Syllabus Algebra I

Prof. Dr. H.W. Lenstra, Jr.

Prof. Dr. F. Oort

Bewerkt en aangevuld door Prof. Dr. B.J.J. Moonen
Met een appendix door Raf Bocklandt

Studiejaar en semester: jaar 1, semester 2
Docent: Lenny Taelman
Studielast: 6 EC
Studiegidsnummer: 51221ALG6Y

Inhoudsopgave

Voorwoord

Deze syllabus is een nieuwe editie van de syllabus *Algebra, Deel A: Groepen* geschreven door de hoogleraren H.W. Lenstra en F. Oort, waarvan eerste versies stammen uit het begin van de jaren 1980. De afgelopen decennia is aan veel Nederlandse universiteiten Algebra onderwezen uit de syllabi van Lenstra en Oort, of uit syllabi die daar sterk door zijn beïnvloed. Vele wiskundigen hebben ergens in hun boekenkast nog wel oorspronkelijke exemplaren liggen, vaak met versleten ruggen en een lijmbinding die na zovele jaren is uitgedroogd, waardoor de pagina's gemakkelijk loslaten.

De syllabi van Lenstra en Oort stammen uit een tijd dat TEX nog niet algemeen in gebruik was en LATEX zelfs nog niet bestond; de wiskundige schreef zijn teksten toen nog met een typemachine. De huidige versie is geproduceerd met behulp van LATEX, en op diverse plaatsen zijn kleine veranderingen aangebracht in de tekst. Op hoofdlijnen is de oorspronkelijke tekst echter ongewijzigd gelaten.

Naast de basistext is er ook een appendix toegevoegd waarin een voorproefje gegeven wordt van de verbanden tussen groepentheorie en verschillende aspecten van de meetkunde. De bedoeling van de appendix is om aan te tonen dat groepentheorie alom tegenwoordig is in de hedendaagse wiskunde en om kennis te maken met een aantal groepen en concepten die vaak terugkomen in verschillende vakgebieden. Sommige van deze groepen zullen we ook gebruiken in de colleges om de theorie uit de syllabus te illustreren.

Onze dank gaat uit naar H.W. Lenstra en F. Oort voor hun permissie om hun syllabus opnieuw in gebruik te nemen, en naar Floor Broekgaarden, Okke van Garderen en Pieter van Niel voor het typewerk dat de basis heeft gevormd voor de huidige editie.

Bij het overtypen van de tekst kunnen er natuurlijk fouten zijn gemaakt. Correcties of suggesties voor verbetering van de tekst zijn altijd welkom op `raf.bocklandt@gmail.com`.

Prof. Dr. B.J.J. Moonen
Nijmegen, oktober 2014

Raf Bocklandt
Amsterdam, januari 2015

Hoofdstuk 0

Gehele getallen

In dit hoofdstuk behandelen we de deelbaarheidseigenschappen van de gehele getallen. We veronderstellen bekendheid met de verzameling $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ der gehele getallen, met de elementaire eigenschappen van optelling en vermenigvuldiging van gehele getallen, met het principe van *volledige inductie* en met een aantal andere algemene begrippen en notaties; zie hiervoor de syllabus Basiswiskunde van G. Oomens.

Stelling 0.1 (Deling met rest)**.** *Laat $a, b \in \mathbb{Z}$ met $b > 0$. Dan bestaan er gehele getallen q en r (het* quotiënt *en de* rest *van a bij deling door b) zodanig dat*

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

Bovendien zijn q en r eenduidig bepaald door a en b.

Voorbeeld 0.2. Voor $a = 23$ en $b = 7$ geldt

$$23 = 3 \cdot 7 + 2$$

dus $q = 3$ en $r = 2$. Voor $a = -23$ en $b = 7$ geldt

$$-23 = -4 \cdot 7 + 5$$

dus $q = -4$ en $r = 5$.

Bewijs van 0.1. Eerst bewijzen we het *bestaan* van q en r. Om te beginnen beschouwen we het geval dat $a \geq 0$. In dit geval gaan we het bestaan van q en r met volledige inductie naar a bewijzen.

Begin van de inductie: $a = 0$. Hiervoor kunnen we $q = 0$ en $r = 0$ nemen.

Inductiestap: $a > 0$. De inductiehypothese zegt, dat we het voor $a - 1$ kunnen:

$$a - 1 = q' \cdot b + r', \qquad q', r' \in \mathbb{Z}, \qquad 0 \leq r' < b.$$

We onderscheiden nu twee gevallen: $r' = b - 1$ of $r' < b - 1$. Als $r' = b - 1$ dan geldt $a - 1 = q' \cdot b + b - 1$ dus

$$a = (q' + 1) \cdot b.$$

Neem nu $q = q' + 1$ en $r = 0$, dan hebben q en r de verlangde eigenschappen.

Als $r' < b - 1$ nemen we $q = q'$, $r = r' + 1$. Dan geldt

$$a = qb + r, \qquad 0 < r < b,$$

dus opnieuw hebben q en r de verlangde eigenschappen. Hiermee is de inductiestap voltooid.

