lang niet iedere abelse groep een basis.

Opgave 5. Laat zien dat een vrije abelse groep geen elementen $x \neq 0$ van eindige orde bevat.

Een abelse groep A heet *eindig voortgebracht* als er een eindige deelverzameling $S \subset A$ bestaat die A voortbrengt. Is $S = \{s_1, s_2, \ldots, s_n\}$ zo'n deelverzameling, dan is de boven gegeven afbeelding $\mathbf{Z}^n \to A$ nog wel surjectief, maar niet noodzakelijk injectief. Wegens de isomorfiestelling 4.9 is er een isomorfisme $A \cong \mathbf{Z}^n/H$ voor zekere $H \subset \mathbf{Z}^n$. De eindig voortgebrachte abelse groepen zijn dus alle van de vorm $\mathbf{Z}^n/H$ voor zekere $n \geq 0$ en $H \subset \mathbf{Z}^n$. Merk op dat ieder quotiënt van een eindig voortgebrachte abelse groep ook weer eindig voorgebracht is.

Alle bewijzen van de structuurstelling 9.11 voor eindige abelse groepen maken op enigerlei wijze gebruik van expliciete kennis van ondergroepen van $\mathbf{Z}^n$. Een tamelijk direct bewijs wordt aangegeven in de opgaven 9.42–43. Wij volgen een iets andere weg, die ons tevens een aantal interessante tussenresultaten levert.

9.7. Stelling. *Iedere ondergroep $A \subset \mathbf{Z}^n$ is vrij van rang $k \leq n$.*

Bewijs. We passen inductie naar n toe. Voor $n = 0$ is $A = 0 = \mathbf{Z}^0$ vrij van rang 0. Stel dat de stelling bewezen is voor ondergroepen van $\mathbf{Z}^{n-1}$, en beschouw de projectie $\pi : \mathbf{Z}^n \to \mathbf{Z}$ op de laatste coördinaat. Dit geeft een korte exacte rij

$$0 \longrightarrow A \cap \ker \pi \longrightarrow A \xrightarrow{\pi} \pi[A] \longrightarrow 0.$$

Wegens de inductiehypothese is de ondergroep $A' = A \cap \ker \pi$ van $\ker \pi \cong \mathbf{Z}^{n-1}$ vrij van rang $k' \leq n-1$. We hebben nu twee gevallen. In het geval $\pi[A] = 0$ volgt direct dat $A = A'$ vrij is van rang $\leq n-1$. In het andere geval is $\pi[A]$ een niet-triviale ondergroep van $\mathbf{Z}$, dus als in 6.2 van de vorm $\pi[A] = m\mathbf{Z} \cong \mathbf{Z}$. Wegens 9.4 is de extensie A van $\pi[A] \cong \mathbf{Z}$ met A' gesplitst, en er volgt dat $A \cong A' \oplus \mathbf{Z}$ vrij is van rang $k' + 1 \leq n$. □

9.8. Voorbeeld. We bepalen met de methode van 9.7 een basis voor de ondergroep $A \subset \mathbf{Z}^3$ gegeven door

$$A = \{(x, y, z) \in \mathbf{Z}^3 : 4x + y + 3z \equiv 0 \bmod 6\}.$$

Is $\pi : A \to \mathbf{Z}$ de projectie op de z-coördinaat, dan geldt $\pi(a) = 1$ voor het element $a = (1, -1, 1) \in A$. Dit geeft $A = A' \oplus \langle a \rangle$ met $A' = \{(x, y, 0) \in \mathbf{Z}^3 : 4x + y \equiv 0 \bmod 6\}$. We kunnen A' opvatten als een ondergroep van $\mathbf{Z}^2$. Voor de projectie $\pi' : A' \to \mathbf{Z}$ op de y-coördinaat geldt $\pi'[A'] = 2\mathbf{Z}$, en we hebben $\pi'(a') = 2$ voor $a' = (1, 2, 0) \in A'$. Er volgt $A' = \ker \pi' \oplus \langle a' \rangle$, en $\ker \pi' = \{(x, 0, 0) \in \mathbf{Z}^3 : 4x \equiv 0 \bmod 6\}$ wordt voortgebracht door $(3, 0, 0)$. We zien dat A vrij is van rang 3, en indien we de elementen van $\mathbf{Z}^3$ als kolomvectoren schrijven hebben we

$$A = \mathbf{Z} \cdot \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix} \oplus \mathbf{Z} \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \oplus \mathbf{Z} \cdot \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}.$$

De resulterende 'bovendriehoeksgedaante' van de basis ten opzichte van de standaardbasis van $\mathbf{Z}^3$ maakt het gemakkelijk om een element van A op deze basis uit te drukken.

Opgave 6. Bepaal in bovenstaand voorbeeld de index van A in $\mathbf{Z}^3$.

9.9. Gevolg. *Zij A een eindig voortgebrachte abelse groep waarin elk element $a \neq 0$ oneindige orde heeft. Dan is A vrij van eindige rang.*

Bewijs. Zij $S \subset A$ een eindige collectie voortbrengers, en $S' \subset S$ een zo groot mogelijke deelverzameling van lineair onafhankelijke elementen. Dan is de ondergroep $F \subset A$ voortgebracht door S' een vrije abelse groep met basis S'. De maximaliteit van S' impliceert dat er voor elk element $s \in S \setminus S'$ een positief getal $m_s \in \mathbf{Z}$ bestaat met $m_s s \in F$. Zij $m \geq 1$ een gemeenschappelijk veelvoud van de getallen m_s voor $s \in S \setminus S'$. Dan is vermenigvuldiging met m een homomorfisme $A \to A$ waarvan het beeld in F ligt. Wegens de aanname is dit homomorfisme injectief. Er volgt dat $A \cong mA \subset F$ isomorf is met een ondergroep van een vrije groep van eindige rang. Wegens 9.7 is dan ook A vrij van eindige rang. □

Met een variatie op het bewijs van 9.9 kan men bewijzen dat discrete ondergroepen van $\mathbf{R}^n$ altijd vrij zijn van eindige rang. Een ondergroep $A \subset \mathbf{R}^n$ heet *discreet* als iedere begrensde deelverzameling van $\mathbf{R}^n$ slechts eindig veel elementen van A bevat. Dergelijke ondergroepen heten ook wel *roosters* in $\mathbf{R}^n$.

9.10. Stelling. *Een discrete ondergroep $A \subset \mathbf{R}^n$ is vrij van rang $k \leq n$.*

Bewijs. Uit de lineaire algebra weten we dat een maximale deelverzameling $S \subset A$ van over $\mathbf{R}$ lineair onafhankelijke elementen niet meer dan n elementen kan bevatten. Zij $S = \{s_1, s_2, \ldots, s_k\}$ zo'n deelverzameling, met $k \leq n$. Dan is ieder element $x \in A$ te schrijven als $x = \sum_{i=1}^{k} r_i s_i$ met $r_i \in \mathbf{R}$. We gaan bewijzen dat de vrije ondergroep $A_0 \subset A$ voortgebracht door S *eindige* index heeft in A.

Ieder reëel getal is de som van een geheel getal en een element $\lambda \in [0, 1)$, dus ieder element van A is te schrijven als de som van een element in A_0 en een element in de verzameling

$$F = \{\textstyle\sum_{i=1}^{k} r_i s_i : 0 \leq r_i < 1\}.$$

Omdat F een begrensde verzameling in $\mathbf{R}^n$ is bevat hij slechts eindig veel elementen uit A, en dus zijn er maar eindig veel nevenklassen van A_0 in A. De index $m = [A : A_0]$ is daarom eindig. Vermenigvuldiging met m is nu een homomorfisme dat A injectief afbeeldt naar de vrije groep A_0 van rang k. Er volgt weer uit 9.7 dat A zelf vrij is van eindige rang, en deze rang is ten hoogste $k \leq n$. □

Opgave 7. Laat zien dat $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}$ een ondergroep van $\mathbf{R}$ is die vrij is van rang 2.

▶ Structuurstelling

We introduceren enige terminologie om de structuurstelling voor eindig voortgebrachte abelse groepen te formuleren.

Een abelse groep A waarin elk element $a \neq 0$ oneindige orde heeft heet *torsievrij*. Een element van A van eindige orde noemt men een *torsie-element* in A. Geldt $ma = 0 \in A$ voor $m \in \mathbf{Z}$, dan wordt a *geannihileerd* door m. We zeggen dat een getal $m \in \mathbf{Z}$ de groep A annihileert als $ma = 0$ geldt voor alle $a \in A$. De torsie-elementen van A vormen de *torsie-ondergroep* $A^{\mathrm{tor}} \subset A$, en A is torsievrij als $A^{\mathrm{tor}} = 0$ geldt. Algemener

is de factorgroep A/A^{tor} altijd torsievrij. Immers, een element $a \in A$ waarvoor ma een torsie-element is voor zekere $m > 0$ is zelf ook torsie.

Opgave 8. Laat zien dat de elementen van eindige orde in een niet-abelse groep niet in het algemeen een ondergroep vormen.

Een abelse groep A heet een *torsiegroep* als $A^{\mathrm{tor}} = A$ geldt. Eindige abelse groepen zijn altijd torsie. De optelgroep $\mathbf{Q}/\mathbf{Z}$ is een voorbeeld van een oneindige torsiegroep.

Een eindig voortgebrachte torsiegroep is eindig. Immers, een surjectie $\mathbf{Z}^n \to A$ die de 'standaardbasis' van $\mathbf{Z}^n$ op elementen afbeeldt die geannihileerd worden door m leidt tot een surjectieve afbeelding $(\mathbf{Z}/m\mathbf{Z})^n \twoheadrightarrow A$ van een eindige groep naar A.

9.11. Stelling. *Iedere eindig voortgebrachte abelse groep A is een directe som van cyclische groepen. Er bestaan $r \geq 0$ en een isomorfisme*

$$A \cong A^{\mathrm{tor}} \oplus \mathbf{Z}^r.$$

De torsie-ondergroep A^{tor} van A is eindig, en isomorf met de directe som van zijn Sylow-p-ondergroepen $A(p)$. Voor elke priem p is er een isomorfisme

$$A(p) \xrightarrow{\sim} \mathbf{Z}/p^{k_1}\mathbf{Z} \oplus \mathbf{Z}/p^{k_2}\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/p^{k_m}\mathbf{Z},$$

waarbij de gehele getallen $m \geq 0$ en $k_1 \geq k_2 \geq \ldots \geq k_m > 0$ uniek bepaald zijn door p.

Het getal r in 9.11, dat 0 is precies wanneer A eindig is, heet de *vrije rang* van A.

Bewijs. Beschouw de exacte rij $0 \to A^{\mathrm{tor}} \to A \to A/A^{\mathrm{tor}} \to 0$. De groep A/A^{tor} is torsievrij en als factorgroep van A weer eindig voortgebracht, dus wegens 9.9 isomorf met $\mathbf{Z}^r$ voor zekere $r \geq 0$. We zagen al na 9.4 (in opgave 9.3) dat een dergelijke exacte rij splitst, en we krijgen een isomorfisme $A \cong A^{\mathrm{tor}} \oplus \mathbf{Z}^r$. De groep $A^{\mathrm{tor}} \cong A/\mathbf{Z}^r$ is als factorgroep van A weer eindig voortgebracht. Omdat hij tevens torsie is, is hij eindig. Wegens 8.10 is A^{tor} nu isomorf met de som van zijn Sylow-p-ondergroepen $A(p)$.

Om de structuurstelling te bewijzen voor de Sylow-p-ondergroepen $A(p)$, die eindige abelse p-groepen zijn, gebruiken we inductie naar de orde van $A(p)$. Voor $A(p)$ van orde 1 of p is er niets te bewijzen.

Stel nu dat iedere abelse p-groep van orde kleiner dan $\#A(p)$ een som van cyclische p-groepen is, en kies een element $x \in A(p)$ dat *maximale* orde p^{k_1} in $A(p)$ heeft. Ieder element van $A(p)$ heeft dan orde p^k met $k \leq k_1$. We beschouwen de exacte rij

$$0 \longrightarrow \langle x \rangle \longrightarrow A(p) \xrightarrow{g} A(p)/\langle x \rangle \longrightarrow 0.$$

Wegens de inductiehypothese hebben we $A(p)/\langle x \rangle \cong \mathbf{Z}/p^{k_2}\mathbf{Z} \oplus \mathbf{Z}/p^{k_3}\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/p^{k_m}\mathbf{Z}$ voor gehele getallen $k_i \leq k_1$, en het is voldoende om te laten zien dat de rij splitst. We willen een sectie s van g construeren, dit betekent dat we voor elk van de voortbrengers $y_2, y_3, \ldots, y_m$ van de cyclische componenten van $A(p)/\langle x \rangle$ een element $s(y_i) \in g^{-1}(y_i)$ moeten aangeven van orde p^{k_i}.

Neem eerst een willekeurig element $x_i \in g^{-1}(y_i)$. We laten zien dat dit element na wijziging met een geschikt veelvoud van x orde p^{k_i} krijgt. Omdat $p^{k_i}x_i$ een element uit $\ker g = \langle x \rangle$ is bestaat een getal n_i met $p^{k_i}x_i = n_i x$. Daar $A(p)$ door p^{k_1} geannihileerd wordt hebben we

$$(p^{k_1-k_i}n_i)x = p^{k_1}x_i = 0.$$

Er volgt dat p^{k_1} een deler is van $p^{k_1-k_i}n_i$, ofwel dat n_i deelbaar is door p^{k_i}. Schrijven we $n_i = p^{k_i}u_i$, dan geldt $p^{k_i}(x_i - u_i x) = 0$, en we concluderen dat $x_i - u_i x \in g^{-1}(y_i)$ de gewenste orde p^{k_i} heeft. Dit laat zien dat er een sectie bestaat, en dat onze rij splitst.

De uniciteit van m en de exponenten k_i volgt ook met inductie naar de orde van $A(p)$. Voor $A(p) = 1$ geldt $m = 0$ en is er niets te bewijzen. Voor $A(p) \neq 1$ krijgt men uit een stel exponenten k_i voor A de exponenten van de ondergroep $pA(p) \subsetneq A(p)$ door steeds k_i door $k_i - 1$ te vervangen, en weg te laten ingeval $k_i - 1 = 0$ geldt. De exponenten van $pA(p)$ zijn wegens de inductiehypothese eenduidig bepaald, dus de exponenten $k_i \geq 2$ van $A(p)$ zijn dat ook. Om de eenduidigheid van *alle* k_i te krijgen is het nu voldoende om op te merken dat het *aantal* exponenten m van $A(p)$ eenduidig door A bepaald wordt. Immers, de gegeven representatie leidt tot een isomorfisme $A(p)/pA(p) \cong (\mathbf{Z}/p\mathbf{Z})^m$, en de orde p^m van $A^{\mathrm{tor}}/pA^{\mathrm{tor}}$ hangt alleen van A af. □

9.12. Gevolg. *Iedere eindige abelse groep A heeft een unieke representatie*

$$A \cong \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_2\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/d_t\mathbf{Z},$$

met getallen $d_i \geq 2$ die voldoen aan de deelbaarheidsrelaties $d_t | d_{t-1} | \ldots | d_2 | d_1$.

Bewijs. Schrijf voor iedere p die de orde van A deelt als in 9.11 de Sylow-p-ondergroep $A(p)$ als een directe som van cyclische p-groepen met ordes $p^{k_{1,p}} \geq p^{k_{2,p}} \geq \ldots \geq p^{k_{m,p}}$. Door waar nodig $k_{i,p} = 0$ te nemen mogen we aannemen dat het aantal exponenten m bij iedere priem p gelijk is aan een vast getal t, en dat er een priem p is met $k_{t,p} \neq 0$. Neem nu $d_i = \prod_p p^{k_{i,p}}$ voor $i = 1, 2, \ldots, t$. Dan geldt $\mathbf{Z}/d_i\mathbf{Z} \cong \prod_p \mathbf{Z}/p^{k_{i,p}}\mathbf{Z}$ wegens 6.16. Het product over i geeft

$$\textstyle\prod_{i=1}^{t} \mathbf{Z}/d_i\mathbf{Z} \cong \prod_p \prod_{i=1}^{t} \mathbf{Z}/p^{k_{i,p}}\mathbf{Z} \cong \prod_p A(p) \cong A.$$

Het bewijs van de uniciteit van de d_i laten we als opgave aan de lezer. □

9.13. Gevolg. *Een abelse groep van kwadraatvrije orde is cyclisch.* □

De getallen d_i in 9.12 heten de *elementaire delers* van A. De grootste elementaire deler d_1 van $A \neq 1$ is de maximale orde van een element van A, en wordt de *exponent* van A genoemd; het is het kleinste positieve getal dat A annihileert. De triviale groep heeft exponent 1. De exponent van A deelt de orde van A, en is gelijk aan $\#A$ precies wanneer A cyclisch is. Is de exponent van A een priemgetal p, dan is A is een directe som van cyclische groepen van orde p en heet A een *elementair-abelse* p-groep.

Het getal t in 9.12 is het minimale aantal elementen dat nodig is om A voort te brengen. Immers, voor iedere priemdeler $p|d_t$ is $A/pA \cong (\mathbf{Z}/p\mathbf{Z})^t$ een vectorruimte

van dimensie t over $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, en die kan niet met minder dan t elementen worden voortgebracht. Definiëren we voor een priemgetal p de *p-rang* van een eindige abelse groep A als de dimensie over het lichaam $\mathbf{Z}/p\mathbf{Z}$ van de vectorruimte A/pA, dan is t het maximum over alle priemen p van de p-rang van A.

Opgave 9. Laat zien dat A cyclisch is dan en slechts dan als al zijn Sylow-p-ondergroepen het zijn.

▶ De groep $(\mathbf{Z}/n\mathbf{Z})^*$

Een veel voorkomende eindige abelse groep is de groep $(\mathbf{Z}/n\mathbf{Z})^*$ van inverteerbare restklassen modulo n uit 6.11. Door het ringisomorfisme 6.16 te beperken tot de eenhedengroep van $\mathbf{Z}/n\mathbf{Z}$ krijgen we een groepsisomorfisme

$$(\mathbf{Z}/n\mathbf{Z})^* \xrightarrow{\sim} \textstyle\prod_p (\mathbf{Z}/p^{\mathrm{ord}_p(n)}\mathbf{Z})^*.$$

Om $(\mathbf{Z}/n\mathbf{Z})^*$ als som (of product) van cyclische groepen te schrijven is het dus voldoende om dit voor elk van de groepen $(\mathbf{Z}/p^k\mathbf{Z})^*$ met p priem en $k \geq 1$ te doen. Voor $k = 1$ weten we uit 7.7 dat $(\mathbf{Z}/p\mathbf{Z})^*$ cyclisch is.

9.14. Lemma. *Zij p een oneven priemgetal en $k \geq 2$ een geheel getal. Dan geldt:*
1. *de orde van $\overline{1+p} \in (\mathbf{Z}/p^k\mathbf{Z})^*$ is p^{k-1};*
2. *de orde van $\overline{5} \in (\mathbf{Z}/2^k\mathbf{Z})^*$ is 2^{k-2}.*

Bewijs. We bewijzen voor p oneven en $s \geq 0$ met inductie naar s de gelijkheid

$$\mathrm{ord}_p[(1+p)^{p^s} - 1] = s + 1.$$

Voor $s = 0$ is de gelijkheid correct. Stel dat hij correct is voor $s = n - 1 \geq 0$, en schrijf $(1+p)^{p^{n-1}} = 1 + up^n$ met $p \nmid u$. Dan geldt voor $s = n \geq 1$ wegens het binomium van Newton

$$(1+p)^{p^n} = (1+up^n)^p = 1 + p \cdot up^n + (\textstyle\sum_{i=2}^{p-1} \binom{p}{i} u^i p^{in}) + u^p p^{pn}.$$

De binomiaalcoëfficiënten in de geïndiceerde som zijn deelbaar door p, dus alle termen van deze som bevatten ten minste $2n + 1 \geq n + 2$ factoren p. Ook de laatste term p^{pn} bevat $pn \geq n + 2$ factoren p—hier gebruiken we de aanname $p \neq 2$. We concluderen dat $(1+p)^{p^n} - 1$ congruent is met up^{n+1} mod p^{n+2}, en dit geeft de gewenste gelijkheid voor $s = n$. De bewezen gelijkheid laat zien dat voor oneven p de p^{k-1}-de macht van $\overline{1+p}$ in $(\mathbf{Z}/p^k\mathbf{Z})^*$ het eenheidselement is, maar de p^{k-2}-de macht niet. De orde van $\overline{1+p}$ is dan gelijk aan p^{k-1}, zoals gesteld in (1).

Het bewijs van (2) is analoog aan dat van (1) en wordt aan de lezer overgelaten. Men bewijst nu de gelijkheid $\mathrm{ord}_2[5^{2^s} - 1] = s + 2$ voor $s \geq 0$. □

9.15. Stelling. *Zij p een oneven priemgetal en $k > 0$ een geheel getal.*
1. *De groep $(\mathbf{Z}/p^k\mathbf{Z})^*$ is cyclisch van orde $p^{k-1}(p-1)$.*
2. *De groep $(\mathbf{Z}/2^k\mathbf{Z})^*$ is cyclisch van orde 2^{k-1} voor $k \leq 2$, en voor $k \geq 3$ geldt*

$$(\mathbf{Z}/2^k\mathbf{Z})^* = \langle\overline{5}\rangle \times \langle\overline{-1}\rangle \quad \cong \quad \mathbf{Z}/2^{k-2}\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

Bewijs. De natuurlijke afbeelding $(\mathbf{Z}/p^k\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$ is surjectief, en de kern is een ondergroep van orde p^{k-1} van $(\mathbf{Z}/p^k\mathbf{Z})^*$ die $\overline{1+p}$ bevat. Uit 9.14 volgt voor oneven p dat $\overline{1+p}$ de kern voortbrengt, en dit geeft een natuurlijk exact rijtje

$$1 \longrightarrow \langle\overline{1+p}\rangle \longrightarrow (\mathbf{Z}/p^k\mathbf{Z})^* \longrightarrow (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow 1.$$

De groep $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclisch van orde $p-1$ wegens 7.7, en omdat $p-1$ en p^{k-1} copriem zijn splitst de rij wegens 9.6. We vinden dat $(\mathbf{Z}/p^k\mathbf{Z})^*$ als product van twee cyclische groepen van coprieme ordes wegens 6.15 zelf ook cyclisch is. Dit bewijst (1).

Het is duidelijk dat $(\mathbf{Z}/2^k\mathbf{Z})^*$ cyclisch is voor $k \leq 2$. Voor $k \geq 3$ kunnen we het bewijs van (1) imiteren, maar in dit expliciete geval kunnen we ook 8.8 toepassen op de ondergroepen $H_1 = \langle\overline{5}\rangle$ en $H_2 = \langle\overline{-1}\rangle$. Wegens 9.14.2 is $H_1 \cong C_{2^{k-1}}$ een cyclische ondergroep van index 2 in $(\mathbf{Z}/2^k\mathbf{Z})^*$. Omdat alle machten van 5 congruent zijn met 1 mod 4 geldt $-1 \notin H_1$ en voldoet $H_2 \cong C_2$ aan $H_1 \cap H_2 = 1$. Toepassing van 8.8 geeft nu het gewenste isomorfisme $(\mathbf{Z}/2^k\mathbf{Z})^* = \langle\overline{5}\rangle \times \langle\overline{-1}\rangle \cong \mathbf{Z}/2^{k-2}\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. □

Opgaven.

10. Zij gegeven het volgende commutatieve diagram van abelse groepen waarvan de rijen korte exacte rijtjes zijn.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & 0. \end{array}$$

    Bewijs dat β injectief (resp. surjectief) is als α en γ het zijn. Concludeer dat β een isomorfisme is als α en γ het zijn.

11. Laat zien dat *ieder* kort exact rijtje van vectorruimtes over een lichaam K splitst.

12. Bepaal alle isomorfietypen van abelse groepen van orde 16. Welke typen zijn te verkrijgen als extensie van C_4 met C_4? En welke als extensie van V_4 met V_4?

13. Zij $f : A \to B$ een injectief homomorfisme naar een abelse groep B en p een retractie van f. Bewijs: $B \cong \operatorname{im} f \oplus \ker p$. Wat is de corresponderende uitspraak voor een surjectief homomorfisme $g : A \to B$ met sectie s?

14. Zij C een eindig voortgebrachte abelse groep met de eigenschap dat ieder kort exact rijtje $0 \to A \to B \to C \to 0$ splitst. Bewijs dat C een vrije groep is. [Vergelijk met 9.4.]

15. Laat zien dat de optelgroep $\mathbf{R}$ van reële getallen torsievrij is, maar niet vrij.

16. Zijn de abelse groepen $\mathbf{Q}$, $\mathbf{R}$ en $\mathbf{Q}/\mathbf{Z}$ eindig voortgebracht? Zijn ze torsievrij? Zelfde vragen voor de multiplicatieve groepen $\mathbf{Q}^*$ en $\mathbf{R}^*$.

17. Een abelse groep A heet *deelbaar* als voor alle $a \in A$ en $k \in \mathbf{Z}_{>0}$ er een element $x \in A$ bestaat met $kx = a$. Bewijs: een deelbare groep $A \neq 0$ is niet vrij.

18. Bewijs: een ondergroep van een eindig voortgebrachte abelse groep is eindig voortgebracht.

*19. Zij $G \subset \mathrm{GL}_2(\mathbf{Q})$ de groep voortgebracht door $\left(\begin{smallmatrix}2 & 0\\ 0 & 1\end{smallmatrix}\right)$ en $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Bewijs dat de ondergroep $H = \{g \in G : \det(g) = 1\} \subset G$ abels is en *niet* eindig voortgebracht.

20. Bepaal een basis voor de groep $A = \{(x, y, z) \in \mathbf{Z}^3 : x + 2y + 3z \equiv 0 \bmod 6\} \subset \mathbf{Z}^3$. Laat zien dat de groep $B \subset \mathbf{Z}^3$ voortgebracht door $v_1 = (4, -5, 2)$, $v_2 = (-1, 2, -1)$ en $v_3 = (1, 7, -5)$ een ondergroep van A is, en bepaal de structuur van $\mathbf{Z}^3/B$ en A/B.

21. Zelfde vraag als boven, maar nu met $v_1 = (4, -5, 8)$, $v_2 = (-1, 2, -1)$ en $v_3 = (1, 7, -5)$.

22. Zij $A \subset \mathbf{Z}^4$ de kern van het homomorfisme

$$\begin{aligned} \mathbf{Z}^4 &\longrightarrow \mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} \\ (w, x, y, z) &\longmapsto (w + x - 5z, w - y + z \bmod 4, -w + 3y - z \bmod 6). \end{aligned}$$

Bepaal een basis voor A en de structuur van $\mathbf{Z}^4/A$.

23. Zij A een abelse groep van orde n en $m > 0$ een deler van n. Bewijs dat A een ondergroep H_m bevat van orde m. Bewijs dat de ondergroep $H_m \subset A$ uniek bepaald is door m voor alle delers $m|n$ dan en slechts dan als A cyclisch is.

24. Laat zien dat een exact rijtje $R : 0 \to A \to B \to C \to 0$ van eindige abelse groepen aanleiding geeft tot een exact rijtje $R_p : 0 \to A(p) \to B(p) \to C(p) \to 0$ van Sylow-p-ondergroepen voor iedere priem p, en dat R splitst dan en slechts dan als dit voor alle R_p het geval is.

25. Laat zien dat ieder kort exact rijtje $0 \to A \to B \to C \to 0$ van abelse groepen aanleiding geeft tot een exact rijtje $0 \to A^{\mathrm{tor}} \to B^{\mathrm{tor}} \to C^{\mathrm{tor}}$, maar dat de afbeelding $B^{\mathrm{tor}} \to C^{\mathrm{tor}}$ niet noodzakelijk surjectief is. Ga na dat het rijtje $0 \to A/A^{\mathrm{tor}} \to B/B^{\mathrm{tor}} \to C/C^{\mathrm{tor}} \to 0$ een kort exact rijtje is dan en slechts dan als $B^{\mathrm{tor}} \to C^{\mathrm{tor}}$ surjectief is.

26. Definieer voor A een eindige abelse groep en p^k een priemmacht de *p^k-rang* van A als het aantal cyclische groepen van orde deelbaar door p^k dat voorkomt in een decompositie van A als een product van cyclische groepen. Laat zien dat deze rang niet afhangt van de gekozen decompositie en voor $k = 1$ de in de tekst gedefinieerde p-rang geeft. Is dit ook waar als we p^k door een willekeurig positief getal vervangen?

27. Laat zien dat eindige abelse groepen die voor iedere $k \geq 1$ evenveel elementen van orde k bevatten isomorf zijn. [Dit is niet algemeen waar voor eindige groepen, zie opgave 6.45.]

28. Stel dat A en B eindig voortgebrachte abelse groepen zijn, en dat voor iedere $k \geq 1$ de ordes van A/kA en B/kB gelijk zijn. Zijn A en B noodzakelijk isomorf?

29. Zij A een eindig voortgebrachte abelse groep met ondergroep H, en stel dat voor iedere priem p de natuurlijke afbeelding $H \to A/pA$ surjectief is. Bewijs: $H = A$. Laat zien dat dit niet voor willekeurige abelse A waar is.

30. Laat zien dat een eindige abelse groep precies dan cyclisch is als hij voor geen enkele priem p een ondergroep isomorf met $\mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$ bevat, en dat een eindig voortgebrachte abelse groep A cyclisch is dan en slechts dan als A/pA cyclisch is voor alle priemen p.

31. Laat zien dat het aantal isomorfieklassen van abelse groepen van orde q^m voor q priem gelijk is aan $p(m)$, waarbij p de partitiefunctie is. Leid hieruit af dat het aantal isomorfieklassen van abelse groepen van orde $n = \prod_q q^{k_q}$ gelijk is aan $\prod_q p(k_q)$.

32. Zij $S \subset \mathbf{R}$ een eindige verzameling met $1 \in S$ en $H \subset \mathbf{R}$ de additieve ondergroep voortgebracht door S. Bewijs: H is discreet in $\mathbf{R} \iff S \subset \mathbf{Q}$.

33. Zij p een oneven priem, en stel dat $x-1$ precies $k \geq 1$ factoren p bevat. Bewijs dat $x^{p^s}-1$ precies $k+s$ factoren p bevat. Laat zien dat voor $k \geq 2$ dit ook waar is voor $p = 2$.

34. Zij $0 \to A \to B \to C \to 0$ een kort exact rijtje van eindig voortgebrachte abelse groepen. Laat zien dat voor de vrije rang van deze groepen de gelijkheid $r(A) + r(C) = r(B)$ geldt. Laat tevens zien dat ingeval B eindig is en p een priemgetal voor de p-rangen de ongelijkheid
$$r_p(A) + r_p(C) \geq r_p(B)$$
geldt. Geef een voorbeeld waarin deze ongelijkheid strikt is.

35. Bepaal de elementaire delers van $(\mathbf{Z}/n\mathbf{Z})^*$ voor $n = 720$, 1000 en 17000.

36. Bepaal de nulpunten van het polynoom $X^2 - 1$ in $\mathbf{Z}/n\mathbf{Z}$ voor $n = 720$, 1000 en 17000.

37. Zij p een priemgetal en $k \geq 1$ een geheel getal. Laat zien dat de natuurlijke afbeelding $(\mathbf{Z}/p^k\mathbf{Z})^* \longrightarrow (\mathbf{Z}/p\mathbf{Z})^*$ een sectie heeft gegeven door $a \bmod p \mapsto a^{p^{k-1}} \bmod p^k$. [Merk op dat het niet a priori duidelijk is dat deze afbeelding *welgedefinieerd* is!]

*38. Zij A eindig voortgebracht abels en $f : A \to A$ een surjectief homomorfisme. Bewijs dat f is een isomorfisme is. Geldt eenzelfde uitspraak voor injectieve homomorfismen?

39. Zij F een vrije abelse groep van eindige rang en $\pi : F \to \mathbf{Z}$ een surjectief homomorfisme. Bewijs dat F een basis heeft waarin π de projectie op de laatste coördinaat is.

40. Zij F een vrije abelse groep van eindige rang en $H \neq 0$ een ondergroep. Zij $\pi : F \to \mathbf{Z}$ een surjectief homomorfisme met $\pi[H] \neq 0$ waarvoor de index $a = [\mathbf{Z} : \pi[H]] > 0$ minimaal is. Bewijs: er is een splitsing $F = F' \oplus \langle x \rangle$ en een ondergroep $H' \subset aF'$ met $H = H' \oplus \langle ax \rangle$.

41. Zij F een vrije abelse groep van rang n en H een ondergroep. Bewijs dat er een basis $x_1, x_2, \ldots, x_n$ van F en gehele getallen d_i bestaan zodat $d_1x_1, d_2x_2, \ldots, d_nx_n$ een basis voor H is en $d_1|d_2|d_3|\ldots|d_n$ geldt. Leid hieruit gevolg 9.12 af.

42. Zij M een $n \times n$-matrix met gehele coëfficiënten. Bewijs dat er matrices $A, B \in \mathrm{SL}_n(\mathbf{Z})$ bestaan waarvoor AMB een diagonaalmatrix is. [Hint: gebruik de vorige opgave.]

43. Zij $A \subset \mathbf{Z}^n$ de ondergroep voortgebracht door de kolommen van de matrix $M = (c_{ij})_{i,j=1}^n$. Bewijs dat A van eindige index is in $\mathbf{Z}^n$ precies wanneer M niet-singulier is, en dat de index $[\mathbf{Z}^n : A]$ in dat geval gelijk is aan $|\det(M)|$.

44. Bepaal de structuur van $\mathbf{Z}^3/A$ als A wordt voortgebracht door de kolommen van de matrix
$$M = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}.$$

45. Zij S een (niet noodzakelijk eindige) verzameling. Een abelse groep $F \supset S$ heet de *vrije abelse groep op de verzameling* S als elke (verzamelingstheoretische) afbeelding $S \to X$ naar een abelse groep X een *unieke* voortzetting heeft tot een homomorfisme $F \to X$. Laat zien dat F bestaat en op isomorfie na uniek bepaald is.

46. Zij gegeven een (niet noodzakelijk eindige) collectie van abelse groepen A_i $(i \in I)$. Een abelse groep D voorzien van homomorfismen $f_i : A_i \to D$ voor alle $i \in I$ heet de *directe som* van de groepen A_i, notatie $D = \oplus_{i\in I} A_i$, als voor iedere collectie homomorfismen $g_i : A_i \to X$ naar een abelse groep X er een uniek homorfisme $g : D \to X$ bestaat met $g \circ f_i = g_i$ voor alle $i \in I$. Laat zien dat D bestaat en op isomorfie na uniek bepaald is. Wat is het verband met de vorige opgave?

47. Definieer voor $A = \mathbf{Q}^*$ en p priem de ondergroep $A_p \subset A$ door $A_p = \{p^k : k \in \mathbf{Z}\}$. Bewijs dat A de directe som is van $A^{\mathrm{tor}} = \langle -1\rangle$ en de ondergroepen A_p voor de priemgetallen p.

48. Zij gegeven een (niet noodzakelijk eindige) collectie van abelse groepen A_i $(i \in I)$. Een abelse groep P voorzien van homomorfismen $f_i : P \to A_i$ voor alle $i \in I$ heet het *directe product* van de groepen A_i, notatie $P = \prod_{i\in I} A_i$, als voor iedere collectie homomorfismen $g_i : X \to A_i$ van een abelse groep X er een uniek homorfisme $g : X \to P$ bestaat met $f_i \circ g = g_i$ voor alle $i \in I$. Laat zien dat P bestaat en op isomorfie na uniek bepaald is.[36]

49. Zij I een verzameling en A een abelse groep. Laat zien dat de verzameling A^I van afbeeldingen $f : I \to A$ een abelse groep wordt onder de 'coördinaatsgewijze optelling' $(f_1 + f_2)(i) = f_1(i) + f_2(i)$, en dat deze groep isomorf is met de productgroep $\prod_{i\in I} A$ in de zin van de vorige opgave.

50. Laat zien dat de directe som van een eindig aantal abelse groepen isomorf is met het directe product van deze groepen, maar dat voor een oneindige collectie van (niet-triviale) abelse groepen dit niet het geval is.

51. Gegeven homomorfismen van abelse groepen $f_i : A \to B_i$ voor $i = 1, 2$ definiëren we de *gevezelde som* $B_1 \oplus_A B_2$ van B_1 en B_2 over A als $(B_1 \oplus B_2)/\langle f_1(a), -f_2(a) : a \in A\rangle$. Evenzo definiëren we voor homomorfismen van abelse groepen $g_i : B_i \to C$ voor $i = 1, 2$ het *gevezelde product* $B_1 \times_C B_2$ van B_1 en B_2 over C als $\{(b_1, b_2) \in B_1 \times B_2 : g_1(b_1) = g_2(b_2)\}$. Laat zien dat dit abelse groepen zijn waarvoor de diagrammen

$$\begin{array}{ccc} A & \xrightarrow{f_1} & B_1 \\ \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle \mathrm{id}\times 0} \\ B_2 & \xrightarrow{0\times\mathrm{id}} & B_1 \oplus_A B_2 \end{array} \qquad \text{en} \qquad \begin{array}{ccc} B_1 \times_C B_2 & \xrightarrow{\pi_2} & B_2 \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle g_2} \\ B_1 & \xrightarrow{g_1} & C \end{array}$$

commuteren. *Kun je 'universele eigenschappen' als in de opgaven 46 en 47 aangeven die gevezelde sommen en producten karakteriseren?

***Homologische algebra**. We beschouwen in de volgende opgaven steeds *abelse* extensies E van een abelse groep C met een abelse groep A. Twee extensies $0 \to A \to E \to C \to 0$ en $0 \to A \to E' \to C \to 0$ heten isomorf als ze passen in een commutatief diagram van de vorm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_C} & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

De verzameling van isomorfieklassen van extensies van C met A geven we aan met $\mathrm{Ext}(C, A)$. Als de pijlen duidelijk zijn spreken we vaak kortweg over 'de extensie $E \in \mathrm{Ext}(C, A)$'. In de onderstaande opgaven laten we zien dat de verzameling $\mathrm{Ext}(C, A)$ zelf weer een groepsstructuur heeft.

52. Geef een voorbeeld van niet-isomorfe extensies $E, E' \in \mathrm{Ext}(C, A)$ waarvoor E en E' isomorf zijn als abelse groep.