Stel vervolgens dat $a < 0$. Dan geldt $-a > 0$, dus wegens het zojuist bewezene geldt $-a = q'b + r'$ voor zekere $q', r' \in \mathbb{Z}$ met $0 \leq r' < b$. Als $r' = 0$ dan geldt $a = (-q') \cdot b$, dus we kunnen $q = -q'$ en $r = 0$ nemen. Als $r' > 0$ dan geldt

$$a = (-q' - 1) \cdot b + (b - r'), \qquad 0 < b - r' < b,$$

dus we kunnen $q = -q' - 1$ en $r = b - r'$ nemen. Hiermee hebben we in alle gevallen het bestaan van q en r aangetoond. Vervolgens gaan we de eenduidigheid bewijzen. Stel dat

$$a = q_1 b + r_1, \qquad q_1, r_1 \in \mathbb{Z}, \qquad 0 \leq r_1 < b,$$

$$a = q_2 b + r_2, \qquad q_2, r_2 \in \mathbb{Z}, \qquad 0 \leq r_2 < b.$$

We willen bewijzen dat $q_1 = q_2$ en $r_1 = r_2$.

Als $q_1 = q_2$ dan ook $r_1 = a - q_1 b = a - q_2 b = r_2$, en we zijn klaar. Als $q_1 \neq q_2$, dan is één van beide, zeg q_1, de grootste (verwissel anders de indices 1 en 2). Uit $q_1 b + r_1 = a = q_2 b + r_2$ volgt dan

$$(q_1 - q_2)b = r_2 - r_1.$$

Uit $q_1 > q_2$ volgt $q_1 - q_2 \geq 1$ dus

$$(q_1 - q_2)b \geq b.$$

Uit $r_2 < b$, $r_1 \geq 0$ volgt evenwel

$$(q_1 - q_2)b = r_2 - r_1 < b.$$

Dit is een tegenspraak.

Hiermee is 0.1 volledig bewezen. □

Definitie 0.3. Laat $a, b \in \mathbb{Z}$. Als er een $q \in \mathbb{Z}$ bestaat zodanig dat $a = qb$, zeggen we dat a *deelbaar* is door b, of dat a een *veelvoud* van b is, of dat b een *deler* van a is, of dat b het getal a *deelt*; notatie: $b \mid a$. Als b géén deler is van a schrijven we $b \nmid a$.

Voorbeelden 0.4. Er geldt

$$5 \mid 15\,, \qquad -3 \nmid 8\,, \qquad 0 \mid 0\,, \qquad 1 \mid -1\,, \qquad 0 \nmid 5\,.$$

De volgende eigenschappen, die we beneden herhaaldelijk zullen gebruiken, zijn directe gevolgen van de definitie:

$$\begin{aligned}
&c \mid b \quad \text{en} \quad b \mid a \quad \Longrightarrow\ c \mid a,\\
&b \mid a \quad \text{en} \quad b \mid a' \quad \Longrightarrow\ b \mid a+a' \quad \text{en} \quad b \mid a-a',\\
&b \mid 0 \quad \text{voor alle } b,\\
&1 \mid a \quad \text{voor alle } a,\\
&0 \mid a \iff a = 0,\\
&b \mid a \iff |b| \text{ deelt } |a|,\\
&b \mid a \quad \text{en} \quad a \neq 0 \implies |b| \leq |a|.
\end{aligned}$$

Hier geven a, a', b en c gehele getallen aan. Uit de laatste eigenschap volgt dat een gegeven geheel getal $a \neq 0$ maar eindig veel delers heeft. Dit betekent dat de volgende definitie zinvol is:

Definitie 0.5. Laat $a, b \in \mathbb{Z}$. Als a en b niet beide nul zijn, is de *grootste gemene deler* van a en b het grootste gehele getal dat zowel een deler van a als van b is; notatie: $\gcd(a,b)$ of (a,b). Bovendien zetten we $\gcd(0,0) = 0$. We noemen a en b *onderling ondeelbaar* of *relatief priem* als $\gcd(a,b) = 1$.

Merk op dat geldt

$$\begin{aligned}
\gcd(0,a) = \gcd(a,0) = |a|, &\qquad \text{voor } a \in \mathbb{Z},\\
\gcd(a,b) = \gcd\big(|a|,|b|\big), &\qquad \text{voor } a,b \in \mathbb{Z}.
\end{aligned}$$

0.6 Het Euclidische algoritme voor de bepaling van $\gcd(a,b)$ werkt als volgt.

Euclides, Alexandrijns wiskundige, ≈ 300 v.Chr.

Laat $a, b \in \mathbb{Z}$. Definieer de niet-negatieve gehele getallen $r_0, r_1, r_2, \ldots$ op de volgende manier:

$$\begin{aligned}
r_0 &= |a|,\\
r_1 &= |b|,\\
r_{n+1} &= \text{ (rest van } r_{n-1} \text{ bij deling door } r_n) \text{ als } r_n \neq 0;
\end{aligned}$$

dus r_{n+1} wordt gevonden uit een deling met rest:

$$r_{n-1} = q_n \cdot r_n + r_{n+1}, \qquad q_n, r_{n+1} \in \mathbb{Z}, \qquad 0 \leq r_{n+1} < r_n.$$

In het geval $r_n = 0$ stopt het algoritme, en we hebben dan $\text{ggd}(a, b) = r_{n-1}$ (dit bewijzen we straks). Merk op dat er beslist een n moet zijn met $r_n = 0$, anders zouden we een oneindige dalende rij $r_1 > r_2 > r_3 > \cdots$ van positieve gehele getallen krijgen, hetgeen onmogelijk is.

Voorbeelden 0.7. Laat $a = r_0 = 1057$ en $b = r_1 = 315$. We vinden achtereenvolgens

$$\begin{aligned} 1057 &= 3 \cdot 315 + 112 && (q_1 = 3, r_2 = 112) \\ 315 &= 2 \cdot 112 + 91 && (q_2 = 2, r_3 = 91) \\ 112 &= 1 \cdot 91 + 21 && (q_3 = 1, r_4 = 21) \\ 91 &= 4 \cdot 21 + 7 && (q_4 = 4, r_5 = 7) \\ 21 &= 3 \cdot 7 + 0 && (q_5 = 3, r_6 = 0). \end{aligned}$$

Er geldt $r_6 = 0$, dus $\text{ggd}(1057, 315) = r_5 = 7$.

Het volgende lemma gebruiken we om te bewijzen dat het algoritme het juiste resultaat oplevert.

Lemma 0.8. *Laat $a, b \in \mathbb{Z}$ met $b \neq 0$, en $a = qb + r$ met $q, r \in \mathbb{Z}$. Dan geldt:*

$$\text{ggd}(a, b) = \text{ggd}(b, r).$$

Bewijs. Laat d een deler van b zijn. Als d ook een deler van a is, dan volgt uit $d \mid a$ en $d \mid qb$ dat

$$d \mid a - qb = r$$

dus d is een deler van r. Omgekeerd, als d ook een deler van r is, dan

$$d \mid qb + r = a,$$

dus d is een deler van a. We zien dus dat de getallen die zowel a als b delen dezelfde zijn als de getallen die zowel r als b delen. Hieruit volgt $\text{ggd}(a, b) = \text{ggd}(r, b)$. Dit bewijst 0.8. □

We bewijzen nu dat het Euclidische algoritme inderdaad de grootste gemene deler berekent. Laat $a, b \in \mathbb{Z}$, laten $r_0, r_1, r_2, \ldots$ gedefinieerd zijn als in 0.6, en zij m het getal waarvoor $r_m = 0$. We moeten bewijzen dat $r_{m-1} = \text{ggd}(a, b)$. Er geldt

$$\text{ggd}(a, b) = \text{ggd}\big(|a|, |b|\big) = \text{ggd}(r_0, r_1).$$

Door herhaald Lemma 0.8 toe te passen (op r_{i-1} en r_i in plaats van a en b) vinden we

$$\text{ggd}(r_0, r_1) = \text{ggd}(r_1, r_2) = \ldots = \text{ggd}(r_{m-1}, r_m).$$

Tenslotte geldt $r_m = 0$, dus

$$\text{ggd}(r_{m-1}, r_m) = \text{ggd}(r_{m-1}, 0) = r_{m-1}.$$

Hiermee hebben we bewezen dat $\text{ggd}(a, b) = r_{m-1}$, zoals verlangd.

Stelling 0.9. *Laat $a, b \in \mathbb{Z}$, en $d = \text{ggd}(a, b)$. Dan bestaan er $x, y \in \mathbb{Z}$ met $xa + yb = d$.*

Bewijs. We gebruiken de notaties uit 0.6. We bepalen twee rijen gehele getallen $x_0, x_1, x_2, \ldots$ en $y_0, y_1, y_2, \ldots$ zodanig dat steeds geldt

$$x_n a + y_n b = r_n.$$

Voor $n = 0$ geldt $r_n = |a| = \pm a$, dus we kunnen $x_0 = \pm 1$ en $y_0 = 0$ nemen. Op dezelfde wijze kunnen we $x_1 = 0$ en $y_1 = \pm 1$ nemen. Als $n \geq 1$, en $r_n \neq 0$, dan bepalen we x_{n+1} en y_{n+1} door van de vergelijking

$$x_{n-1} a + y_{n-1} b = r_{n-1}$$

q_n keer de vergelijking

$$x_n a + y_n b = r_n$$

af te trekken. Wegens $r_{n-1} - q_n r_n = r_{n+1}$ geeft dit

$$(x_{n-1} - q_n x_n) \cdot a + (y_{n-1} - q_n y_n) \cdot b = r_{n+1},$$

dus we kunnen $x_{n+1} = x_{n-1} - q_n x_n$ en $y_{n+1} = y_{n-1} - q_n y_n$ kiezen. Zo voortgaande vinden we op een gegeven ogenblik $r_m = 0$, en dan geldt

$$x_{m-1} a + y_{m-1} b = r_{m-1} = d.$$

Hiermee is 0.9 bewezen. □

Voorbeelden 0.10. Met $a = 1057$ en $b = 315$ vinden we achtereenvolgens

$$\begin{aligned}
1 \cdot 1057 + 0 \cdot 315 &= 1057 && \\
0 \cdot 1057 + 1 \cdot 315 &= 315 && \text{(deze 3x van de vorige aftrekken)} \\
1 \cdot 1057 + (-3) \cdot 315 &= 112 && \text{(deze 2x van de vorige aftrekken)} \\
(-2) \cdot 1057 + 7 \cdot 315 &= 91 && \text{(deze 1x)} \\
3 \cdot 1057 + (-10) \cdot 315 &= 21 && \text{(deze 4x)} \\
(-14) \cdot 1057 + 47 \cdot 315 &= 7. &&
\end{aligned}$$

Dit levert de oplossing $(x, y) = (-14, 47)$ van $x \cdot 1057 + y \cdot 315 = \text{ggd}(1057, 315) = 7$. Het is niet de enige oplossing (zie Opgave 0.5(a)) maar wel de kleinste (zie Opgave 0.5(c)).