53. Voor $E \in \mathrm{Ext}(C, A_1)$ en $\phi : A_1 \to A_2$ een groepshomomorfisme definieren we $\phi_* E$ als de gevezelde som $A_2 \oplus_{A_1} E$. Laat zien dat dit tot een natuurlijke afbeelding $\phi_* : \mathrm{Ext}(C, A_1) \to \mathrm{Ext}(C, A_2)$ leidt.

54. Voor $E \in \mathrm{Ext}(C_2, A)$ en $\phi : C_1 \to C_2$ een groepshomomorfisme definieren we $\phi^* E$ als het gevezelde product $E \times_{A_2} C_1$. Laat zien dat dit tot een natuurlijke afbeelding $\phi^* : \mathrm{Ext}(C_2, A) \to \mathrm{Ext}(C_1, A)$ leidt.

55. Gegeven twee extensies $E_1, E_2 \in \mathrm{Ext}(C, A)$ definieert men de *Baer som* $E_1 + E_2 \in \mathrm{Ext}(C, A)$ door de som $E_1 \oplus E_2 \in \mathrm{Ext}(C \oplus C, A \oplus A)$ (definitie duidelijk) af te beelden naar $\mathrm{Ext}(C, A)$ via afbeeldingen

$$\mathrm{Ext}(C \oplus C, A \oplus A) \xrightarrow{\Delta^*} \mathrm{Ext}(C, A \oplus A) \xrightarrow{\nabla_*} \mathrm{Ext}(C, A).$$

    Hier is $\Delta : C \to C \oplus C$ de 'diagonale inbedding' $c \mapsto (c, c)$ en $\nabla : A \oplus A \to A$ de 'optelling' $(a, a') \mapsto a + a'$. Laat zien dat $\mathrm{Ext}(C, A)$ met deze optelling een abelse groep wordt met als eenheidselement de gesplitste extensie $0 \to A \to A \oplus C \to C \to 0$.

56. Zij p een priemgetal. Laat zien dat $\mathrm{Ext}(C_p, C_p)$ orde p heeft.

57. Zij p een oneven priemgetal. Bewijs:
    a. Als $a, b \in \{2, 3, \ldots, p-1\}$ voldoen aan $ab \equiv 1 \bmod p$, dan is de orde van $(a \bmod p^2)$ of de orde van $(b \bmod p^2)$ in $(\mathbf{Z}/p^2\mathbf{Z})^*$ deelbaar door p.
    b. Er is een primitieve wortel modulo p^2 in $\{2, 3, \ldots, p-1\}$.

10 Eindige groepen

In de vorige paragraaf hebben we gezien dat eindige abelse groepen 'gesplitst' kunnen worden in een som van cyclische groepen. In deze paragraaf proberen we willekeurige eindige groepen G op een soortgelijke manier te analyseren. Voor niet-abelse groepen komen we het probleem tegen dat we weliswaar gemakkelijk niet-triviale ondergroepen aan kunnen geven, maar dat die vaak niet *normaal* zijn. De Sylowstellingen in deze paragraaf zijn in veel gevallen nuttig om normaaldelers te creëren. Hebben we een normaaldeler $N \triangleleft G$, dan is de situatie nog vaak aanzienlijk ingewikkelder dan in het abelse geval. Voor splitsende rijtjes krijgen we in het algemeen geen splitsing van G in een direct product, maar in een *semidirect product*.

Voor getallen n met weinig delers kunnen we de groepen van orde n als product van eenvoudige groepen 'ontrafelen', en een lijst van alle isomorfietypen van groepen van orde n aanleggen. Voor hoog deelbare getallen n is zo'n expliciete classificatie, het fundamentele *classificatieprobleem* van de eindige groepentheorie, niet mogelijk.

▶ Niet-abelse exacte rijtjes

We beginnen met het niet-abelse analogon van 9.2.

10.1. Definitie. *Een kort exact rijtje* $1 \to N \longrightarrow G \xrightarrow{g} H \to 1$ *van groepen heet gesplitst als er een sectie* $s : H \to G$ *bestaat met* $g \circ s = \mathrm{id}_H$.

Is G abels, dan zijn N en H het ook en is de definitie wegens 9.4 equivalent met 9.2.

Als het rijtje in 10.1 splitst kunnen we H via de injectie s als ondergroep van G opvatten. Er geldt dan $N \cap H = 1$ en $G = \{nh : n \in N, h \in H\}$. Stelling 8.13 is dus van toepassing, en G is het semidirecte product van N met H. Omgekeerd is in een semidirect product de projectie $\pi_H : N \rtimes H \to H$ op de H-coördinaat een surjectie met kern N die aanleiding geeft tot een kort exact rijtje als in 10.1. Semidirecte producten en splitsende korte exacte rijtjes zijn dus in de volgende zin 'dezelfde dingen'.

10.2. Stelling. *Laten* N *en* H *groepen zijn, en* $\sigma : H \to \mathrm{Aut}(N)$ *een homomorfisme. Dan past het semidirecte product* $N \rtimes_\sigma H$ *in een korte exacte rij*

$$1 \to N \longrightarrow N \rtimes_\sigma H \xrightarrow{\pi_H} H \to 1$$

die gesplitst wordt door de natuurlijke sectie $h \mapsto (1_N, h)$ *van* π_H.
Omgekeerd geeft iedere sectie $s : H \to G$ *van* g *in een korte exacte rij van groepen*

$$1 \to N \longrightarrow G \xrightarrow{g} H \to 1$$

aanleiding tot een isomorfisme $N \rtimes_\sigma H \xrightarrow{\sim} G$ *gegeven door* $(n, h) \mapsto ns(h)$. *Hier is* $\sigma : H \to \mathrm{Aut}(N)$ *de door* s *geïnduceerde conjugatiewerking:* $\sigma(h)(n) = s(h)ns(h)^{-1}$.□

Het splitsen van een exact rijtje $1 \to N \to G \to G/N \to 1$ komt neer op het vinden van een ondergroep $H \subset G$ met $N \cap H = 1$ en $G = NH$. Een dergelijke ondergroep H heet wel een *complement* van N in G. Voor zo'n complement geeft het natuurlijke

isomorfisme $G/N = NH/N \xrightarrow{\sim} H/(H \cap N) = H \subset G$ een bijbehorende sectie. Al in het abelse geval zagen we dat niet iedere normaaldeler $N \lhd G$ een complement heeft. Een complement is bovendien niet noodzakelijk uniek.

Opgave 1. Laat zien dat voor een normaaldeler N van een *eindige* groep G een ondergroep $H \subset G$ met $N \cap H = 1$ een complement van N is dan en slechts dan als H orde $[G : N]$ heeft.

10.3. Voorbeelden. 1. We zagen in 8.12.2 dat de ondergroep C_n van rotaties in de dihedrale groep D_n een normaaldeler is van index 2, en met het splitsende exacte rijtje

$$1 \to C_n \longrightarrow D_n \xrightarrow{\det} \langle -1 \rangle \to 1$$

correspondeert het semidirecte product $D_n = C_n \rtimes \langle \sigma \rangle$ uit 8.12.2. Iedere afbeelding $s : \langle -1 \rangle \to D_n$ die -1 naar een spiegeling $\sigma \in D_n$ stuurt geeft een sectie, en voor *iedere* keuze van σ werkt -1 op D_n door inversie (vergelijk opgave 11).

2. Voor $n \geq 2$ is de kern A_n van de tekenafbeelding $\varepsilon : S_n \to \langle -1 \rangle$ een normaaldeler van index 2 in de symmetrische groep S_n. De exacte rij

$$1 \to A_n \longrightarrow S_n \xrightarrow{\varepsilon} \langle -1 \rangle \to 1$$

is gesplitst omdat ieder homomorfisme $s : \langle -1 \rangle \to S_n$ dat -1 naar een 2-cykel stuurt een sectie van de tekenafbeelding is. Algemener brengt *ieder* oneven element van orde 2 in S_n een complement van A_n voort. We hebben ook hier een semidirect product $S_n \cong A_n \rtimes \langle -1 \rangle$, maar anders dan in het vorige voorbeeld hangt de werking van -1 op A_n voor niet te kleine n nu *wel* van de keuze van de sectie s af. Kennelijk kunnen geheel verschillende werkingen van H op N aanleiding geven tot isomorfe semidirecte producten. Zie opgave 14 voor een amusant voorbeeld van dit fenomeen.

3. De symmetrische groep S_4 past wegens 8.3.2 in een splitsende exacte rij

$$1 \to V_4 \longrightarrow S_4 \longrightarrow S_3 \to 1$$

geïnduceerd door het tetraëderhomomorfisme uit §5. De extensie wordt gesplitst door S_3 als stabilisator van een punt in S_4 op te vatten. De resulterende werking $S_3 \to \mathrm{Aut}(V_4)$ permuteert de niet-triviale elementen van V_4 en is een isomorfisme.

4. Op de groep $I_2(\mathbf{R})$ van isometrieën van het vlak geeft het 'lineaire deel'-homomorfisme L uit 3.9 aanleiding tot een exacte rij

$$1 \longrightarrow T \longrightarrow I_2(\mathbf{R}) \xrightarrow{L} O_2(\mathbf{R}) \longrightarrow 1.$$

Deze rij splitst door $O_2(\mathbf{R})$ op de bekende manier als ondergroep van $I_2(\mathbf{R})$ op te vatten, en dit geeft het al uit 8.10 bekende semidirecte product.

▶ Classificatie voor eenvoudige groepsordes

Het classificatieprobleem voor groepen van orde n is makkelijk als $n = p$ een priemgetal is: de enige groep van orde p is de cyclische groep C_p. Voor het product $n = pq$ van twee priemgetallen $p \leq q$ is er wegens de stelling van Cauchy 5.14 een cyclische ondergroep $C_q \subset G$ van orde q en index p. Wegens 5.10 is C_q normaal in G, dus we hebben een exacte rij

$$1 \to C_q \longrightarrow G \longrightarrow C_p \longrightarrow 1.$$

Voor $p \neq q$ is deze rij gesplitst. Immers, G bevat dan wegens 5.14 een ondergroep van orde p die isomorf op C_p wordt afgebeeld; de inverse van dit isomorfisme geeft een sectie. Voor $p = q$ splitst de rij niet in het geval dat G elementen van orde p^2 bevat, en dus cyclisch is. In het geval van een splitsende rij vinden we $G = C_q \rtimes_\phi C_p$ voor een afbeelding

$$\phi : C_p \longrightarrow \mathrm{Aut}(C_q) \cong (\mathbf{Z}/q\mathbf{Z})^* \cong C_{q-1}.$$

We gebruiken hier de isomorfismen uit 8.15 en 7.7. Als p *geen* deler van $q - 1$ is, is ϕ triviaal en vinden we $G = C_p \times C_q$, een abelse groep die wegens de Chinese reststelling 6.15 voor $q \neq p$ cyclisch is. Als p een deler is van $q - 1$, dan bevat $\mathrm{Aut}(C_q)$ een unieke cyclische ondergroep van orde p, en een niet-triviale werking ϕ identificeert C_p met deze ondergroep. Dit voltooit het bewijs van het volgende resultaat.

10.4. Stelling. *Laat p en q priemgetallen zijn met $p < q$.*

1. *Iedere groep van orde p^2 is abels, en isomorf met $C_p \times C_p$ of met C_{p^2};*
2. *Voor $p \nmid q - 1$ is iedere groep van orde pq cyclisch;*
3. *Voor $p | q - 1$ is iedere groep van orde pq isomorf met C_{pq} of met het semidirecte product $C_q \rtimes C_p$ van C_q met de cyclische ondergroep $C_p \subset \mathrm{Aut}(C_q)$.* □

Voor $p = 2$ is de niet-abelse groep $C_q \rtimes C_2$ de diëdergroep D_q uit 10.3.1.

10.5. Stelling. *Er zijn precies vijf isomorfieklassen van groepen van orde 8. De abelse groepen zijn $C_2 \times C_2 \times C_2$ en $C_4 \times C_2$ en C_8, de niet-abelse groepen zijn de diëdergroep D_4 en de quaternionengroep Q.*

Bewijs. Voor G van orde 8 zijn 1, 2, 4 en 8 de mogelijke ordes van elementen in G. Als G een element van orde 8 bevat, dan geldt $G \cong C_8$. Als $a^2 = 1$ geldt voor alle $a \in G$, dan is G een elementair-abelse 2-groep en vinden we $G \cong C_2 \times C_2 \times C_2$. Neem dus verder aan dat G een element a van orde 4 bevat, en geen element van orde 8. De cyclische ondergroep $C_4 = \langle a \rangle$ heeft index 2 in G en is dus normaal. We krijgen een exact rijtje $1 \to C_4 \to G \to C_2 \to 1$.

We bekijken eerst het geval dat dit rijtje splitst. Er is dan een element b van orde 2 in G dat niet in $C_4 = \langle a \rangle$ ligt, en we hebben $G = C_4 \rtimes C_2$, waarbij het niet-triviale element $b \in C_2$ door conjugatie op C_4 werkt. Daar $\mathrm{Aut}(C_4) \cong (\mathbf{Z}/4\mathbf{Z})^*$ uit de identiteit en inversie bestaat vinden we hiermee 2 groepen: het abelse directe product $C_4 \times C_2$ en de niet-abelse diëdergroep D_4.

Neem ten slotte aan dat het rijtje niet splitst. Dit betekent dat ieder element b in de vezel $G \setminus \langle a \rangle$ orde 4 heeft. Kies zo'n b. Dan geldt $b^2 \in \langle a \rangle$, en omdat b^2 orde 2 heeft

geldt $b^2 = a^2 = a^{-2}$ en $a^2b^2 = 1$. De elementen a en b commuteren niet, want dan zou $ab \notin \langle a \rangle$ orde 2 hebben. Omdat $bab^{-1} \in \langle a \rangle$ orde 4 heeft geldt kennelijk $bab^{-1} = a^{-1}$. De structuur van $G = \langle a, b \rangle$ ligt nu vast door het feit dat a en b orde 4 hebben en aan de relaties $b^2 = a^2$ en $bab^{-1} = a^{-1}$ voldoen. In meer traditionele notatie schrijven we $a = i$ en $b = j$ en $i^2 = j^2 = -1$. Merk op dat -1 met i en j, en dus met alle elementen van de groep commuteert. Schrijven we ook nog $ij = k$, dan krijgen we de presentatie van de quaternionengroep Q uit 8.7. □

Opgave 2. Bepaal het aantal ondergroepen van orde 2 en 4 van elk van de groepen in 10.5.

► Sylow-p-ondergroepen

Tot dusver is de stelling van Cauchy 5.14 ons belangrijkste hulpmiddel geweest bij het construeren van ondergroepen van een abstracte eindige groep G. We geven nu een belangrijke verscherping die in de zeventiger jaren van de negentiende eeuw door de Noor L. Sylow (1832–1918) bewezen werd. Deze verscherping zegt onder meer dat voor iedere *priemmacht* p^i die de orde van een eindige groep G deelt er een ondergroep $H \subset G$ is van orde p^i. Zo'n ondergroep heet een p-ondergroep van G.

Opgave 3. Laat zien dat de groep A_4 van orde 12 geen ondergroep heeft van orde 6.

Voor een gegeven priemgetal p kunnen we de orde van een eindige groep G schrijven als $\#G = p^k m$ met $p \nmid m$. Een ondergroep H van G heet een *Sylow-p-ondergroep* van G als H orde p^k heeft. Zo'n H is een 'maximale p-ondergroep' in G, en alleen niet-triviaal als p de groepsorde deelt. Hij hoeft niet normaal te zijn in G. Men maakt Sylow-p-ondergroepen door te beginnen met een uit 5.14 verkregen ondergroep van priemorde en deze stapsgewijs groter te maken. Hierbij gebruikt men het volgende lemma.

10.6. Lemma. *Zij H een p-ondergroep van een eindige groep G. Dan geldt*

$$[N_G(H) : H] \equiv [G : H] \bmod p.$$

Bewijs. Laat H regulier door linksvermenigvuldiging werken op $X = G/H$. Een nevenklasse xH is invariant onder vermenigvuldiging met H als $hxH = xH$ geldt voor $h \in H$, oftewel $hx \in xH$ en $h \in xHx^{-1}$ voor alle $h \in H$. Dit betekent precies dat $xHx^{-1} = H$ geldt, dus we hebben $x \in N_G(H)$ en $X^H = N_G(H)/H$. Wegens 5.15 geldt $\#X^H \equiv \#X \bmod p$, en daar de ordes van $X^H = N_G(H)/H$ en $X = G/H$ gelijk zijn aan respectievelijk $[N_G(H) : H]$ en $[G : H]$ is dit de te bewijzen congruentie. □

10.7. Stelling. *Zij G een eindige groep en p een priemgetal. Dan heeft G een Sylow-p-ondergroep. Iedere p-ondergroep van G is bevat in een Sylow-p-ondergroep van G.*

Bewijs. We nemen $p|\#G$, anders is de stelling triviaal. Wegens Cauchy bevat G een ondergroep van orde p, dus het is voldoende de tweede uitspraak te bewijzen.

Zij $H \subset G$ een p-ondergroep. Als $[G : H]$ niet deelbaar is door p, dan bevat $\#H$ wegens 4.7 evenveel factoren p als $\#G$ en is H zelf een Sylow-p-ondergroep van G. Als $[G : H]$ wel deelbaar is door p zullen we laten zien dat er een ondergroep $H' \supset H$ in G bestaat die H als ondergroep van index p bevat. Dan is H' een grotere p-ondergroep

van G, en door het argument zo vaak als nodig te herhalen krijgen we een Sylow-p-ondergroep $P \supset H$.

Voor de constructie van H' merken we op dat voor $[G : H]$ deelbaar door p de orde van de *groep* $N_G(H)/H$ wegens 10.6 ook deelbaar is door p. Dan bestaat er een ondergroep van orde p in $N_G(H)/H$, en volgens 8.1 is deze te schrijven als H'/H voor een ondergroep $H' \supset H$ van G. Dit geeft $[H' : H] = \#(H'/H) = p$. □

De verzameling Sylow-p-ondergroepen van G wordt aangeven met $\mathrm{Syl}_p(G)$. Voor de orde n_p van $\mathrm{Syl}_p(G)$ is er de volgende nuttige stelling.

10.8. Stelling van Sylow. *Zij G een eindige groep van orde $p^k m$ met $p \nmid m$ priem. Dan is het aantal n_p van Sylow-p-ondergroepen in G een deler van m, en er geldt $n_p \equiv 1 \bmod p$. Alle Sylow-p-ondergroepen van G zijn geconjugeerd in G.*

Bewijs. We bewijzen eerst dat ieder tweetal Sylow-p-ondergroepen P en P' van G geconjugeerd is. Neem hiertoe de verzameling X van ondergroepen geconjugeerd met P', en laat G door conjugatie werken op X. Het aantal met P' geconjugeerde ondergroepen, dat gelijk is aan $\#X = [G : N_G(P')]$, is een deler van $[G : P'] = m$ en daarom geen p-voud. Passen we 5.15 toe voor de conjugatiewerking van P op X, dan vinden we $\#X^P \equiv \#X \not\equiv 0 \bmod p$. In het bijzonder is X^P niet leeg, dus er is ten minste één met P' geconjugeerde ondergroep P'' die onder conjugatie met elementen uit P op zijn plaats blijft. We beweren dat $P = P''$ geldt, zodat P en P' inderdaad geconjugeerd zijn. Om dit te bewijzen kijken we naar de normalisator $N_G(P'')$ van P''. Deze bevat $N = P''$ als normaaldeler en $H = P$ als ondergroep. Stelling 8.2 geeft ons een isomorfisme

$$P/(P \cap P'') \xrightarrow{\sim} PP''/P''.$$

Links staat een p-groep, rechts een groep waarvan de orde $[G : P''] = m$ deelt. Beide groepen zijn dus triviaal, en dit betekent dat we $P = P''$ hebben.