Gevolg 0.11. *Laat $a, b \in \mathbb{Z}$, en $d = \text{ggd}(a, b)$. Dan is elk getal dat zowel een deler van a als van b is ook een deler van d.*

Bewijs. Schrijf $d = xa + yb$, met $x, y \in \mathbb{Z}$. Als $c \mid a$ en $c \mid b$, dan volgt $c \mid xa + yb = d$. Dit bewijst 0.11. □

Gevolg 0.12. *Twee gehele getallen a en b zijn onderling ondeelbaar dan en slechts dan als er $x, y \in \mathbb{Z}$ bestaan met $xa + yb = 1$.*

Bewijs. De implicatie '$\Rightarrow$' is het speciale geval $d = 1$ van 0.9. Voor '$\Leftarrow$': Als $d = \text{ggd}(a, b)$, dan geldt $d \mid a$ en $d \mid b$, dus $d \mid xa + yb = 1$. Hieruit volgt $d = 1$. Dit bewijst 0.12. □

Gevolg 0.13. *Laten a, b, c gehele getallen zijn, met a en b onderling ondeelbaar. Dan geldt: $a \mid bc \implies a \mid c$.*

Bewijs. Kies $x, y \in \mathbb{Z}$ met $xa + yb = 1$. Uit $a \mid bc$ volgt $a \mid xac + ybc = (xa + yb)c = 1 \cdot c = c$, zoals verlangd. Dit bewijst 0.13. □

Definitie 0.14. Een *priemgetal* is een geheel getal p, dat groter dan 1 is en behalve 1 en p geen positieve delers heeft.

Voorbeelden 0.15. De getallen 2, 3, 5, 7, 101 en 170141183460469231731687303715884105727 zijn priemgetallen.

Voor meer informatie over priemgetallen, zie bijvoorbeeld D.B. Zagier, The first 50 million prime numbers, The Mathematical Intelligencer, vol. 0 (1977), 7–19. [1]

Stelling 0.16. *Laat p een priemgetal zijn, en $b, c \in \mathbb{Z}$. Dan geldt: $p \mid bc \implies p \mid b$ of $p \mid c$.*

Bewijs. Omdat $\text{ggd}(b, p)$ een positieve deler van p is, geldt $\text{ggd}(b, p) = 1$ of $\text{ggd}(b, p) = p$. Als $\text{ggd}(b, p) = 1$ dan kunnen we 0.13 toepassen (met $a = p$), en we zien: Als $p \mid bc$, dan $p \mid c$. Als $\text{ggd}(b, p) = p$, dan geldt $p \mid b$. Dus in beide gevallen geldt $p \mid b$ of $p \mid c$. Hiermee is 0.16 bewezen. □

Gevolg 0.17. *Laat p een priemgetal zijn, en $b_1, b_2, \ldots, b_u$ gehele getallen met $p \mid b_1 b_2 \cdots b_u$. Dan is er een $i \in \{1, 2, \ldots, u\}$ met $p \mid b_i$.*

Bewijs. Dit volgt uit 0.16 met volledige inductie naar u. De precieze uitvoering van het bewijs laten we aan de lezer over. Dit bewijst 0.17. □

Stelling 0.18 (Eenduidige priemfactorontbinding)**.** *Elk positief geheel getal a kan geschreven worden als product van een eindig aantal priemgetallen:*

$$a = p_1 p_2 \cdots p_t, \qquad \textit{waarbij } t \geq 0 \textit{ en waarbij de } p_i \textit{ priemgetallen zijn } (1 \leq i \leq t).$$

Bovendien is een dergelijke schrijfwijze eenduidig bepaald op de volgorde van de factoren na.

Bewijs. Eerst bewijzen we, met volledige inductie naar a, dat a als een product van priemgetallen te schrijven is.

Als $a = 1$ dan nemen we $t = 0$: het lege product is bij afspraak gelijk aan 1. Als a een priemgetal is dan nemen we $t = 1$ en $p_1 = a$. Tenslotte, stel dat a geen priemgetal is, en $a > 1$. Dan heeft a een deler b met $1 < b < a$, dus we kunnen schrijven $a = bc$, met $b, c < a$. Omdat b en c kleiner dan a zijn, kunnen we de inductiehypothese op b en c toepassen. Dan vinden we, dat b en c elk als product van priemgetallen geschreven kunnen worden. Dit geldt dan ook voor $a = bc$.

[1] `http://people.mpim-bonn.mpg.de/zagier/files/doi/10.1007/BF03039306/fulltext.pdf`

Hiermee hebben we aangetoond dat elk positief geheel getal a een priemfactorontbinding bezit. We bewijzen nu, dat deze priemfactorontbinding eenduidig bepaald is. Dit gebeurt ook met volledige inductie naar a. Het geval $a = 1$ is triviaal: alleen het lege product kan 1 opleveren. Laat nu $a > 1$, en stel

$$a = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_u$$

met $t \geq 1$ en $u \geq 1$, waarbij de getallen p_i (voor $1 \leq i \leq t$) en q_j (voor $1 \leq j \leq u$) priemgetallen zijn. We moeten bewijzen dat beide ontbindingen overeenstemmen, eventueel op de volgorde der factoren na. Er geldt $p_1 \mid p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_u$, en p_1 is priem, dus wegens 0.17 is minstens één van $q_1, q_2, \ldots, q_u$, zeg q_k, deelbaar door p_1. Maar q_k is priem, dus dit is alleen mogelijk als $q_k = p_1$. Laat nu in de eerste ontbinding van a de factor p_1 weg, en in de tweede de factor q_k. Dan krijgen we twee ontbindingen van het getal $a/p_1 = a/q_k$ in priemfactoren. Maar $a/p_1 < a$, dus de inductiehypothese, toegepast op a/p_1, vertelt ons dat deze twee ontbindingen dezelfde zijn (op volgorde na). Voegen we de factoren $p_1 = q_k$ weer toe, dan concluderen we dat ook de ontbindingen $a = p_1 p_2 \ldots p_t$ en $a = q_1 q_2 \ldots q_u$ dezelfde zijn (op volgorde na). Hiermee is de eenduidigheid van de priemfactorontbinding bewezen. Dit voltooit het bewijs van 0.18. □

Als p een priemgetal is en $a \in \mathbb{Z}$ met $a > 0$, dan geven we het aantal keren dat p voorkomt in de priemfactorontbinding van a aan met $\mathrm{ord}_p(a)$, of met $v_p(a)$. Er geldt dus

$$a = \prod_{p \text{ priem}} p^{\mathrm{ord}_p(a)}$$

waarbij het product zich uitstrekt over alle priemgetallen p; het product is weliswaar oneindig (zie Opgave 0.7), maar voor bijna alle p (d.w.z.: voor alle p op eindig veel na) geldt $\mathrm{ord}_p(a) = 0$, dus $p^{\mathrm{ord}_p(a)} = 1$. Er zijn dus maar eindig veel factoren die 'meetellen' en bijgevolg is het oneindige product betekenisvol.

Gevolg 0.19. *Voor p priem en a, b positieve gehele getallen geldt:*

$$\mathrm{ord}_p(a \cdot b) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b).$$

Bewijs. Een priemfactorontbinding van ab verkrijgt men door de priemfactorontbinding van a en b naast elkaar te zetten. Hieruit volgt 0.19. □

Gevolg 0.20. *Voor positieve gehele getallen c, d geldt:*

$$d \mid c \iff \text{voor alle priemgetallen } p \text{ geldt } \mathrm{ord}_p(d) \leq \mathrm{ord}_p(c).$$

Bewijs. $\Rightarrow$: Als $d \mid c$, dan $c = qd$ voor een $q \in \mathbb{Z}, q > 0$, dus 0.19 levert: $\mathrm{ord}_p(c) = \mathrm{ord}_p(d) + \mathrm{ord}_p(q) \geq \mathrm{ord}_p(d)$, voor ieder priemgetal p.

$\Leftarrow$: Er geldt

$$\frac{c}{d} = \frac{\prod_{p \text{ priem}} p^{\mathrm{ord}_p(c)}}{\prod_{p \text{ priem}} p^{\mathrm{ord}_p(d)}} = \prod_{p \text{ priem}} p^{\mathrm{ord}_p(c) - \mathrm{ord}_p(d)}.$$

Als nu voor alle p geldt $\mathrm{ord}_p(c) \geq \mathrm{ord}_p(d)$, dan zijn alle exponenten $\mathrm{ord}_p(c) - \mathrm{ord}_p(d)$ groter dan of gelijk aan nul, dus dan zien we dat c/d een *geheel* getal is, m.a.w. $d \mid c$. Dit bewijst 0.20. □

Gevolg 0.21. *Voor positieve, gehele getallen a en b geldt*

$$\mathrm{ggd}(a,b) = \prod_{p \text{ priem}} p^{\min\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}$$

Bewijs. Laat $d \in \mathbb{Z}_{>0}$. Volgens 0.20 is d een gemeenschappelijke deler van a en b dan en slechts dan als voor alle priemgetallen p geldt dat

$$\mathrm{ord}_p(d) \leq \mathrm{ord}_p(a) \quad \text{en} \quad \mathrm{ord}_p(d) \leq \mathrm{ord}_p(b).$$

Dit is hetzelfde als

$$\mathrm{ord}_p(d) \leq \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\},$$

voor alle p, hetgeen wegens 0.20 equivalent is met

$$d \mid \prod_{p \text{ priem}} p^{\min\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}$$

We zien dus dat de positieve gemeenschappelijke delers van a en b dezelfde zijn als de positieve delers van het getal $c = \prod_p p^{\min\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}$. Dan is ook de *grootste* gemeenschappelijke deler van a en b gelijk aan de grootste deler van c, en dat is $c = \prod_p p^{\min\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}$ zelf. Hiermee is 0.21 bewezen. □

Merk op dat dit argument ook een nieuw bewijs van 0.11 levert.