Nu we weten dat alle Sylow-p-ondergroepen in G geconjugeerd zijn geldt hierboven $X = \mathrm{Syl}_p(G)$, en het gegeven argument laat zien dat $P'' = P$ het *enige* dekpunt is voor de conjugatieactie van P op X. We vinden $n_p = \#X \equiv \#X^P = 1 \bmod p$. □

10.9. Gevolg. *Een normale p-ondergroep $N \triangleleft G$ is bevat in iedere Sylow-p-ondergroep van G. Voor een normale Sylow-p-ondergroep $P \triangleleft G$ geldt $\mathrm{Syl}_p(G) = \{P\}$.*

Bewijs. Er bestaat een Sylow-p-ondergroep $P \supset N$ wegens 10.7. Iedere andere Sylow-p-ondergroep is wegens 10.8 van de vorm gPg^{-1} en bevat daarom $gNg^{-1} = N$. De tweede uitspraak volgt gemakkelijk. □

10.10. Gevolg. *Stel dat alle Sylow-ondergroepen van G normaal zijn. Dan is G isomorf met het directe product van zijn Sylow-ondergroepen.*

Bewijs. Omdat de Sylow-p-ondergroepen $N_p \triangleleft G$ voor verschillende priemen p normaaldelers van coprieme orde zijn geldt $N_p \cap N_{p'} = 1$ voor $p \neq p'$. Dit impliceert dat een element $n \in N_p$ altijd commuteert met een element $n' \in N_{p'}$. Immers, de commutator $[n, n'] = n(n'n^{-1}n'^{-1}) = (nn'n^{-1})n'^{-1}$ ligt wegens de eerste schrijfwijze in N_p en

wegens de tweede in $N_{p'}$. Er volgt $[n, n'] = e$. De afbeelding

$$\prod_{p|\#G} N_p \longrightarrow G$$

van het product van de Sylow-ondergroepen naar G gegeven door uitvermenigvuldiging van de coördinaten is nu een homomorfisme, en men ziet gemakkelijk in dat het surjectief is. Omdat de ordes aan beide kanten gelijk zijn is het een isomorfisme. □

Een eindige groep G met de eigenschap dat al zijn Sylow-ondergroepen normaal zijn heet *nilpotent*. Merk op dat eindige *abelse* groepen altijd nilpotent zijn. Voor niet-abelse groepen is nilpotentie een zware eis.

10.11. Voorbeeld. We bepalen de Sylow-p-ondergroepen van S_4 en S_5. Hierbij maken we gebruik van de in 5.11 bepaalde conjugatieklassen.

Voor de groep S_4 van orde $24 = 2^3 \cdot 3$ zien we uit 10.8 dat we $n_2 \in \{1, 3\}$ en $n_3 \in \{1, 4\}$ hebben. Elk van de acht 3-cykels in de S_4 is bevat in een Sylow-3-ondergroep, die orde 3 heeft en dus twee 3-cykels bevat; we vinden $n_3 = 4$. De 16 elementen van S_4 die geen 3-cykel zijn hebben orde 1, 2 of 4 en zijn bevat in een Sylow-2-ondergroep, die orde 8 heeft. Dit impliceert $n_2 > 1$, en dus $n_2 = 3$.

Om de Sylow-2-ondergroepen in S_4 expliciet aan te geven merken we op dat de ondergroep

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \lhd S_4$$

normaal is in S_4, en dus wegens 10.9 bevat in elke Sylow-2-ondergroep. Nemen we nu een willekeurig element van orde 2 of 4 buiten V_4, bijvoorbeeld (12), dan krijgen we hiermee een Sylow-2-ondergroep van orde 8:

$$P = \langle V_4, (12)\rangle = V_4 \cup \{(12), (34), (1324), (1423)\}.$$

De groep P wordt voortgebracht door $\rho = (1324)$ en $\sigma = (12)$ die aan de relatie $\sigma\rho = \rho^{-1}\sigma$ voldoen, dus we hebben $P \cong D_4$. Vervangt men in het voorafgaande (12) door (13) of (14), dan krijgt men met P geconjugeerde groepen P' en P''. Er geldt $\mathrm{Syl}_2(S_4) = \{P, P', P''\}$. Merk op dat we dit al tegen zijn gekomen in 8.3.2.

In het geval van de groep S_5 van orde $120 = 2^3 \cdot 3 \cdot 5$ vindt men $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 4, 10, 40\}$ en $n_5 \in \{1, 6\}$. Omdat er 24 verschillende 5-cykels in S_5 zijn is direct duidelijk dat $n_5 = 6$ geldt, met steeds de 4 niet-triviale machten van een 5-cykel per Sylow-5-ondergroep. Evenzo vindt men $n_3 = 10$ uit de 20 verschillende 3-cykels in S_5. Voor de Sylow-2-ondergroepen, die geen priemorde hebben en dus niet noodzakelijk paarsgewijs disjunct zijn, kan men niet direct n_2 uit de aantallen elementen van 2-macht orde aflezen. Omdat er echter $1 + 10 + 30 + 15 = 56$ elementen van orde 1, 2 of 4 zijn en een Sylow-2-ondergroep orde 8 heeft hebben we $n_2 > 7$, en dus $n_2 = 15$. Deze 15 groepen krijgt men door S_4 op één van de 5 voor de hand liggende manieren in S_5 te leggen en vervolgens één van de 3 Sylow-2-ondergroepen van S_4 te nemen.

▶ Constructie van normaaldelers

Met behulp van de Sylow-stellingen lukt het vaak om normaaldelers te maken in groepen waarvan we alleen de orde kennen. Soms bewijst men direct dat er een priemdeler $p|\#G$ is met $n_p = 1$, soms maakt men normaaldelers door G door conjugatie te laten werken op geschikte verzamelingen $\mathrm{Syl}_p(G)$.

10.12. Voorbeelden. 1. Zij G een groep van orde $42 = 2 \cdot 3 \cdot 7$. Dan is $n_7 \equiv 1 \bmod 7$ een deler van 6. Er volgt $n_7 = 1$, dus G heeft een normale ondergroep van orde 7.

2. Zij G een groep van orde $30 = 2 \cdot 3 \cdot 5$. Dan geldt $n_5 \in \{1, 6\}$ en $n_3 \in \{1, 10\}$. Zou $n_5 = 6$ gelden, dan heeft G precies $6 \times 4 = 24$ elementen van orde 5 en vinden we $n_3 = 1$ 'bij gebrek aan ruimte'. Dus G heeft een normale ondergroep van orde 3 of 5.

3. Zij G een groep van orde $300 = 2^2 \cdot 3 \cdot 5^2$. Dan geldt $n_5 \in \{1, 6\}$. In het geval $n_5 = 1$ heeft G een normaaldeler van orde 25. In het geval $n_5 = 6$ kunnen we G door conjugatie op $\mathrm{Syl}_5(G)$ laten werken. Dit geeft een transitieve werking $\phi : G \to S(\mathrm{Syl}_5(G)) \cong S_6$. De kern N van dit homomorfisme is een normaaldeler $N \neq G$. Is H de stabilisator van een ondergroep in $\mathrm{Syl}_5(G)$, dan heeft H index 6 in G wegens de transitiviteit van de werking. Wegens $N \subset H$ is de orde van N dus een deler van $300/6 = 50$. Omdat $\#G = 300 = 2^2 \cdot 3 \cdot 5^2$ geen deler is van $6! = 720 = 2^4 \cdot 3^2 \cdot 5$ is de orde van N deelbaar door 5. Dus G heeft een N van orde 5, 10, 25 of 50.

Heeft men een normaaldeler $N \triangleleft G$ gevonden, dan kan men proberen om G met behulp van 10.2 uit N en G/N 'op te bouwen'. Behalve N dient men hiertoe ook $\mathrm{Aut}(N)$ te kennen. Dit is eenvoudig voor cyclische N (8.15), of voor elementair abelse N (opgave 43). Indien de groepsorde n een product van slechts weinig priemgetallen is kan men vaak op deze manier een volledige classificatie van de isomorfietypen van groepen van orde n geven.

10.13. Stelling. *Er zijn precies vijf isomorfieklassen van groepen van orde* 12. *De abelse groepen zijn $C_6 \times C_2$ en C_{12}, de niet-abelse groepen zijn de alternerende groep op 4 letters A_4, de diëdergroep D_6 en het semidirecte product $C_3 \rtimes_\phi C_4$ met betrekking tot de unieke surjectie $\phi : C_4 \to \mathrm{Aut}(C_3)$.*

Bewijs. Zij G van orde 12. Dan is het aantal Sylow-3-ondergroepen $n_3(G)$ gelijk aan 1 of 4. In het eerste geval hebben we $G = N_3 \rtimes H_4$ voor een normale Sylow-3-ondergroep $N_3 \subset G$ en een Sylow-2-ondergroep H_4 die we als complement daarvan kunnen nemen. In het tweede geval zijn er 8 elementen van orde 3 in G en vormen de andere 4 elementen een normale Sylow-2-ondergroep $N_4 \subset G$. Dit geval geeft $G = N_4 \rtimes C_3$ voor een Sylow-3-ondergroep C_3.

Neem eerst aan dat $G = N_4 \rtimes C_3$ geldt. Als $N_4 = C_4$ cyclisch is heeft $\mathrm{Aut}(N_4) \cong (\mathbf{Z}/4\mathbf{Z})^*$ orde 2 en kan C_3 slechts triviaal werken. In dit geval is $G = C_4 \times C_3 \cong C_{12}$ cyclisch. Als $N_4 = V_4$ de viergroep van Klein is heeft $\mathrm{Aut}(V_4) \cong S_3$ een unieke ondergroep van orde 3. We kunnen in dit geval behalve het directe product $G \cong V_4 \times C_3 \cong C_6 \times C_2$ ook het semidirecte product $G \cong V_4 \rtimes C_3 \cong A_4$ maken. Dit is de ondergroep van index 2 in de groep $S_4 = V_4 \rtimes S_3$ uit 10.3.3.

Neem vervolgens aan dat $G = N_3 \rtimes_\phi H_4$ geldt voor een werking $\phi : H_4 \to \mathrm{Aut}(N_3) \cong (\mathbf{Z}/3\mathbf{Z})^*$. Als dit product direct is krijgen we één van de abelse groepen uit de vorige alinea, dus neem ϕ niet-triviaal. Als H_4 cyclisch is bepaalt dit ϕ uniek: de voortbrenger van $H_4 = C_4$ werkt door inversie op $N_3 = C_3$, en we vinden de niet abelse groep $G \cong C_3 \rtimes C_4$. Als $H_4 = V_4$ de viergroep van Klein is kunnen we $H_4 = \langle x\rangle \times \langle y\rangle$ schrijven voor een element x dat met C_3 commuteert en een element y dat door inversie op C_3 werkt. Omdat x zijn eigen inverse is kunnen we ook zeggen dat y door inversie op $C_3 \times \langle x\rangle \cong C_6$ werkt, en dit geeft $G \cong C_6 \rtimes C_2 = D_6$. □

Opgave 4. Welke groep in 10.13 is isomorf met $S_3 \times C_2$?

Met behulp van de tot dusver behaalde resultaten kennen we de isomorfietypen van alle groepen van orde $n \leq 15$. Ze staan in de 'tabel van kleine groepen' die op deze paragraaf volgt. Voor het *aantal* isomorfietypen $I(n)$ van orde $n \leq 32$ hebben we het volgende.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16*
$I(n)$	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14
n	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32*
$I(n)$	1	5	1	5	2	2	1	15	2	2	5	4	1	4	1	51

Voor de bepaling van $I(n)$ voor de waarden $17 \leq n \leq 31$ die niet onder 10.4 vallen verwijzen we naar de opgaven. De bepaling van $I(n)$ voor de met een ster gemerkte ordes valt buiten het bestek van deze syllabus.

De lijst laat zien dat $I(p^n)$ voor priemmachtorde p^n snel groeit met n. De waarden $I(2^n)$ zijn nog met de hand uitgerekend voor $n \leq 6$, voor de recente berekening van waarden als $I(2^7) = I(128) = 2328$ en $I(2^8) = I(256) = 56092$ heeft men computers gebruikt. Bij dit soort uitspraken is het verifiëren van de correctheid van een bewijs een probleem op zich. In 1997 werd voor $I(2^9) = I(512)$ de waarde 10 494 213 gevonden[37].

▶ Oplosbare groepen

Voor willekeurige eindige groepen heeft men geen garantie dat de groep 'stapsgewijs op te bouwen' is uit kleinere groepen. Deze aanpak werkt echter goed voor zogenaamde *oplosbare groepen*.

10.14. Definitie. *Een eindige groep G heet oplosbaar indien er een keten van ondergroepen*

$$G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_k = 1$$

in G bestaat waarvoor steeds H_{i+1} normaal is in H_i en H_i/H_{i+1} cyclisch van priemorde.

De historische aanleiding tot deze naamgeving is een verband met het oplossen van polynoomvergelijkingen door worteltrekkingen dat we later in de *Galoistheorie* tegen zullen komen. De *oplosbaarheidsketen* in 10.14 is niet altijd uniek.

Opgave 5. Laat zien dat S_3 een unieke oplosbaarheidsketen heeft, maar C_6 niet.

De stelling van Cauchy 5.14 geeft aanleiding tot cyclische ondergroepen van priemorde. Als men niet gehinderd wordt door normaliteitsproblemen, bijvoorbeeld omdat de groep in kwestie abels is, geeft dit inductief aanleiding tot oplosbaarheid.

10.15. Propositie. *Eindige abelse groepen zijn oplosbaar.*

Bewijs. We voeren het bewijs met inductie naar de groepsorde. Voor $G = 1$ is er niets te bewijzen. Voor G niet-triviaal bestaat er wegens Cauchy een element $x \in G$ van priemorde. De ondergroep $H = \langle x \rangle$ is normaal in G omdat G abels is, en de factorgroep G/H is wegens de inductiehypothese oplosbaar. Schrijf de bijbehorende keten van ondergroepen als $G/H = M_0 \supset M_1 \supset M_2 \supset \ldots \supset M_k = H/H = 1$. Wegens 8.1 hebben we $M_i = H_i/H$ voor ondergroepen $H_i \supset H$ van G, en de quotiënten $H_i/H_{i+1} \cong M_i/M_{i+1}$ zijn cyclisch van priemorde. De keten

$$G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_k = H \supset 1$$

laat nu zien dat G oplosbaar is. □

Merk op dat 10.15 ook direct uit de structuurstelling 9.11 volgt. Het gegeven bewijs is echter interessant omdat het abels zijn van G slechts wordt gebruikt om normaliteit van de ondergroep $H = \langle x \rangle$ te garanderen.

Opgave 6. Laat zien dat A_4 geen normale ondergroepen van priemorde heeft.

Een normale ondergroep van priemorde bestaat altijd als G een *p-groep* is, d.w.z. een eindige groep G waarvan de orde een macht van een priemgetal p is.

10.16. Lemma. *Zij G een eindige p-groep. Dan geldt $Z(G) \neq 1$.*

Bewijs. We laten G op zichzelf werken door conjugatie. De dekpunten onder deze werking zijn de elementen in het centrum van G, en congruentie 5.15 levert ons $\#Z(G) \equiv \#G \equiv 0 \bmod p$. De orde van $Z(G)$ is dus deelbaar door p. □

Voor een element $x \in Z(G)$ is de ondergroep $H = \langle x \rangle$ conjugatie-invariant en dus normaal in G. Voor een p-groep G blijft het bewijs van 10.15 daarom geldig met als enige wijziging dat men voor de voortbrenger x van H een element van orde p in $Z(G)$ neemt.

10.17. Stelling. *Iedere eindige p-groep is oplosbaar.* □

Voor het geval van de 2-groep $D_4 = \langle \rho, \sigma \rangle$ van orde 8 zijn er diverse oplosbaarheidsketens. De keten $D_4 \supset \langle \rho \rangle \supset Z(D_4) = \langle \rho^2 \rangle \supset 1$ bestaat uit normaaldelers in D_4, de keten $D_4 \supset \langle \rho^2, \sigma \rangle \supset \langle \sigma \rangle \supset 1$ heeft een niet-normale ondergroep van orde 2.

Opgave 7. Laat zien dat iedere p-groep een oplosbaarheidsketen van normaaldelers toelaat.

▶ Simpele groepen

De strategie om G te analyseren via zijn normaaldelers heeft alleen kans van slagen als G een niet-triviale normaaldeler bezit. Voor de meeste kleine groepen die niet van priemorde zijn kan men zonder al te veel moeite bewijzen dat ze een niet-triviale normaaldeler bezitten. Dit leidt tot de volgende bekende stelling, waarvan we het bewijs als opgave aan de lezer laten.

10.18. Stelling. *Iedere groep van orde $n < 60$ is oplosbaar.* □

De alternerende groep A_5 van orde $60 = 2^2 \cdot 3 \cdot 5$ is niet oplosbaar. Uit 5.11 leidt men namelijk gemakkelijk af dat de klassenformule uit opgave 5.42 voor A_5 gegeven wordt door $60 = 1 + 15 + 20 + 12 + 12$. Iedere normaaldeler $N \triangleleft A_5$ is een vereniging van conjugatieklassen die de klasse van het eenheidselement (van orde 1) bevat. Omdat daarnaast de orde van N een deler van 60 is volgt gemakkelijk dat alleen de triviale gevallen $N = 1$ en $N = A_5$ op kunnen treden.

Dit argument laat niet alleen zien dat A_5 geen oplosbaarheidsketen heeft, maar helemaal geen niet-triviale normaaldelers. Een groep $G \neq 1$ met deze eigenschap heet een *simpele groep*. Iedere eindige groep G laat een keten

$$G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_k = 1$$

toe waarvoor steeds H_{i+1} normaal is in H_i en het quotiënt H_i/H_{i+1} simpel. Als G triviaal of simpel is, is deze uitspraak direct duidelijk. Voor $G \neq 1$ niet simpel neemt men een niet-triviale normaaldeler $N \triangleleft G$, en maakt inductief een keten voor G uit een keten voor N en het onder $G \to G/N$ teruggehaalde beeld van een keten voor G/N. Iedere eindige groep kan dus worden opgebouwd uit 'simpele stapjes', en de oplosbare groepen zijn precies degenen waarvoor alleen cyclische priemstapjes nodig zijn. In enigszins fysisch aandoende terminologie kan men stellen dat de simpele groepen de 'elementaire bouwstenen' van de eindige groepentheorie zijn.

Opgave 8. Laat zien dat een abelse simpele groep cyclisch van priemorde is.