Voorbeeld 0.22. Er geldt $\mathrm{ggd}(600, 1260) = \mathrm{ggd}(2^3 \cdot 3 \cdot 5^2, 2^2 \cdot 3^2 \cdot 5 \cdot 7) = 2^2 \cdot 3 \cdot 5 = 60$.

De in 0.21 gegeven formule voor de grootste gemene deler van a en b is alleen van praktisch belang als de priemfactorontbinding van a en b bekend is. In andere gevallen verdient het Euclidische algoritme 0.6 de voorkeur.

Definitie 0.23. Laat $a, b \in \mathbb{Z}$. Als $a \neq 0$ en $b \neq 0$, dan is het *kleinste gemene veelvoud* van a en b het kleinste positieve gehele getal dat zowel een veelvoud van a als van b is; notatie: $\mathrm{kgv}(a, b)$. Bovendien zetten we $\mathrm{kgv}(a, 0) = \mathrm{kgv}(0, b) = 0$ voor alle $a, b \in \mathbb{Z}$.

Stelling 0.24. *Laat $a, b \in \mathbb{Z}$. Dan is ieder getal dat zowel van a als van b een veelvoud is, een veelvoud van* $\mathrm{kgv}(a, b)$. *Als $a > 0$ en $b > 0$ geldt*

$$\mathrm{kgv}(a,b) = \prod_{p \text{ priem}} p^{\max\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}.$$

Bewijs. Beschouw eerst het geval waarbij $a > 0$ en $b > 0$. Laat $d \in \mathbb{Z}_{>0}$. Volgens 0.20 is d een gemeenschappelijk veelvoud van a en b dan en slechts dan als voor alle priemgetallen p geldt dat

$$\mathrm{ord}_p(a) \leq \mathrm{ord}_p(d) \text{ en } \mathrm{ord}_p(b) \leq \mathrm{ord}_p(d).$$

Dit is hetzelfde als

$$\max\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\} \leq \mathrm{ord}_p(d),$$

voor alle p, hetgeen wegens 0.20 equivalent is met

$$\prod_p p^{\max\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}} \mid d.$$

We zien dus dat de positieve gemeenschappelijke veelvouden van a en b dezelfde zijn als de positieve veelvouden van het getal $c = \prod_p p^{\max\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}$. Dan is ook het *kleinste* positieve gemeenschappelijke veelvoud van a en b gelijk aan het kleinste positieve veelvoud van c, en dat is $c = \prod_p p^{\max\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}$ zelf. Hiermee is de in de stelling gegeven formule voor $\mathrm{kgv}(a,b)$ bewezen. Van de nog te bewijzen bewering:

$$a \mid d \quad \text{en} \quad b \mid d \quad \Longrightarrow \quad \mathrm{kgv}(a,b) \mid d \tag{0.24.1}$$

hebben we in bovenstaand bewijs bovendien reeds het geval afgehandeld waarbij a, b en d positief zijn. Het algemene geval laat zich, door het nemen van absolute waarden, tot dit speciale geval terugvoeren, behalve als a, b of d nul is; maar dan kan men (0.24.1) eenvoudig direct controleren. Hiermee is 0.24 bewezen. □

De grootste gemene deler en het kleinste gemene veelvoud kunnen ook voor meer dan twee getallen gedefinieerd worden: $\mathrm{ggd}(a_1, a_2, \ldots, a_t)$ is de grootste gemeenschappelijke deler van $a_1, a_2, \ldots, a_t$, behalve als alle a_i nul zijn, en $\mathrm{ggd}(0, 0, \ldots, 0) = 0$; en $\mathrm{kgv}(a_1, a_2, \ldots, a_t)$ is het kleinste positieve gemeenschappelijke veelvoud van $a_1, a_2, \ldots, a_t$, behalve als minstens één a_i nul is; in dit laatste geval $\mathrm{kgv}(a_1, a_2, \ldots, a_t) = 0$. Het formuleren en bewijzen van de met 0.9, 0.11, 0.21 en 0.24 overeenkomende beweringen laten we aan de lezer over.

Opgaven

0.1 ('Het b-tallig stelsel'). Laat $a, b \in \mathbb{Z}$ met $a \geq 0$ en $b \geq 2$. Bewijs dat er $t \in \mathbb{Z}_{\geq 0}$ en $c_0, c_1, \ldots, c_t \in \{0, 1, \ldots, b-1\}$ bestaan zodanig dat

$$a = c_t b^t + \cdots + c_2 b^2 + c_1 b + c_0.$$

Bewijs dat we in het geval $a \neq 0$ bovendien kunnen bereiken dat $c_t > 0$, en dat met deze extra voorwaarde de getallen t en $c_0, c_1, \ldots, c_t$ eenduidig bepaald zijn. (Aanwijzing: schrijf $a = qb + r$ als in 0.1, neem $c_0 = r$, en pas voor q de inductiehypothese toe.)

0.2 Laat $a, b \in \mathbb{Z}$, niet beide nul. Bewijs dat $a/\mathrm{ggd}(a,b)$ en $b/\mathrm{ggd}(a,b)$ onderling ondeelbaar zijn.