Niet-abelse simpele groepen zijn relatief zeldzaam. Het eerste voorbeeld na A_5 van een niet-abelse simpele groep is de groep $\mathrm{SL}_2(\mathbf{F}_7)/\{\pm 1\}$, die orde 168 heeft. De in de jaren '50 ondernomen *classificatie van eindige simpele groepen* is één van de grootste projecten in de groepentheorie geweest. Deze classificatie zegt dat er naast een aantal bekende oneindige families van simpele groepen, zoals de groepen van priemorde en de alternerende groepen A_n voor $n \geq 5$, precies 26 eindige simpele groepen bestaan. De laatste van deze 26 zogenaamde *sporadische simpele groepen* zijn pas rond 1970 gevonden en hebben exotische namen als *monster* en *baby monster*. Het vele duizenden bladzijden tellende bewijs van de correctheid van de classificatie is verspreid over enige honderden artikelen die gedeeltelijk nog ongepubliceerd zijn. Ten einde de status van dit 'bewijs' te verbeteren is er een 'revisieproject' gestart dat zich ten doel stelt een nieuw en compleet bewijs[38] te publiceren.

Opgaven

9. Stel dat een semidirect product $N \rtimes_\phi H$ abels is. Bewijs dat N en H abels zijn en dat de afbeelding $\phi : H \to \mathrm{Aut}(N)$ triviaal is.

10. Zij $1 \to N \xrightarrow{f} G \to H \to 1$ een exact rijtje van groepen, en stel dat f een sectie $p : G \to N$ toelaat. Bewijs dat G isomorf is met $N \times H$.

11. Zij gegeven een extensie $1 \to A \to G \to H \to 1$ waarin A abels is, en stel dat de extensie splitst. Laat zien dat de conjugatiewerking $H \to \mathrm{Aut}(A)$ onafhankelijk is van de keuze van de sectie $s : H \to G$. [Vergelijk met 4.4.]

12. Laat zien dat er in de voorafgaande opgave ook een natuurlijke conjugatiewerking $H \to \mathrm{Aut}(A)$ is als de extensie *niet* splitst. Beschrijf deze werking voor $A = \langle i \rangle \subset G = Q$ en $H = Q/A \cong \mathbf{Z}/2\mathbf{Z}$.

13. Laat zien dat er voor ieder exact rijtje $1 \to N \to G \to H \to 1$ een geïnduceerd homomorfisme $H \to \mathrm{Out}(N)$ is, met $\mathrm{Out}(N)$ als in opgave 4.55.

14. Zij G een groep en $\phi : G \to \mathrm{Aut}(G)$ de conjugatiewerking van G op zichzelf. Bewijs dat het semidirecte product $G \rtimes_\phi G$ isomorf is met het directe product $G \times G$.
[Hint: kies een 'betere' sectie $G \to G \rtimes_\phi G$ om te zien dat dit minder onwaarschijnlijk is dan het op het eerste gezicht lijkt.]

15. Zij p een priemgetal. Bewijs dat $C_p \times C_p$ en C_{p^2} op isomorfie na de enige groepen van orde p^2 zijn.

16. Zij G een niet-abelse groep van orde p^3 met p priem. Bewijs dat $Z(G) = [G, G]$ van orde p is, en dat er een isomorfisme $G/Z(G) \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ is.

17. Bewijs dat de dihedrale groep D_n oplosbaar is voor $n \geq 1$.

18. Zij G een eindige groep en $N \lhd G$ een normaaldeler. Bewijs dat G oplosbaar is dan en slechts dan als N en G/N het zijn.

19. Zij A een abelse groep van orde n. Bewijs dat er voor iedere deler m van n een ondergroep $B \subset A$ van orde m is.

20. Zij p een priemgetal. Laat zien dat de conjugatieactie van G op $X = \mathrm{Syl}_p(G)$ transitief is. Wat is de kern van de corresponderende afbeelding $G \to S(X)$?

21. Laat zien dat de reguliere werking van G op de verzameling $X = G/P$ met $P \in \mathrm{Syl}_p(G)$ transitief is. Wat is de kern van de corresponderende afbeelding $G \to S(X)$? Zijn $\mathrm{Syl}_p(G)$ en G/P isomorf als G-verzamelingen?

22. Bepaal voor de priemen p die de groepsorde delen de aantallen Sylow-p-ondergroepen in A_4 en A_5 en hun structuur.

23. Bepaal voor elke deler d van 24 het aantal ondergroepen in S_4 van orde d. Welke van deze ondergroepen zijn normaal?

24. Zij $\mathcal{C}$ de conjugatieklasse van $(12)(34) \in S_n$. Bewijs dat voor $n \in \{4, 5\}$ de afbeelding $x \mapsto N_x$ (de normalisator van x) een bijectie $\mathcal{C} \longrightarrow \mathrm{Syl}_2(S_n)$ geeft.

25. Laat zien dat iedere groep van orde 200 een niet-triviale normaaldeler bevat.

26. Laat zien dat er precies vier isomorfieklassen van groepen van orde 30 zijn: de cyclische groep C_{30} en de niet-abelse groepen D_{15}, $D_3 \times C_5$ en $D_5 \times C_3$.

27. Zij G een groep van orde pq^n voor $p < q$ beide priem en $n \geq 1$. Bewijs: G is oplosbaar[39]. [De *p-q-stelling van Burnside* zegt dat dit tevens het geval is voor groepen van orde $p^m q^n$.]

28. Zij G een groep van orde $2n$ met n oneven. Bewijs dat er een isomorfisme $G \cong N \rtimes C_2$ is voor een normaaldeler $N \triangleleft G$ van orde n.

29. Zij G een groep van even orde, en stel dat de Sylow-2-ondergroepen van G cyclisch zijn. Bewijs dat G een normaaldeler van index 2 bevat.

30. Zij p priem en $G_p = \mathrm{Aff}(\mathbf{Z}/p\mathbf{Z})$ de affiene groep over $\mathbf{Z}/p\mathbf{Z}$. Bewijs dat G_p voor iedere priemdeler $q|p-1$ een unieke ondergroep van orde pq bevat, en dat deze niet abels is.

31. Zij p een priemgetal en $H_p \subset \mathrm{GL}_n(\mathbf{F}_p)$ een Sylow-p-ondergroep. Bewijs: H_p is geconjugeerd met de ondergroep van bovendriehoeksmatrices van de vorm

$$\begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix}.$$

32. Bewijs stelling 10.18.

*33. Zij G een simpele groep van orde 60. We gaan bewijzen dat G isomorf is met A_5.
   a. Zij $n > 1$ de *minimale* index van een echte ondergroep $H \subsetneq G$. Bewijs: er geldt $n \geq 5$, en $G \cong A_5$ als $n = 5$.
   b. Bewijs: G heeft $n_3 = 10$, $n_5 = 6$, en $n_2 \in \{5, 15\}$; in het geval $n_2 = 5$ geldt $G \cong A_5$.
   c. Bewijs: ieder tweetal verschillende Sylow-2-groepen H_2 en H_2' in G heeft doorsnede $H_2 \cap H_2' = 1$. Concludeer: $n_2 \neq 15$, dus $G \cong A_5$ wegens b.
   [Hint: kijk naar de normalisator van $H_2 \cap H_2'$.]

*34. Bewijs dat A_n simpel is voor $n \geq 5$.
[Hint: Neem $N \triangleleft A_n$ niet-triviaal en $n \geq 5$. Voor iedere ondergroep $G_i = \{\sigma \in A_n : \sigma(i) = i\} \cong A_{n-1}$ geldt dan $N \cap G_i = 1$, en N heeft orde n. Het beeld van de Cayleyafbeelding $N \to S(N)$ is nu een normaaldeler van de groep $\mathrm{Alt}(N)$ van even permutaties van de verzameling N, en iedere even permutatie van N die het eenheidselement vasthoudt is een automorfisme.]

35. Zij G een groep van orde 255. Bewijs dat G cyclisch is.
[Een groot verschil derhalve tussen $I(255) = I(257) = 1$ en $I(256)$.]

*36. Zij G een eindige groep, en stel dat iedere *maximale* ondergroep van G abels is. Bewijs dat G oplosbaar is.
[Men noemt een ondergroep $H \subset G$ maximaal als $H \neq G$ geldt, en iedere ondergroep $H' \supsetneq H$ van G gelijk is aan G.]

37. Zij n een positief geheel getal. Bewijs dat equivalent zijn:
   i. $I(n) = 1$;
   ii. $I(d) = 1$ voor iedere deler d van n;
   iii. iedere groep van orde n is cyclisch;

iv. n is onderling ondeelbaar met $\varphi(n)$.

38. Bepaal alle isomorfieklassen van groepen van orde 20 en 28. Generaliseer naar orde $4p$ voor $p > 3$ priem.

39. Zij $G \neq 1$ een groep met $\mathrm{Aut}(G) = 1$.
    a. Stel dat G eindig is. Bewijs: $\#G = 2$.
       [Hint: Bewijs eerst dat G abels is, kijk dan naar inversie.]
    b. Laat zien dat de aanname in a dat G eindig is in feite overbodig is.

40. Zij A een eindig voortgebrachte abelse groep. Bewijs dat $\mathrm{Aut}(A)$ eindig is dan en slechts dan als de vrije rang van A niet groter is dan 1.

41. Zij G een groep van orde $n = pq^2$ met $p < q$ priem. Bewijs: als p geen deler is van $q^2 - 1$, dan is G abels, en er zijn twee isomorfieklassen van groepen van orde pq^2. Wat is de kleinste waarde van n die aan deze voorwaarden voldoet?

42. Laat zien dat ieder automorfisme van de optelgroep $\mathbf{Q}$ van de vorm $x \mapsto ax$ is met $a \in \mathbf{Q}^*$. Concludeer: $\mathrm{Aut}(\mathbf{Q}) \cong \mathbf{Q}^*$.

43. Laat zien dat voor $n \geq 1$ kwadraatvrij en $G = (\mathbf{Z}/n\mathbf{Z})^k$ er een isomorfisme $\mathrm{Aut}(G) \cong \mathrm{GL}_k(\mathbf{Z}/n\mathbf{Z})$ is.

44. Laat zien dat $\mathrm{Aut}(C_2 \times C_4)$ een elementair abelse 2-groep van orde 8 is.

45. Laat zien dat er voor $n > 2$ een isomorfisme $\mathrm{Aut}(D_n) \cong \mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ is, met $\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ de affiene groep uit 8.12.4.

46. Laat zien dat het kransproduct $C_p \wr C_2$ orde $2p^2$ heeft, en ga na welk van de groepen uit 11.7 dit is voor $p > 2$ priem.

47. Zij p een priemgetal en $B_p \subset \mathrm{GL}_3(\mathbf{F}_p)$ de groep van matrices van de vorm

$$M_{i,j,k} = \begin{pmatrix} 1 & i & j \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{met } i, j, k \in \mathbf{F}_p.$$

    Bewijs dat B_p een niet-abelse groep van orde p^3 is, en dat B_p het semidirecte product is van $N = \{M_{i,j,0} : i, j \in \mathbf{F}_p\} \subset B_p$ met $H = \{M_{0,0,k} : k \in \mathbf{F}_p\} \subset B_p$. Welke groep van orde 8 is B_2? En welk van beide groepen in stelling 11.8 is B_p voor $p > 2$?

48. Zij Q de quaternionengroep, $x \in Q$ een element van orde 4 en $y \in Q$ een element van $Q \setminus \langle x \rangle$. Bewijs dat er een automorfisme $\phi \in \mathrm{Aut}(Q)$ is met de eigenschappen $\phi(i) = x$ en $\phi(j) = y$, en dat $\mathrm{Aut}(Q)$ orde 24 heeft.

49. Laat zien dat ieder automorfisme van Q een automorfisme induceert van $Q/Z(Q) \cong V_4$, en dat dit tot een exact rijtje $1 \to K \to \mathrm{Aut}(Q) \to \mathrm{Aut}(Q/Z(Q)) \to 1$ aanleiding geeft. Bewijs dat K een groep is isomorf met V_4 en bestaat uit de identiteit en de automorfismen van Q die precies twee van de drie elementen $i, j, k \in Q$ naar hun inverse sturen. Leid hieruit af dat er een isomorfisme $\mathrm{Aut}(Q) \cong S_4$ is.

*50. Zij V de reële 3-dimensionale vectorruimte met basis $\{i, j, k\}$ en $\mathrm{Aut}(Q) \to \mathrm{GL}(V)$ de natuurlijke lineaire werking van $\mathrm{Aut}(Q)$ op V. Bewijs dat $\mathrm{Aut}(Q)$ de vier 1-dimensionale

vectorruimtes opgespannen door elk van de elementen van de vorm $i \pm j \pm k$ permuteert, en dat dit aanleiding geeft tot een isomorfisme $\mathrm{Aut}(Q) \cong S_4$.

51. Bepaal $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ voor $G = Q$ en voor $G = D_n$.

52. Zij N een abelse groep, en stel dat H_1 en H_2 geconjugeerde ondergroepen van $\mathrm{Aut}(N)$ zijn. Bewijs dat er een isomorfisme $N \rtimes H_1 \cong N \times H_2$ is.

*53. Bepaal de isomorfieklassen van de groepen van orde 24.
[Hint: er geldt $n_2 \in \{1, 3\}$ en $n_3 \in \{1, 4\}$. Er zijn 5 groepen met $n_2 = n_3 = 1$ wegens 10.5; er zijn slechts 2 groepen van orde 8 met een een automorfisme van orde 3, *dus* 2 groepen met $n_2 = 1$ en $n_3 = 4$; er zijn 7 groepen met $n_2 = 3$ en $n_3 = 1$; de enige groep met $n_2 = 3$ en $n_3 = 4$ is S_4. Dit laatste ziet men in door de conjugatieactie van de groep op zijn Sylow-3-ondergroepen te beschouwen.]

54. De groep $G = \mathrm{GL}_2(\mathbf{F}_3)$ van orde 48 heeft een factorgroep $\mathrm{PSL}_2(\mathbf{F}_3) = G/\{\pm 1\}$ en een ondergroep $\mathrm{SL}_2(\mathbf{F}_3)$ die elk orde 24 hebben. Bepaal voor elk van deze beide groepen n_2 en n_3, alsmede hun plaats in het lijstje uit de vorige opgave.

55. Zij p een priemgetal en G een elementair-abelse p-groep van rang k. Bewijs: $\mathrm{Aut}(G)$ is isomorf met de groep $\mathrm{GL}_k(\mathbf{F}_p)$ van inverteerbare $k \times k$-matrices over $\mathbf{F}_p$, en heeft orde $\prod_{i=0}^{k-1}(p^k - p^i)$.

56. Zij p een oneven priemgetal en G een niet-abelse groep van orde $2p^2$. Bewijs: G is isomorf met de diëdergroep D_{p^2}, het directe product $C_p \times D_p$ of het semidirecte product $(C_p \times C_p) \rtimes C_2$ met betrekking tot de inversie-actie van C_2 op $C_p \times C_p$. Concludeer: $I(2p^2) = 5$.

57. Zij p een oneven priemgetal. Bewijs dat er een niet-abelse groep van orde p^3 bestaat waarin elk element $x \neq e$ orde p heeft. *Is deze groep op isomorfie na uniek bepaald?

*58. Zij p een oneven priemgetal en G een niet-abelse groep van orde p^3 die een element van orde p^2 bevat. Bewijs: G is isomorf met het semidirecte product $C_{p^2} \rtimes C_p$ van C_{p^2} met de unieke ondergroep $C_p \subset \mathrm{Aut}(C_{p^2})$.

59. Bewijs: $I(p^3) = 5$ voor ieder priemgetal p.

Tabel van kleine groepen

orde	abels	niet-abels
1	C_1	
2	C_2	
3	C_3	
4	C_4, V_4	
5	C_5	
6	C_6	D_3
7	C_7	
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$	D_4, Q
9	C_9, $C_3 \times C_3$	
10	C_{10}	D_5
11	C_{11}	
12	C_{12}, $C_6 \times C_2$	A_4, D_6, $C_3 \rtimes_\phi C_4$
13	C_{13}	
14	C_{14}	D_7
15	C_{15}	

Notatie:

A_n : de alternerende groep op n symbolen
C_n : een cyclische groep van orde n
D_n : de diëdergroep van orde $2n$
Q : de quaternionengroep
V_4 : de viergroep van Klein

Rechtvaardiging:

orde 1: opgave
ordes 2, 3, 5, 7, 11, 13: opgave 4.8
ordes 4 en 9: stelling 10.4(1)
ordes 6, 10 en 14: stelling 10.4(3)
orde 8: stelling 10.5
orde 12: stelling 10.13
orde 15: stelling 10.4(2)

Literatuurverwijzingen

De verwijzingen in dit deel van de syllabus geven een handvat om zelfstandig in een wiskundebibliotheek rond te neuzen zonder direct door de bomen het bos niet meer te zien. De hier verzamelde referenties variëren van populair-wetenschappelijke artikelen, zoals men die in tijdschriften als *Scientific American* en de *Mathematical Intelligencer* vindt, tot leerboeken en onderzoeksartikelen. Verwacht niet alles in één keer te begrijpen—er is meer wiskunde dan een mensenhoofd kan bevatten.

Nederlandstalige wiskunde van enig niveau is uiterst schaars, want Nederlanders drukken zich te pas en te onpas uit in het Engels. Iets oudere literatuur of boeken met grotere oplage zijn vaak in één van onze beide andere buurtalen, Duits en Frans, geschreven of vertaald. Voor wie meer Europees dan provinciaal georiënteerd is, kan dat geen groot bezwaar zijn. Zie eventueel de Europese pagina voor een paar lastige woorden.

1. Er is geen reden om het bij voorbaat eens te zijn met mijn definitie van algebra. Vorm een eigen oordeel door één van de vele boeken met de titel 'Algebra' van de plank te trekken en eens door te bladeren. Ik noem een aantal boeken die het inkijken meer dan waard zijn, nu en in de loop van je studie. Naarmate ons college vordert wordt waarschijnlijk duidelijker waar al deze boeken over gaan. Wie elk half jaar opnieuw kijkt kan zien hoe zijn kennis groeit.

- M. Artin, *Algebra*. Prentice Hall, 1991.

Een aardig modern boek, enigszins in de geest van deze tekst. Sla hoofdstuk 1 gewoon over.

- I. R. Shafarevich, *Algebra I. Basic notions of algebra*. Encyclopaedia of Mathematical Sciences 11, Springer, 1990.

Geen eerstejaars tekstboek, maar panoramisch geschreven. De standaardvolgorde 'groepen-ringen-lichamen' wordt in dit boek omgedraaid. Een goed medicijn voor wie denkt dat de wiskunde uit losse onderdelen bestaat die weinig met elkaar of de andere exacte wetenschappen te maken hebben.

- S. Lang, *Algebra*. Springer, revised 3rd edition, 2002.

Een standaardreferentie voor de moderne algebra die door velen gebruikt wordt. Iedere nieuwe editie is dikker dan de vorige—de laatste heeft ruim 900 bladzijden.

- M. A. Armstrong, *Groups and symmetry*, Springer UTM, 1988.

Een leesbaar, niet te dik boekje dat ongeveer dezelfde onderwerpen behandelt als deze syllabus.

- J. A. Gallian, *Contemporary Abstract Algebra*, D. C. Heath and Company, 6th edition, 2005.

Een representant uit de Amerikaanse cultuur van 'college texts'. Minder zwaar op de hand dan voorafgaande teksten, vol citaten, computerprogramma's en biografieën van wiskundigen die een belangrijke bijdrage hebben geleverd aan het ontstaan van de moderne algebra. Om de paar jaar verschijnt er een 'nieuwe' editie.