0.3

(a) Bepaal $\mathrm{ggd}(4511, 1625)$, en bepaal $x, y \in \mathbb{Z}$ met

$$x \cdot 4511 + y \cdot 1625 = \mathrm{ggd}(4511, 1625)\,.$$

(b) Bepaal $\mathrm{ggd}(20342, 14077)$, en bepaal $x, y \in \mathbb{Z}$ met

$$x \cdot 20342 + y \cdot 14077 = \mathrm{ggd}(20342, 14077)\,.$$

0.4 Laat $a, b \in \mathbb{Z}$ met $a \geq b > 0$. In deze opgave hebben $d, r_0, r_1, \ldots, q_0, q_1, \ldots$ dezelfde betekenis als in 0.6 en 0.9, de getallen $x_0, x_1, \ldots$ en $y_0, y_1, \ldots$ zijn de in het bewijs van 0.9 gekozene, en m is het getal waarvoor $r_m = 0$.

(a) Bewijs:

$$0 = x_1 < x_2 \leq -x_3 < x_4 < -x_5 < \ldots < (-1)^m x_m,$$

$$0 = y_0 < y_1 \leq -y_2 < y_3 < -y_4 < \ldots < (-1)^{m+1} y_m.$$

(b) Bewijs:

$$x_n y_{n+1} - x_{n+1} y_n = (-1)^n \text{ voor } 0 \leq n < m.$$

(c) Bewijs:

$$x_m = (-1)^m \cdot b/d, \quad y_m = (-1)^{m+1} \cdot a/d.$$

(Aanwijzing: gebruik dat $x_m a + y_m b = r_m = 0$, en dat x_m en y_m wegens (b) onderling ondeelbaar zijn.)

(d) Stel dat $a > b$. Bewijs dat de in het bewijs van 0.9 geconstrueerde oplossing x, y van $xa + yb = d$ voldoet aan

$$|x| \leq b/2d, \quad |y| \leq a/2d.$$

0.5 Laat $a, b \in \mathbb{Z}_{>0}$ en $d = \text{ggd}(a, b)$, en $x, y \in \mathbb{Z}$ zodanig dat $xa + yb = d$.

(a) Bewijs dat voor elke $t \in \mathbb{Z}$ de getallen

$$x' = x + t \cdot b/d, \quad y' = y - t \cdot a/d \qquad (*)$$

geheel zijn en voldoen aan de vergelijking

$$x'a + y'b = d. \qquad (\#)$$

(b) Omgekeerd, stel dat $x', y' \in \mathbb{Z}$ voldoen aan (#). Bewijs dat er een $t \in \mathbb{Z}$ is waarvoor (*) geldt.

(c) Veronderstel dat $a \neq b$, en dat x, y de in het bewijs van 0.9 geconstrueerde getallen met $xa+yb = d$ zijn. Bewijs: als $x', y' \in \mathbb{Z}$ voldoen aan (#), dan

$$|x'| \geq |x|, \quad |y'| \geq |y|.$$

(Aanwijzing: gebruik (*) en het resultaat van Opgave 0.4(d).)

0.6 Laat $p \in \mathbb{Z}, p > 1$. Bewijs: p is een priemgetal $\iff$ p bezit geen deler d met $1 < d \leq \sqrt{p}$.

0.7 (Euclides) Bewijs dat er oneindig veel priemgetallen bestaan.

0.8 Bereken

$$\text{ggd}(5400, 15000)$$

en

$$\text{ggd}(223553581, 397483969)$$

allebei met de formule van 0.21 en volgens de methode van Euclides 0.6.

0.9 Laat $a, b \in \mathbb{Z}$. Bewijs: $\text{ggd}(a, b) \cdot \text{kgv}(a, b) = |ab|$.

0.10 Laat $a, b, c \in \mathbb{Z}$. Bewijs:

(a) Als $\text{ggd}(a, b) = \text{ggd}(a, c) = 1$ dan is $\text{ggd}(a, bc) = 1$.

(b) Als $\text{ggd}(a, b) = 1$ en $a \mid c$ en $b \mid c$ dan geldt $ab \mid c$.

0.11 Laat $a, b, c \in \mathbb{Z}_{>0}$. Bewijs: $c \cdot \text{ggd}(a, b) = \text{ggd}(ca, cb)$.

0.12 Laat $a, b \in \mathbb{Z}_{>0}$.

(a) Zij r de rest van a bij deling door b. Bewijs dat $2^r - 1$ de rest van $2^a - 1$ bij deling door $2^b - 1$ is.

(b) Bewijs: $2^b - 1 \mid 2^a - 1 \iff b \mid a$.

(c) Bewijs: $\text{ggd}(2^a - 1, 2^b - 1) = 2^{\text{ggd}(a,b)} - 1$.

(d) Zijn (a), (b), (c) ook waar als men 2 vervangt door een geheel getal $c > 2$?

0.13 Laat $a, b, n \in \mathbb{Z}$, $n > 0$.

(a) Bewijs: $a - b \mid a^n - b^n$.

(b) Bewijs: als n oneven is, dan $a + b \mid a^n + b^n$.