- B.L. van der Waerden, *Algebra*, Springer, 1930. Diverse edities sinds de eerste Duitse uitgave, nu ook in het Engels.

Het eerste moderne algebraboek. Nog steeds de moeite waard.

2. Wie geïnteresseerd is in de tragisch verlopen levens van een aantal grondleggers van de groepentheorie zoals Galois en Abel kan voor geromantiseerde, enigszins oppervlakkige verhalen terecht bij Bell. Bondiger zijn de schetsjes in het ten zeerste aanbevolen geschiedenisboekje

van Stillwell. Voor uitgebreidere biografische gegevens is er het laatstgenoemde standaardwerk, een uittreksel uit de *Dictionary of Scientific Biography*.

- E.T. Bell, *Men of mathematics,* Simon & Schuster, 1937. Diverse herdrukken.
- J. Stillwell, *Mathematics and its history*, Springer UTM, 1989.
- *Biographical dictionary of mathematicians*, 4 vols, Scribner's, New York, 1991.

3. In de negentiende eeuw werden permutaties ook wel 'substituties' genoemd. Wie oude wiskundeliteratuur leuk vindt kan eens kijken in Netto's boek, en het vervolgens vergelijken met de moderne tekst van Dixon en Mortimer.

- E. Netto, *Substitutionentheorie und ihre Anwendungen auf die Algebra*, Teubner, 1882. Er is een Engelse vertaling, herdrukt bij Chelsea.
- J. D. Dixon, B. Mortimer, *Permutation groups*, Springer, 1996.

4. De mededeling dat twee permutaties in S_n 'al snel' de hele groep (of in ieder geval A_n) voortbrengen krijgt een precieze betekenis in onderstaand artikel.

- John D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110**, 199–205 (1969).

5. Sam Loyd's puzzeltje staat bekend als *Sam Loyd's Fifteen*. Onderstaand boek ging onder meer de geschiedenis na, en claimt dat de Amerikaanse postbeambte Noyes Chapman de eigenlijke uitvinder is. Zie ook www.daviddarling.info/encyclopedia/F/Fifteen_Puzzle.html.

- Jerry Slocum, Dic Sonneveld. *The 15 Puzzle*, Slocum Puzzle Foundation: 2006.

6. Over Rubik's kubus is veel geschreven, van oplosmethodes tot lijsten van 'mooie patronen'. Bekijk in onderstaande referenties 'van het eerste uur' de literatuurverwijzingen, of kijk op www.rubiks.com.

- J. van de Craats, *De magische kubus van Rubik*, De Muiderkring, 1981.
- D. Hofstadter, *Metamagical Themas*, Scientific American **244**, 20–39 (1981).

7. De partitiefunctie $p(n)$, die al bestudeerd werd door Euler, groeit nogal snel met n. Er geldt

$$p(n) \approx e^{\pi\sqrt{2n/3}}/(4n\sqrt{3}).$$

Opgave 2.59 laat zien dat de waarden van $p(n)$ de machtreekscoëfficiënten zijn van een eenvoudige *genererende functie*. Studie van deze functie, die in essentie een *modulaire vorm* is, heeft in deze eeuw geleid tot representaties van $p(n)$ die de functie ook voor grote n berekenbaar maken. De waarden van $p(n)$ voor zulke n, waarin niemand ooit enige bijzondere structuur met betrekking tot hun delers heeft gevonden, worden als test-input gebruikt voor *factorisatiealgoritmen* zoals genoemd in §7. Hoofdstuk XIX in de volgende klassieke referentie geeft enige details, hoofdstuk 7 in Grosswald is moderner.

- G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 1938. Er zijn diverse verbeterde herdrukken.
- E. Grosswald, *Topics from the Theory of Numbers*, 2nd edition, Birkhäuser, 1984.

8. Voor de maximale orde $g(n)$ van een element in S_n in opgave 2.60 geldt voor grote n de relatie $\log g(n) \approx \sqrt{n}\log n$. Omdat je in essentie n als een som van een boel kleine priemgetallen wilt schrijven is het niet verwonderlijk dat Landau's boek een bewijs van dit resultaat geeft,

in §61. Andere interessante eigenschappen van de functie $g(n)$, zoals het feit dat er willekeurig lange intervallen bestaan waarop g constant is, vind je in het artikel van Nicolas.

- E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, 1909. Heruitgave: Chelsea, New York, 1953.
- J.-L. Nicolas, *Sur l'ordre maximum d'un élément dans le groupe S_n des permutations*, Acta Arithm. **14**, 315–332 (1967/68).

9. De Sinterklaaslootjesobservatie in opgave 2.63 komt in veel varianten voor en gaat terug tot Montmort (1708). Lees hierover de pagina's 99–101 in onderstaand boek, dat veel interessant materiaal bevat voor wie van combinatorische problemen houdt.

- W. Feller, *An introduction to probability theory*, Wiley, 1950.

10. Het bestaan van enantiomeren is van belang in scheikunde en biologie. Wie zelf wil weten waarom het al dan niet nuttig is om rechtsdraaiende yoghurt te eten raadplege zijn scheikundeboeken.

11. Het Erlanger Programm van Felix Klein maakte de groep tot een centraal en unificerend wiskundig concept. Later ontwikkelde takken van meetkunde, zoals de algebraïsche meetkunde, passen niet direct binnen het programma van Klein.

- F. Klein, *Vergleichende Betrachtungen über neuere geometrische Forschungen*, Math. Annalen **43**, 63–100 (1893).

Voor een 'historische evaluatie' van het Erlanger Programm, en algemener een goed historisch perspectief op wiskundige ideeën, is er een klassiek werk, in voordelige pocketeditie beschikbaar.

- M. Kline, *Mathematical thought from ancient to modern times*, Oxford University Press, 1972. Paperback edition, 1990.

12. Voor wie zich wil vermaken met begrippen als oriëntatie, binnen en buiten en andere topologische concepten in het platte vlak is er een klassiek science fiction-achtig boekje, dat nu ook verfilmd is (www.flatlandthemovie.com). Verkrijgbaar als Dover-pocket, maar ook in een recente geannoteerde editie. Zie voor een recensie www.ams.org/notices/200210/rev-dewdney.pdf.

- E. A. Abbott, *Flatland*, 1882. Heruitgave: *The annotated Flatland, a romance of many dimensions*, introduction and notes by Ian Stewart, The Perseus Press, 2002.

13. De eindige ondergroepen van de rotatiegroep $O_3^+(\mathbf{R})$ in 3 dimensies zijn, naast de groepen C_n en D_n die door realisaties van vlakke symmetrieën als ruimtelijke rotaties ontstaan, alleen de groep $T^+ \cong A_4$ van rotaties van de tetraëder, de draaiingsgroep K^+ van de kubus, en de groep $\mathrm{Icos}^+ \cong A_5$ van rotaties van een regelmatig twaalf- of twintigvlak. Zie hiervoor de onder referentie **1** genoemde boeken van Artin (stelling V.9.1) of Armstrong (hoofdstuk 19). Met een beetje extra werk krijgt men hieruit een beschrijving van alle eindige ondergroepen van de orthogonale groep $O_3(\mathbf{R})$ in 3 dimensies, zie de pagina's 276–277 in onderstaand boek.

- H. S. M. Coxeter, *Introduction to Geometry*, Wiley, New York, 1969.

14. Het idee dat veel 'standaardconstructies' in de wiskunde op een soort universele manier beschreven kunnen worden heeft geleid tot het concept van categorieën. Veel resultaten in deze hoek staan te boek als 'abstract nonsense'. Onze isomorfiestelling 4.9 en soortgelijke stellingen in §8 als de homomorfiestelling 8.4 zijn representatieve voorbeelden. Veel moderne

algebraboeken hebben een paragraaf over categorieën. Het betreft meer een taalgebruik dan een theorie.

- P. J. Hilton, U. Stammbach, *A course in homological algebra*, Springer GTM 4, 1971.
- S. MacLane, *Categories for the working mathematician*, Springer GTM 5, 1971.

15. De actie van de modulaire groep $\mathrm{SL}_2(\mathbf{Z})$ op het complexe bovenhalfvlak is één van de fundamentele groepswerkingen in de algebra en de complexe analyse. Deze werking en zijn varianten geven aanleiding tot de theorie van *modulaire functies* en *modulaire vormen*. De rijke verbanden met getaltheorie, meetkunde en complexe analyse maken dit tot een centraal en intensief bestudeerd deel van de wiskunde. De populariteit ervan is nog eens toegenomen na het verschijnen van Wiles' bewijs van de laatste stelling van Fermat – zie verwijzing **22**. Hoofdstuk VII van Serre's boekje geeft een compacte inleiding.

- J.-P. Serre, *A course in arithmetic*, Springer GTM 7, 1973. [Dit is de Engelse vertaling van *Cours d'arithmétique*, Presses Universitaires de France, 1970.]

16. De constructie van *quotiëntruimtes* of *identificatieruimtes* komt men in meetkunde en topologie tegen. Stillwell's boekje, dat tevens een aardige inleiding bevat over overeenkomsten en verschillen tussen Euclidische, sferische en hyperbolische meetkunde, is toegankelijk en heeft veel plaatjes.

- J. Stillwell, *Geometry of surfaces*, Springer Universitext, 1992.

17. De beste gepubliceerde afschatting van de functie $I(n)$ in opgave 5.40 schijnt $I(n) < n^k$ met $k = \mathrm{cst} \cdot n^{2/3} \log n$ te zijn.

- P. X. Gallagher, *Counting finite groups of given order*, Math. Zeitschrift **102**, 236–237 (1967).

18. Het blijkt dat men groepen soms goed kan bestuderen door ze te laten werken op zogenaamde 'bomen'. Zie hiervoor het onder **1** genoemde boek van Armstrong (Chapter 28), alsook onderstaand boek van Serre. Serre geeft een voorbeeld van een oneindige groep met precies twee conjugatieklassen in I.1.4.

- J.-P. Serre, *Trees*, Springer, 1980. [Dit is de Engelse vertaling van *Arbres, amalgames,* SL_2, Astérisque **46** (1977).]

19. De axiomatische beschrijving van de natuurlijke getallen door Peano gaat uit van een 'verzameling' $\mathbf{N}$ van 'natuurlijke getallen' met een begrip 'opvolger'. De axioma's zeggen achtereenvolgens dat er een natuurlijk getal '0' is, dat ieder natuurlijk getal een opvolger heeft, dat zo'n opvolger nooit 0 is, en dat getallen met dezelfde opvolger gelijk zijn. Tenslotte volgt het bekende *axioma van volledige inductie*. Zie het onder **11** genoemde boek van Kline of een logicaboek naar keuze.

20. Er zijn eindeloos veel open problemen met betrekking tot de elementaire eigenschappen van de gehele getallen.

- D. Shanks, *Solved and unsolved problems in number theory*, Chelsea, New York, 3rd edition, 1985.

21. De *Elementen* van Euclides vormden eeuwenlang de bijbel van de wiskunde, en na de echte bijbel de bestseller van de boekdrukkunst. De klemtoon op de tweede lettergreep in *Euclídes* is ook al eeuwen oud – maar niet iedereen lijkt dat nog te weten.

Er zijn erg veel edities van de Elementen, onder meer een Dover-pocket in 3 delen met commentaar van Heath en een handzaam Duits deeltje van de Wissenschaftliche Buchgesellschaft. De boeken VII-IX behandelen getaltheorie, en wie zich niet door de meetkundige formuleringen van de wijs laat brengen vindt diverse stellingen uit §6 terug. Stelling 6.5 = IX, §20. Lemma 6.6 = VII, §30. Stelling 6.7 komt alleen als speciaal geval voor: IX, §14. Wie liever een klassieke stelling als de *stelling van Pythagoras* naslaat: I, §47. Zie voor meer informatie ook de desbetreffende paragraaf in het in **11** genoemde boek van Kline.

22. De beroemde laatste stelling van Fermat, die meer dan 350 jaar een open probleem is geweest, is uiteindelijk bewezen door Andrew Wiles. Er is veel publiciteit rond dit bewijs geweest, en de BBC maakte er een aardige documentaire over. De stelling werd aan het eind van de jaren tachtig door Ribet afgeleid uit een onbewezen vermoeden over *elliptische krommen* dat onder de naam Shimura-Taniyama-vermoeden bekend staat. Wiles' artikel, dat een belangrijk deel van dit vermoeden bewijst, sluit niet naadloos aan op dit college. De proceedings van de grote Boston-conferentie in 1995 over Wiles' bewijs bevatten aanvullende informatie en de eerste vereenvoudigingen van het bewijs.

- K. A. Ribet, *From the Taniyama-Shimura conjecture to Fermat's last theorem*, Ann. Fac. Sci. Toulouse Math. (5) 11 no. 1, 116–139 (1990).
- A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141**(3), 443–551 (1995).
- G. Cornell, J. H. Silverman, G. Stevens (eds), *Modular forms and Fermat's last theorem*, Springer, 1997.

23. Een gedegen uitleg van de werking van locaal-globaal-principes behoort tot de *algebraïsche getaltheorie*. Er zijn tamelijk veel boeken over dit onderwerp. Hoofdstuk 3 uit onderstaand boek is redelijk elementair.

- H. E. Rose, *A course in number theory*, 2nd edition, Oxford, 1994.

24. De stelling van Dirichlet over priemen in rekenkundige rijen zegt dat voor $n \geq 1$ en $a \in (\mathbf{Z}/n\mathbf{Z})^*$ er oneindig veel priemgetallen $p \equiv a \bmod n$ bestaan. Met andere woorden: in de rekenkundige rij a, $a+n$, $a+2n$, ... komen oneindig veel priemgetallen voor. De stelling werd in 1837 met methoden uit de complexe functietheorie bewezen door de Duitser Gustav Peter Lejeune Dirichlet (1805–1857).

- H. Davenport, *Multiplicative Number Theory*, 3rd edition, Springer GTM 74, 2000.

25. Mersenne-priemen zijn genoemd naar de Franse monnik Marin Mersenne (1588–1648). De lijst van Mersenne-priemen $M_p = 2^p - 1$ is naar men vermoedt oneindig, maar dit is onbewezen. In april 2009 werd de 47e waarde van p gevonden waarvoor M_p priem is. De grootste Mersenne-exponent is nog steeds de in augustus 2008 gevonden waarde $p = 43\,112\,609$, corresponderend met een priemgetal van bijna dertien miljoen decimale cijfers. Er is een Great Internet Mersenne Prime Search waaraan iedereen met een computer met 'ijdele tijd' deel kan nemen. Zie www.mersenne.org voor de bijbehorende internet-site.

26. Fermat merkte op dat de getallen $F_n = 2^{2^n} + 1$ priem zijn voor $n = 0, 1, 2, 3, 4$. Zijn optimistische gedachte dat dit voor alle n zo zou zijn bleek niet juist: er zijn geen getallen $n > 4$ bekend waarvoor F_n priem is. De rij van getallen $2^{2^n} + 1$ groeit dubbelexponentieel in n, en het vermoeden is dat er slechts eindig veel priemgetallen bij zijn. Zie

www.prothsearch.net/fermat.html voor een 'statusoverzicht', en Chris Caldwell's *Prime Pages* (http://primes.utm.edu) voor allerhande andere informatie over priemgetallen.

27. In 1992 bewezen Alford, Granville en Pomerance dat er oneindig veel Carmichael-getallen bestaan. De voordracht van Pomerance op ons nationale KWG-congres van 1992 is uitgewerkt in het Nieuw Archief.

- C. Pomerance, *Carmichael numbers*, Nieuw Arch. Wisk. (4) 11, no. 3, 199–209 (1993).
- W. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math. **140**, 703–722 (1994).

28. Voor een enigszins algoritmische blik op primaliteit, factorisatie en de eigenschappen van pseudo-priemtests is het boek van Crandall en Pomerance de beste referentie. Het besteedt ook aandacht aan de toepassingen van elliptische krommen op primaliteit en factorisatie. Dunner en meer op de cryptografie gericht zijn de boeken van Koblitz en Buchmann.

Het overzichtsartikel van René Schoof over primaliteitstests in het recent verschenen MSRI-boek over algoritmische getaltheorie geeft niet alleen de AKS-primaliteitstest uit 2002, maar ook een beschrijving van de iets oudere, nog steeds zeer effectieve methoden. Ook het originele AKS-artikel is zeer leesbaar.

- R. Crandall, C. Pomerance, *Prime numbers—a computational perspective*, second edition, Springer, 2005.
- N. Koblitz, *A Course in Number Theory and Cryptography*, Springer GTM 114, 1987. Second edition 1994.
- J. Buchmann, *Einführung in die Kryptographie*, Springer, 1999. In diverse talen vertaald.
- M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Annals of Math. **160**, 781–793 (2004). Online-versie: www.math.princeton.edu/~ annals/issues/2004/Sept2004/Agrawal.pdf.
- J. P. Buhler, P. Stevenhagen (eds), *Algorithmic number theory*, MSRI Publications vol. 44, Cambridge University Press, 2008. Webversie op mijn homepage.

29. Hoewel er zogenaamde 'elementaire bewijzen' van de priemgetalstelling bestaan, maken de meeste bewijzen gebruik van enige geavanceerde functietheorie of functionaalanalyse. Een bewijs van de eerste soort wordt in het onder **7** genoemde boek van Hardy en Wright gegeven. Voor de tweede soort is er meer keus.

- J. Korevaar, *On Newman's quick way to the prime number theorem*, Math. Intelligencer 4, no. 3, 108–115 (1982).
- W. Rudin, *Functional analysis*, McGraw-Hill, 1973.

30. De hier gegeven beschrijving van 'textbook RSA' gaat voorbij aan een aantal details dat belangrijk is om een daadwerkelijk veilig systeem te verkrijgen. Zo vermijdt men tegenwoordig in RSA-implementaties liever al te kleine publieke exponenten.

- D. Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices Amer. Math. Soc. **46**(2), 203–213 (1999).

31. De getallenlichamenzeef is op dit moment één van de meest effectieve methodes om grote getallen te factoriseren. Het onder **28** genoemde MSRI-boek heeft een overzichtsartikel van mijn hand, het Lenstra-boekje heeft meer details. De succesvolle toepassing op de factorisatie van het negende Fermat-getal F_9 is ook goed gedocumenteerd.

- A. K. Lenstra, H. W. Lenstra, Jr. (eds), *The development of the number field sieve*, Springer Lecture Notes 1554, 1993.
- A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61**, no. 203, 319–349 (1993).

32. Er blijkt een onverwacht verband te bestaan tussen 5 mod p en p mod 5: de eerste is een kwadraat in $(\mathbf{Z}/p\mathbf{Z})^*$ dan en slechts dan als de tweede een kwadraat is in $(\mathbf{Z}/5\mathbf{Z})^*$. Dit is een speciaal geval van de kwadratische reciprociteitswet, die wij in 26.4 zullen bewijzen. Deze wet werd in 1744 ontdekt door Euler en in 1796 bewezen door de 19-jarige Gauss. Er zijn bewijzen door 'slim tellen', zoals in het boek van Hardy en Wright uit **6**, en meer conceptuele bewijzen zoals het bewijs dat wij in §26 zullen geven.

33. Het is niet bekend of 5 mod p een primitieve wortel is voor oneindig veel priemgetallen p. Een door de Duitser Emil Artin (1898–1962) uitgesproken vermoeden zegt dat dit wel zo is, en maakt precies hoeveel van zulke priemen men kan verwachten. Onder aanname van een onbewezen vermoeden, de zogenaamde gegeneraliseerde Riemann-hypothese voor de ligging van nulpunten van zeta-functies, kan men Artin's vermoeden bewijzen.

- M. Ram Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer 10, no. 4, 59–67 (1988).

34. Goursat's lemma, dat genoemd is naar de Fransman Edouard Jean-Baptiste Goursat (1858–1936), is bijzonder nuttig in de Galoistheorie. Niet iedereen die het lemma kent, kent het onder deze naam.

35. Het manipuleren van exacte rijtjes wordt meestal tot de *homologische algebra* gerekend. Naast het al in **14** genoemde boek van Hilton en Stammbach is er de herdruk van een klassiek boek van MacLane, één van de grondleggers van het vak.

- S. Maclane, *Homology*, Springer Classics in Mathematics, 1995.

36. Het karakteriseren van objecten als sommen en producten in deze en de twee voorafgaande opgaven door een zogenaamde *universele eigenschap* is een goede gewoonte uit de al onder **14** genoemde categorieëntheorie. Objecten met zo'n karakterisering zijn automatisch op isomorfie na uniek bepaald. Existentie is echter niet verzekerd!

37. Er zijn verschillende artikelen van Bettina Eick en co-auteurs waarin $I(n)$ voor $n < 2000$ wordt bepaald.

- H. U. Besche, B. Eick, E. A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. 12 (2002), no. 5, 623–644.

38. De eerste delen van het nu in boekvorm verschijnende bewijs van de classificatie van eindige simpele groepen zijn inmiddels verschenen. Er is een overzichtsartikel naar aanleiding van het verschijnen van deel 1.

- R. Solomon, *On finite simple groups and their classification*, Notices of the Amer. Math. Soc. **42**(2), 231–239 (1995).

39. De zogenaamde p-q-stelling van Burnside zegt algemener dat iedere groep van orde $p^m q^n$ met p en q priem oplosbaar is. Er is meer groepentheorie voor een bewijs nodig dan deze syllabus bevat. Zie stelling 28.24 in Isaacs voor meer informatie.

- I. M. Isaacs, *Algebra, a graduate course*, Brooks-Cole, 1994.

Europese pagina's

Het lezen van wiskunde in Engels, Frans of Duits vereist, anders dan het schrijven in deze talen, weinig meer dan een basiskennis van de taal in kwestie. De overgrote meerderheid van het wiskundig jargon is min of meer internationaal, en een woord als 'homomorfisme' verschilt in vrijwel geen enkele taal veel van het Nederlandse woord. Er zijn een paar 'lastige' termen waarvan de vertaling niet direct voor de hand ligt. Van de in deze syllabus behandelde termen volgen hieronder de belangrijkste.

Engels

corollary	gevolg
coset	nevenklasse
faithful	trouw
fibre, fiber	vezel
field	lichaam
to generate	voortbrengen
gcd (greatest common divisor)	ggd
glide, glide reflection	glijspiegeling
integer	geheel getal
lcm (least common multiple)	kgv
odd	oneven
orbit	baan
residue class	restklasse
solvable	oplosbaar

Frans

anneau	ring
application	afbeelding
corps	lichaam
de type fini	eindig voortgebracht
engendrer	voortbrengen
ensemble	verzameling
opérer sur	werken op
par récurrence sur	met inductie naar
ppcm (plus petit commun multiple)	kgv
pgcd (plus grand commun diviseur)	ggd
premier	priem
scinder	splitsen
sous-groupe distingué	normaaldeler
suite	rijtje

Duits

Auswertung	evaluatie
Bedingung	voorwaarde
Darstellung	representatie
Einschränkung	beperking
enthalten	bevatten
erzeugen	voortbrengen
Faser	vezel
gerade, ungerade	even, oneven
Gitter	rooster
Klammer	haakje
Körper	lichaam
Menge	verzameling
Operation	werking
Satz	stelling
Schranke	grens
Spalte (einer Matrix)	kolom (van een matrix)
stetig	continu
Urbild	origineel
Verfahren	methode
Voraussetzung	aanname
Zerlegung	ontbinding

Het griekse alfabet

In de wiskunde is grote behoefte aan symbolen om de diverse variabelen van een passende aanduiding te voorzien. Naast enkele losse letters uit niet-Europese alfabetten, zoals de Hebreeuwse aleph $\aleph$, wordt het gehele Griekse alfabet standaard gebruikt.

A	α	alfa	N	ν	nu
B	β	bèta	Ξ	ξ	xi
Γ	γ	gamma	O	o	omicron
Δ	δ	delta	Π	π, ϖ	pi
E	ϵ, ε	epsilon	P	ρ, ϱ	rho
Z	ζ	zèta	Σ	σ, ς	sigma
H	η	èta	T	τ	tau
Θ	θ, ϑ	thèta	Υ	υ	upsilon
I	ι	iota	Φ	ϕ, φ	phi
K	κ	kappa	X	χ	chi
Λ	λ	lambda	Ψ	ψ	psi
M	μ	mu	Ω	ω	omega

Faculteit WINS
Plantage Muidergracht 24
1018 TV Amsterdam

Tentamen Algebra A, woensdag 19 maart 1997, 9.30–12.30 uur

1. Definieer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 11 & 9 & 8 & 1 & 2 & 5 & 10 & 7 & 4 & 6 \end{pmatrix} \in S_{11}$.
   a. Bepaal het teken van σ.
   b. Bereken de orde van $\tau^5\sigma^{1000}\tau^{-5} \in S_{11}$ voor $\tau = (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7)$.

2. a. Bepaal een geheel getal x waarvoor $139x + 1$ deelbaar is door 1111.
   b. Bepaal het kleinste positieve gehele getal y waarvoor $y - 139^{1997}$ deelbaar is door 1111.

3. a. Laat zien dat de verzameling $G = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbf{R}^*, b \in \mathbf{R}\}$ van matrices een ondergroep is van $GL_2(\mathbf{R})$.
   b. Bewijs dat $N = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in \mathbf{R}\}$ een normaaldeler van G is, en dat er een isomorfisme $G/N \cong \mathbf{R}^*$ is.

4. a. Bepaal het aantal elementen in $\mathrm{Hom}(D_3, \mathbf{C}^*)$ en in $\mathrm{Hom}(D_3, A_4)$.
   b. Bepaal of de verzamelingen $\mathrm{Hom}(C_3, O_2(\mathbf{R}))$ en $\mathrm{Hom}(D_3, O_2(\mathbf{R}))$ eindig zijn.
   Motiveer in alle gevallen je antwoord.

5. Zij n een *oneven* getal, D_n de diëdergroep van orde $2n$, en C_n de ondergroep van D_n voortgebracht door een element van orde n. Voor $x \in D_n$ geven we met $f(x)$ het aantal elementen in de conjugatieklasse van x in D_n aan.
   a. Bewijs: voor $x \in C_n$ verschillend van e geldt $f(x) = 2$.
   b. Bewijs: voor $x \notin C_n$ geldt $f(x) = n$.
   c. Zij $N \triangleleft D_n$ een normaaldeler die *niet* bevat is in C_n. Bewijs: $N = D_n$.

De uitslag van het tentamen is later op de dag op de webpagina van het college te vinden.

Antwoorden bij het tentamen van 19 maart 1997.

Opgave 1.

a. $\sigma = (1\ 3\ 9\ 7\ 5)(2\ 11\ 6)(4\ 8\ 10)$, dus $\varepsilon(\sigma) = 1 \cdot 1 \cdot 1 = 1$.

b. de orde van $\tau^5\sigma^{1000}\tau^{-5} \in S_{11}$ is gelijk aan de orde σ^{1000} (geconjugeerd!), en $\sigma^{1000} = (2\ 11\ 6)(4\ 8\ 10)$ heeft orde 3.

Opgave 2.

a. $x = -139^{-1} \in (\mathbf{Z}/1111\mathbf{Z})^*$, standaardmethode geeft $x = 1103$. Inderdaad: $8 \cdot 139 = 1112$, dus $139^{-1} = 8 = -1103 \in (\mathbf{Z}/1111\mathbf{Z})^*$.

b. $(\mathbf{Z}/1111\mathbf{Z})^* \cong (\mathbf{Z}/11\mathbf{Z})^* \times (\mathbf{Z}/101\mathbf{Z})^*$ is een product van groepen van orde 10 en 100, dus er geldt $a^{100} = 1$ in deze groep. Dan $139^{1997} = 139^{-3} = 8^3 = 512 \bmod 1111$, dus $y = 512$.

Opgave 3.

a. gewoon uitschrijven – triviaal.

b. de determinantafbeelding $G \to \mathbf{R}^*$ is surjectief met kern N, dus N is normaal en de isomorfiestelling geeft $G/N \cong \mathbf{R}^*$.

Opgave 4.

a. $\#\operatorname{Hom}(D_3, \mathbf{C}^*) = \#\operatorname{Hom}(D_3/[D_3, D_3], \mathbf{C}^*) = \#\operatorname{Hom}(C_2, \mathbf{C}^*) = 2$.
Omdat A_4 geen ondergroep van orde 6 heeft (die zou normaal zijn, en dat geeft snel een tegenspraak) heeft ieder homomorfisme $D_3 \to A_4$ een abels beeld; we krijgen nu $\#\operatorname{Hom}(D_3, A_4) = \#\operatorname{Hom}(C_2, A_4) = 4$, immers A_4 bevat 4 elementen x met $x^2 = e$.

b. De groep $O_2(\mathbf{R})$ bevat 3 elementen x met $x^3 = e$, namelijk de identiteit en de rotaties over $\pm 2\pi/3$. Dus $\#\operatorname{Hom}(C_3, O_2(\mathbf{R})) = 3$. Iedere ondergroep van $O_2(\mathbf{R})$ voortgebracht door de rotatie over $2\pi/3$ en een willekeurige spiegeling is isomorf met D_3. Er zijn ook oneindig veel homomorfismen $D_3 \to O_2(\mathbf{R})$ met kern C_3 en beeld voortgebracht door een spiegeling.

Opgave 5.

a. Voor $x \in C_n$ en $\sigma \in D_n \setminus C_n$ geldt $\sigma x \sigma^{-1} = x^{-1}$, en x commuteert met de elementen van C_n. Omdat n oneven is geldt $x \neq x^{-1}$ voor $x \neq e$: er is geen $x \in C_n$ van orde 2. Dus $f(x) = 2$. (Alternatief: de normalisator van x bevat C_n maar is niet de hele groep, dus index $= 2 = f(x)$.)

b. Voor $\rho \in C_n$ en $\sigma \in D_n \setminus C_n$ hebben we $\rho\sigma\rho^{-1} = \rho^2\sigma$. Als ρ over C_n loopt, dan doet ρ^2 dat ook (n oneven!), dus alle n elementen in $D_n \setminus C_n$ zijn geconjugeerd. Ze zijn niet met elementen in C_n geconjugeerd, dus $f(x) = n$. (Alternatief: de normalisator van x bevat $\langle x \rangle$ maar geen elementen van $C_n \setminus \{e\}$, dus is gelijk aan $\langle x \rangle$ en heeft index $n = f(x)$.)

c. Als N een element van $D_n \setminus C_n$ bevat, dan ook al zijn n geconjugeerden. Met $e \in N$ hebben we dan al $n + 1$ elementen in N. Dat is meer dan de helft van de groepsorde $2n$, dus $N = D_n$.

Faculteit WINS
Plantage Muidergracht 24
1018 TV Amsterdam

Tentamen Algebra A, maandag 16 maart 1998, 9.30–12.30 uur

N.B. Motiveer in geval van open vragen ('bestaat er ...') steeds je antwoord!

1. Definieer de permutaties $\alpha, \beta \in S_{11}$ door

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 6 & 9 & 7 & 8 & 3 & 11 & 1 & 2 & 10 & 4 \end{pmatrix}$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 5 & 6 & 2 & 8 & 9 & 11 & 4 & 10 & 3 & 1 \end{pmatrix}$$

   a. Bereken de orde van α, β en $\alpha\beta$.
   b. Bestaat er een element $\sigma \in S_{11}$ met $\sigma\alpha = \beta\sigma$?

2. Zij S_n de permutatiegroep op $n > 1$ elementen, $\mathbf{R}$ de optelgroep van reële getallen en $\mathbf{R}^*$ de vermenigvuldiggroep van reële getallen verschillend van 0.
   a. Bestaat er een niet-triviaal homomorfisme $f : S_n \to \mathbf{R}$?
   b. Zij $g : S_n \to \mathbf{R}^*$ een niet-triviaal homomorfisme. Bewijs: $g(\sigma) = 1$ voor iedere 3-cykel $\sigma \in S_n$, en g is gelijk aan de tekenafbeelding $\varepsilon : S_n \to \{\pm 1\} \subset \mathbf{R}^*$.

3. Op een cursus bezigheidstherapie maakt men *Zen-vierkanten* door 4 gekleurde staafjes van gelijke lengte aan elkaar te solderen tot een vierkant. Hoeveel (echt) verschillende Zen-vierkanten kan men maken als de staafjes in 10 verschillende kleuren beschikbaar zijn?

4. De groep G van reële bovendriehoeksmatrices van determinant 1 is de ondergroep

$$G = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{R}) : ad = 1\}$$

   van de groep $\mathrm{GL}_2(\mathbf{R})$ van inverteerbare reële 2×2-matrices.
   a. Laat zien dat $H_1 = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G : b = 0\}$ een ondergroep van G is die isomorf is met $\mathbf{R}^*$. Is H_1 normaal in G?
   b. Bewijs dat $H_2 = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G : a = d = 1\}$ een normale ondergroep van G is met quotiëntgroep $G/H_2 \cong \mathbf{R}^*$.

5. Zij $G = (\mathbf{Z}/1998\mathbf{Z})^*$ de groep van inverteerbare restklassen modulo 1998.
   a. Bereken de orde van G.
   b. Bewijs: voor alle $x \in G$ is de orde van x een deler van 36.
   c. Bestaat er een element $x \in G$ van orde 36?

De uitslag van het tentamen is later op de dag op de webpagina van het college te vinden.

Antwoorden bij het tentamen van 16 maart 1998.

Opgave 1.

a. $\alpha = (1\ 5\ 8)(2\ 6\ 3\ 9)(4\ 7\ 11)$ en $\beta = (1\ 7\ 11)(2\ 5\ 8\ 4)(3\ 6\ 9\ 10)$, en door vermenigvuldiging $\alpha\beta = (1\ 11\ 5)(2\ 8\ 7\ 4\ 6)(9\ 10)$ (eerst β, dan α!). Ordes zijn $12 = \mathrm{kgv}(3,4,3)$, $12 = \mathrm{kgv}(3,4,4)$, en $30 = \mathrm{kgv}(3,5,2)$.

b. Uit $\sigma\alpha = \beta\sigma$ volgt $\sigma\alpha\sigma^{-1} = \beta$. Maar α en β zijn niet geconjugeerd: ze hebben verschillende cykeltypes.

Opgave 2.

a. Omdat S_n eindig is, heeft ieder element in $\sigma \in S_n$ eindige orde. De orde van $f(\sigma)$ deelt de orde van σ en is dus ook eindig. Maar $0 \in \mathbf{R}$ is het enige element met eindige orde, dus $f(\sigma) = 0$ en f is triviaal.

b. Voor een 3-cykel $\sigma \in S_n$ geldt $g(\sigma)^3 = g(\sigma^3) = g(\mathrm{id}) = 1$, dus $g(\sigma) = 1$. Omdat $\ker(g)$ alle 3-cykels bevat geldt nu $A_n \subset \ker(g)$. Wegens $\ker(g) \neq S_n$ hebben we $\ker(g) = A_n$. Nu is $g[S_n] \cong S_n/A_n$ een ondergroep van orde 2 in $\mathbf{R}^*$, dus $g[S_n] = \{\pm 1\}$ en g is de tekenafbeelding.

Opgave 3.

De groep D_4 van symmetrieën van het vierkant werkt op de verzameling van de 10^4 mogelijke Zen-vierkanten, dus we gebruiken de banenformule. Het aantal verschillende kleuren dat we kunnen kiezen voor een vierkant invariant onder $\sigma \in D_4$ is respectievelijk 4 (identiteit), 1 (twee kwartslagen), 2 (halve slag), 2 (twee spiegelingen in de diagonalen) en 3 (de twee andere spiegelingen). Voor x kleuren geeft dit

$$\tfrac{1}{8}(x^4 + 2x + x^2 + 2x^2 + 2x^3) = \tfrac{1}{8}(x^4 + 2x^3 + 3x^2 + 2x)$$

echt verschillende vierkanten. Voor $x = 10$ krijgen we $12320/8 = 1540$.

Opgave 4.

a. De afbeelding $\mathbf{R}^* \to G$ gegeven door $a \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ is een injectief homomorfisme met beeld H_1, dus H_1 is een ondergroep van G en isomorf met $\mathbf{R}^*$. Hij is niet normaal: conjugatie van $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1/2 \end{smallmatrix}\right) \in H_1$ met $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G$ geeft bijvoorbeeld $\left(\begin{smallmatrix} 2 & -3/2 \\ 0 & 1/2 \end{smallmatrix}\right) \notin H_1$. [Onderliggende gedachte: als e_1 en e_2 eigenvectoren met verschillende eigenwaarden zijn, dan is $e_1 + e_2$ geen eigenvector.]

b. De afbeelding $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mapsto a$ (of d) is een surjectief homomorfisme $G \to \mathbf{R}^*$ met kern H_2, dus H_2 is een normale ondergroep van G en de isomorfiestelling geeft $G/H_2 \cong \mathbf{R}^*$.

Opgave 5.

a. De ontbinding $1998 = 2 \cdot 3^3 \cdot 37$ geeft $\#G = \phi(1998) = \phi(2)\phi(3^3)\phi(37) = 1 \cdot 18 \cdot 36 = 648$.

b. De Chinese reststelling geeft G als een product $G \cong (\mathbf{Z}/2\mathbf{Z})^* \times (\mathbf{Z}/27\mathbf{Z})^* \times (\mathbf{Z}/37\mathbf{Z})^*$ van drie groepen van orde 1, 18 en 36. In elk van deze groepen geldt $x^{36} = 1$ voor alle x, dus hetzelfde geldt in G.

c. Het is voldoende om te laten zien dat er een element $x \in (\mathbf{Z}/37\mathbf{Z})^*$ is van orde $36 = 2^2 \cdot 3^2$. Omdat iedere echte deler van 36 een deler is van $36/3 = 12$ of $36/2 = 18$ moeten we een x vinden met $x^{12} \neq 1$ en $x^{18} \neq 1$. De eerste keus $x = 2$ werkt direct. (Bewijs: een paar keer kwadrateren modulo 37 geeft $2^4 = 16$, $2^8 = -3$ en $2^{16} = 9$. Dit geeft $2^{12} = 16 \cdot -3 = -11$ en $2^{18} = 4 \cdot 9 = -1$.)

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 1, dinsdag 23 mei 2000, 14.00–17.00 uur

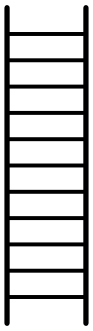
Motiveer steeds je antwoord, en noem de stellingen die je gebruikt.

1. Definieer de permutaties $\alpha, \beta \in S_{10}$ door

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 8 & 9 & 1 & 6 & 2 & 10 & 7 \end{pmatrix};$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 6 & 4 & 8 & 5 & 1 & 9 & 7 & 3 & 10 \end{pmatrix}.$$

a. Bereken de orde van $\alpha\beta$ en $\beta\alpha\beta^{-1}$.
b. Zijn α en α^{2000} geconjugeerd in S_{10}? Zelfde vraag voor β en β^{2000}.

2. Een *Leidsche ladder* wordt verkregen door 2 lange en 11 korte buizen zoals aangegeven aaneen te lassen. (De ladder is dus symmetrisch in alle gesuggereerde opzichten...) Lange buizen zijn verkrijgbaar in de kleuren rood, wit en blauw. Korte buizen zijn verkrijgbaar in zwart, zilver, goud en oranje. Hoeveel echt verschillende ladders kan men maken?



3. Definieer een groep G van reële 2×2-matrices als

$$G = \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) : a \in \mathbf{R}^*, b \in \mathbf{R}\} \subset \mathrm{GL}_2(\mathbf{R}).$$

a. Is de groep G abels?
b. Welke van de drie volgende afbeeldingen definiëren homomorfismen?

$$f\colon G \to \mathbf{R}^* \text{ gegeven door } \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mapsto a;$$
$$g\colon G \to \mathbf{R} \text{ gegeven door } \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mapsto b;$$
$$h\colon G \to \mathbf{R} \text{ gegeven door } \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mapsto b/a.$$

Bepaal voor de homomorfismen kern en beeld.
c. Geldt $G \cong \mathbf{R}^* \times \mathbf{R}$?

4. a. Zij $f\colon D_4 \to C_{24}$ een homomorfisme. Bewijs: voor alle $a \in D_4$ geldt $f(a)^2 = e$.
b. Bepaal het aantal elementen van $\mathrm{Hom}(D_4, C_{24})$.

5. Bereken de twee eindcijfers (in decimale notatie) van $(3^4)^5$ en van 3^{4^5}.

Uitslagen vanavond op collegekaartnummer op de webpagina van het college.

Tentamen Algebra 1, 21 Mei 2002

Geef steeds een volledige uitwerking, eventueel met verwijzingen naar stellingen uit de syllabus.

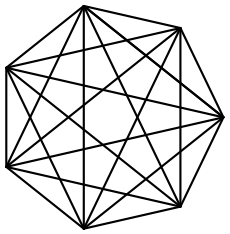
1. (a) Wat is de orde van het element $\sigma = (123)(234567)(78)$ in de S_8?
(b) Hoeveel dekpunten heeft σ^2 op de verzameling $\{1, 2, 3, 4, 5, 6, 7, 8\}$?
(c) Hoeveel elementen heeft de conjugatieklasse van σ in S_8?

2. Waarschuwing: $7^{7^7} = 7^{(7^7)} \neq \left(7^7\right)^7 = 7^{7^2}$.
(a) Wat is de orde van het element $(7 \bmod 30)$ van $(\mathbf{Z}/30\mathbf{Z})^*$?
(b) Bepaal de rest bij deling van $7^{7^{7^7}}$ door 30.
(c) Bewijs dat voor elke $n \in \mathbf{Z}_{\geq 1}$ de rij

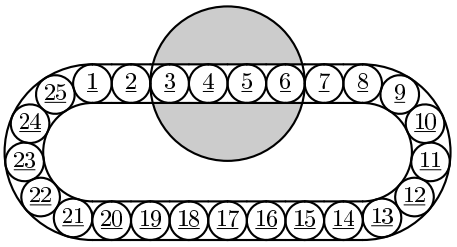
$$(7 \bmod n), (7^7 \bmod n), (7^{7^7} \bmod n), (7^{7^{7^7}} \bmod n), \ldots$$

in $\mathbf{Z}/n\mathbf{Z}$ bestaat uit een eindig beginstuk, en daarna een constante staart.

3. De symmetriegroep D_7 van de regelmatige 7-hoek werkt op de verzameling verbindingslijnstukken van verschillende hoekpunten.
(a) Hoeveel banen heeft deze werking?
(b) We kleuren nu elk van deze lijnstukken blauw of rood. Op hoeveel niet-equivalente manieren kan dat? (Twee kleuringen heten equivalent als een element van D_7 de ene in de ander overvoert.)



4. Hiernaast is een schuifpuzzeltje afgebeeld waarbij 25 schijfjes in een geultje achter elkaar liggen. Er zijn steeds twee zetten mogelijk: de 25 schijfjes cyclisch doorschuiven, of de grijze schijf 180 graden om zijn middelpunt draaien. In de stand op de afbeelding zou die laatste zet 3 en 6 verwisselen, en 4 en 5 verwisselen.



Bewijs de volgende uitspraken. Je mag steeds de voorgaande uitspraak gebruiken, ook als je die niet kon bewijzen!

(a) Er is geen zettenreeks waarvan het totaal effect is dat schijfje 1 en 2 van plek wisselen, en elk ander schijfje op zijn plaats blijft.
(b) De ondergroep $H_1 = \langle (14)(23), (25)(34) \rangle$ van S_5 is isomorf met D_5, en (12345) is bevat in H_1.
(c) De ondergroep $H_2 = \langle (12345), (23456) \rangle$ van S_6 bevat een drie-cykel.
(d) $H_2 = A_6$.
(e) Voor elke $\sigma \in A_{25}$ is er een zettenreeks die de 25 schijfjes permuteert als σ.
(f) Een zettenreeks als bedoeld bij (a) bestaat wèl als we 26 in plaats van 25 schijfjes in de lus hebben.

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 1, maandag 12 mei 2003, 10.00–13.00 uur

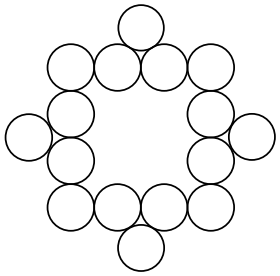
Motiveer steeds je antwoord, en noem de stellingen die je gebruikt.

1. Definieer de permutaties $\alpha, \beta \in S_8$ door

$$\alpha = (1\ 2\ 3\ 4\ 5)(1\ 5\ 4\ 3\ 7\ 2\ 8)(4\ 6)$$
$$\beta = (1\ 2\ 3)(5\ 6)(2\ 3\ 8)(4\ 7)$$

a. Bereken de orde van α en β.
b. Zijn $\alpha\beta$ en $(\alpha\beta)^{2003}$ geconjugeerd in S_8?
c. Bepaal de orde van de ondergroep $\langle \alpha, \beta \rangle \subset S_8$ voortgebracht door α en β.

2. Het CDA produceert in het kader van de formatie *moederdag-onderzetters* verkregen door 16 platte kurkjes zoals aangegeven aaneen te plakken. De onderzetter is symmetrisch in alle gesuggereerde opzichten, en heeft geen specifieke boven- en onderkant. De kurkjes zijn leverbaar in de kleuren zuurstokroze, babyblauw en mintgroen. Bereken het aantal echt verschillende onderzetters, en laat zien dat dat genoeg is om alle Nederlandse moeders een verschillend exemplaar te geven.



3. Definieer $G, H \subset \mathrm{GL}_2(\mathbf{R})$ door

$$G = \{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbf{R}^*, b \in \mathbf{R} \};$$
$$H = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbf{R} \}.$$

a. Laat zien dat G een ondergroep van $\mathrm{GL}_2(\mathbf{R})$ is, en H een ondergroep van G.
b. Laat zien dat H normaal is in G, en dat $G/H \cong \mathbf{R}^*$ geldt.
c. Geldt $G \cong H \times \mathbf{R}^*$?

4. Bepaal de laatste 3 cijfers (in decimale notatie) van 2003^{2003} en van $2003^{2003^{2003}}$.

5. Zij $G = \mathrm{GL}_2(\mathbf{F}_3)$ de groep van inverteerbare 2×2-matrices met coëfficiënten in het lichaam $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z}$.

a. Wat is de orde van G?

Laat G op de natuurlijke manier werken op de 2-dimensionale vectorruimte $V = \mathbf{F}_3^2$ over $\mathbf{F}_3$, en op de verzameling X van lijnen door de oorsprong in V.

b. Bepaal $\#X$, en kern en beeld van de afbeelding $G \to S(X)$ gegeven door deze werking.
c. Geldt $\mathrm{SL}_2(\mathbf{F}_3)/\{\pm I\} \cong A_4$?

Uitslagen donderdagmiddag op collegekaartnummer op de webpagina van het college.

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 1, maandag 7 juni 2004, 10.00–13.00 uur

Motiveer steeds je antwoord, en noem de stellingen die je gebruikt.

Opgave 1. (a) Schrijf twee elementen σ, $\tau \in S_{28}$ op met

$$\text{orde}(\sigma) = 35, \qquad \tau\sigma\tau^{-1} = \sigma^2.$$

(b) Toon aan: voor *iedere* $\sigma \in S_{28}$ met $\text{orde}(\sigma) = 35$ is er een $i \in \{1, 2, \ldots, 28\}$ met $\sigma(i) = i$.

Opgave 2. Zij G een groep met de eigenschap dat voor alle elementen a, b, $c \in G$ de elementen abc en cba geconjugeerd zijn. Bewijs dat G abels is.

Opgave 3. Een *negenwiel* is een wagenwiel met negen spaken die allemaal paars of geel geschilderd zijn. Hoeveel echt verschillende negenwielen zijn er?

Opgave 4. Zij V_4 de viergroep van Klein.
(a) Hoeveel ondergroepen heeft V_4? En hoeveel hiervan zijn normaal?
(b) Hoeveel niet-injectieve groepshomomorfismen $V_4 \to S_4$ zijn er?

Opgave 5. Stel dat n een positief geheel getal is met

$$2^7 \equiv 2 \bmod n, \qquad 3^7 \equiv 3 \bmod n.$$

Bewijs: voor alle $a \in \mathbf{Z}$ geldt $a^7 \equiv a \bmod n$.

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 1, woensdag 9 juni 2004, 10.00–13.00 uur

Motiveer steeds je antwoord, en noem de stellingen die je gebruikt.

Notatie. Voor een niet-negatief geheel getal n geven we met S_n de verzameling permutaties van $\{1, 2, \ldots, n\}$ aan.

Opgave 1. (a) Schrijf een permutatie $\sigma \in S_9$ op met de eigenschap dat voor alle $x \in \{1, 2, \ldots, 9\}$ geldt:

$$\sigma(x) \equiv 5x + 2 \bmod 9.$$

(b) Bereken de orde van σ en van σ^{999}.

Opgave 2. Stel G is een groep met de eigenschap dat elk element van G geconjugeerd is met zijn inverse. Bewijs: voor alle $a, b \in G$ zijn de elementen ab en $a^{-1}b^{-1}$ geconjugeerd.

Opgave 3. Een *Ajaxtaart* is een ronde marsepeinen taart met zeven kaarsjes, één in het midden en de andere zes regelmatig verdeeld langs de rand; elk kaarsje is rood of wit, maar niet alle kaarsjes hebben dezelfde kleur. Hoeveel echt verschillende Ajaxtaarten zijn er?

Opgave 4. Zij D_5 de diëdergroep van orde 10.

(a) Hoeveel ondergroepen heeft D_5? En hoeveel hiervan zijn normaal?

(b) Hoeveel groepshomomorfismen $D_5 \to S_3$ zijn er?

Opgave 5. (a) Bewijs: $a^6 \equiv a^2 \bmod 60$ voor alle $a \in \mathbf{Z}$.

(b) Stel dat n een positief geheel getal is met de eigenschap dat voor alle $a \in \mathbf{Z}$ geldt: $a^6 \equiv a^2 \bmod n$. Bewijs: n is een deler van 60.

Tentamen Algebra 1, Leiden, 6 juni 2005, 10:00-13:00

Geef steeds een volledige uitwerking, eventueel met verwijzingen naar stellingen uit de syllabus. De uitslag staat hedenavond op de webpagina.

Opgave 1. Laat $\sigma = (123)(345)(567) \in S_7$.

(a) Bepaal de orde van σ.

(b) Bewijs dat de conjugatieklasse van σ in S_7 precies $6! = 720$ elementen heeft.

(c) Bepaal $\left(\sigma^{2005}\right)^{2005}$ en $\sigma^{\left(2005^{2005}\right)}$.

Opgave 2. Bepaal een geheel getal x met $x \equiv 2 \bmod 9$ en $x \equiv 1 \bmod 7$. Is er ook een geheel getal y met $y \equiv 2 \bmod 9$ en $y \equiv 1 \bmod 21$?

Opgave 3. Laat G een groep zijn, en $x, y \in G$.

(a) Stel dat x en y commuteren. Bewijs dat $(xy)^n = x^n y^n$ geldt voor alle gehele $n \geq 1$.

(b) Neem omgekeerd aan dat $(xy)^n = x^n y^n$ voor alle gehele $n \geq 1$. Volgt daaruit dat x en y commuteren?

(c) Stel dat k een positief geheel getal is met $x^k = 1$. Stel ook dat x commuteert met de commutator $[x, y]$. Bewijs dat $[x, y]^k = 1$.

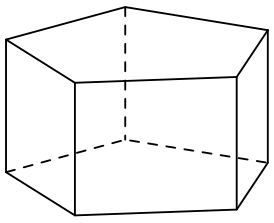
Opgave 4. Laat D_5 de diëdergroep van orde 10 zijn, en laat C_{10} de cyclische groep van orde 10 zijn.

(a) Zijn C_{10} en D_5 isomorf? (Bewijs je antwoord!)

(b) Bepaal $\#\mathrm{Hom}(C_{10}, D_5)$.

(c) Bepaal $\#\mathrm{Hom}(D_5, C_{10})$.

Opgave 5. Een Vijfhuizer prisma is een veelvlak met een regelmatige vijfhoek als onder- en bovenvlak, en vijf vierkanten als zijvlakken.



(a) Bewijs dat de rotatiegroep van een Vijfhuizer prisma isomorf is met de D_5.

(b) We kleuren de 7 vlakken van een Vijfhuizer prisma met twee kleuren. We noemen twee kleuringen hetzelfde als de één door een draaiing in de ander overgaat. Hoeveel verschillende kleuringen zijn er mogelijk?

— SUCCES —

Tentamen Algebra 1, 15 juni 2006, 14:00 – 17:00

Motiveer steeds je antwoord, en noem de stellingen die je gebruikt. Je mag de syllabus, boeken en aantekeningen gebruiken, maar gebruik van een rekenmachine is niet toegestaan.

Opgave 1. Definieer $\sigma, \tau \in S_9$ door

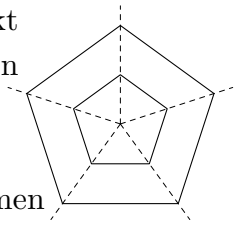
$$\sigma = (1\ 3)(2\ 4\ 6)(3\ 5)(2\ 6\ 4)(2\ 4\ 6\ 8)(8\ 9),$$
$$\tau = (1\ 5\ 7)(2\ 3\ 4).$$

(a) Bepaal de orde van σ in S_9.
(b) Bepaal de orde van $\tau\sigma\tau^{-1}$.
(c) Bereken $\sigma^{2006^{1506}}$.

Opgave 2. Zij C_6 de cyclische groep van orde zes en S_3 de permutatiegroep op drie elementen. Bepaal $\#\mathrm{Hom}(C_6, S_3)$.

Opgave 3.
(a) Bestaat er een $a \in \mathbf{Z}$ zodat $15a \equiv 1 \bmod 651$? Zo ja, bepaal zo'n a.
(b) Bestaat er een $b \in \mathbf{Z}$ zodat $16b \equiv 1 \bmod 651$? Zo ja, bepaal zo'n b.

Opgave 4. De symmetriegroep D_5 van de regelmatige 5-hoek werkt op natuurlijke wijze op de verzameling van tien vetgedrukte lijnstukken van het hiernaast afgebeelde spinnenweb.



(a) Hoeveel banen heeft deze werking?
(b) We kleuren elk van deze tien lijnstukken goud of zilver. We noemen twee kleuringen equivalent als een element van D_5 de ene in de andere overvoert. Hoeveel niet-equivalente kleuringen zijn er?

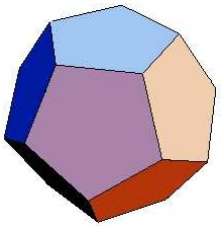
Opgave 5. Zij X de verzameling van lijnen in $\mathbf{R}^2$ die door de oorsprong gaan, en zij $\mathrm{GL}_2(\mathbf{R})$ de groep van inverteerbare 2×2-matrices met coëfficiënten uit $\mathbf{R}$. Definieer een werking $\circ$ van $\mathrm{GL}_2(\mathbf{R})$ op X door $A \circ l = \{Av : v \in l\} \in X$ voor $A \in \mathrm{GL}_2(\mathbf{R})$ en $l \in X$.
(a) Bepaal de stabilisator van de x-as.
(b) Laat zien dat alle stabilisatoren van elementen uit X geconjugeerd zijn.

De uitslagen zijn vanavond op collegekaartnummer op de webpagina van het college te vinden.

Tentamen Algebra 1, 12 Juni 2008, 14:00-17:00

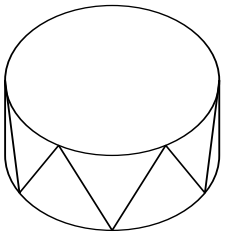
Opgave 1. Bepaal de rest bij deling van $11^{(345^{678})}$ door 13.

Opgave 2. Laat G de rotatiegroep van de dodecaeder (regelmatig 12-vlak) zijn. Deze groep werkt transitief op de verzameling X van 12 zijvlakken.



(a) Hoeveel elementen heeft de stabilisator van zo'n zijvlak?
(b) Leid uit (a) af hoeveel elementen G heeft.
(c) Laat H de stabilisator van een hoekpunt zijn. Hoeveel banen heeft H op X?

Opgave 3. Een *triangeltrommel* is een cilindrische trommel met 12 identieke driehoekjes op de rand, zoals in het plaatje. De boven- en onderkant zijn identiek en kunnen allebei gebruikt worden om op te trommelen. We noemen twee triangeltrommels hetzelfde als de één verkregen kan worden door de ander te draaien in de ruimte. We gaan de driehoekjes kleuren en we hebben 10 kleuren tot onze beschikking.



(a) Laat zien dat de symmetriegroep van ruimtelijke rotaties van een triangeltrommel vóór het kleuren 12 elementen heeft.
(b) Hoeveel echt verschillende triangeltrommels zijn er mogelijk?

Opgave 4. Hoeveel homomorfismen zijn er van de permutatiegroep S_4 naar de cyclische groep C_4? En van C_4 naar S_4?

Opgave 5. Definieer de groep G door $G = (\mathbf{Z}/18\mathbf{Z}) \times (\mathbf{Z}/60\mathbf{Z})$, en definieer het homomorfisme $f\colon G \to G$ door $f(x) = 4x = x + x + x + x$.

(a) Wat is de orde van het element $(4, 5) \in G$?
(b) Bepaal het aantal elementen van de kern van f en van het beeld van f.
(c) Voor $n \geq 1$ definiëren we de n-voudige samenstelling $f^n\colon G \to G$ door $f^1 = f$ en $f^n = f^{n-1} \circ f$ voor $n \geq 2$. Bepaal de kleinste $n \geq 2$ waarvoor $f^n = f$.

— SUCCES —