0.14 Laten a, n gehele getallen > 1 zijn. Bewijs:

$$a^n - 1 \text{ is een priemgetal } \implies a = 2 \text{ en } n \text{ is een priemgetal.}$$

Geldt de omkering ook?

0.15 Laat p een priemgetal zijn, p' het kleinste priemgetal $> p$, en p'' het kleinste priemgetal $> p'$.

(a) Bewijs dat $p + p'$ niet geschreven kan worden als product van twee priemgetallen.

(b) Vind drie priemgetallen p waarvoor $p + p''$ het product van twee priemgetallen is.

0.16 Laat p een priemgetal > 3 zijn. Bewijs: $24 \mid p^2 - 1$.

0.17 Stel dat q_1, q_2, q_3, q_4, q_5 priemgetallen zijn met $q_1q_2q_3q_4q_5+1 = p^2$, met p priem. Bewijs: $p = 7, 11$ of 13.

0.18 Laat p een priemgetal zijn met de eigenschap dat $p^2 + 8$ ook een priemgetal is. Bewijs dat ook $p^3 + 4$ een priemgetal is.

0.19 Laat $x \in \mathbb{Q}$ met $x > 0$. Bewijs: er is een eenduidig bepaalde rij gehele getallen $(n_2, n_3, n_5, \ldots)$, bijna alle gelijk aan nul, zodanig dat

$$x = \prod_{p \text{ priem}} p^{n_p}.$$

0.20 Laten $p_1, p_2, \ldots, p_t$ verschillende priemgetallen zijn. Bewijs dat $\log p_1, \log p_2, \ldots, \log p_t$ lineair onafhankelijk over $\mathbb{Q}$ zijn, d.w.z., als $x_1, x_2, \ldots, x_t$ rationale getallen zijn met

$$x_1 \log p_1 + x_2 \log p_2 + \cdots + x_t \log p_t = 0$$

dan geldt $x_1 = x_2 = \cdots = x_t = 0$.

0.21

(a) Bewijs dat iedere $a \in \mathbb{Z}$ eenduidig te schrijven is als $a = \sum_{i=0}^{\infty} \varepsilon_i \cdot 3^i$, met $\varepsilon_i \in \{-1, 0, 1\}$ voor alle i, en $\varepsilon_i = 0$ voor bijna alle i.

(b) Bewijs dat iedere $a \in \mathbb{Z}$ eenduidig te schrijven is als $a = \sum_{i=0}^{\infty} \varepsilon_i \cdot 2^i$, met $\varepsilon_i \in \{-1, 0, 1\}$ voor alle i, en $\varepsilon_i = 0$ voor bijna alle i, en $\varepsilon_i\varepsilon_{i+1} = 0$ voor alle i.

Hoofdstuk 1

Groepen

Definitie 1.1. Een *bewerking* op een verzameling G is een afbeelding $G \times G \to G$.

Een bewerking is dus niets anders dan een afbeelding die aan elk geordend paar (a, b) van elementen van G een nieuw element van G toevoegt, dat we bijvoorbeeld $a \circ b$ kunnen noemen. Welk symbool we kiezen voor de bewerking is niet van belang: in plaats van $a \circ b$ hadden we ook $a \square b$, of $a \star b$, of iets anders kunnen schrijven. In de groepentheorie gebruiken we vaak ofwel de notatie $a \cdot b$, die doet denken aan een vermenigvuldiging, ofwel de notatie $a + b$, die doet denken aan een optelling. We zullen hier later op terugkomen.

Een bewerking zoals hier gedefinieerd wordt ook wel een *binaire* bewerking genoemd, om te benadrukken dat er *twee* elementen van G als "input" nodig zijn.

Een situatie die we herhaaldelijk zullen tegenkomen, is dat G gegeven is als een deelverzameling van een grotere verzameling X en dat we op X een bewerking $(a, b) \mapsto a \circ b$ hebben. In deze situatie zeggen we dat G *gesloten* is onder de bewerking $\circ$, als voor elk paar $(a, b) \in G \times G \subset X \times X$ geldt dat $a \circ b$ weer een element is van G. Als G gesloten is onder $\circ$ dan beperkt de afbeelding $\circ\colon X \times X \to X$ (de gegeven bewerking op X) tot een afbeelding $\circ\colon G \times G \to G$ en geeft dus een bewerking op G.

Definitie 1.2. Een *groep* is een verzameling G met daarop een bewerking $G \times G \to G$ (die we hier zullen aangeven met $(a, b) \mapsto a \circ b$), zodanig dat aan de volgende voorwaarden voldaan is:

(G1) (*Associativiteit* van $\circ$.) Voor alle $a, b, c \in G$ geldt $a \circ (b \circ c) = (a \circ b) \circ c$.

(G2) (Bestaan van een *neutraal element* of *eenheidselement*.) Er is een $e \in G$ zodanig dat

$$e \circ a = a \circ e = a$$

voor alle $a \in G$. Eén zo'n eenheidselement geven we in het vervolg met e aan.

(G3) (Bestaan van een *inverse*.) Voor elke $a \in G$ bestaat er een element $a^* \in G$ zodanig dat

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

De groep G heet *commutatief* of *abels* als bovendien voldaan is aan:

(G4) (*Commutativiteit* van $\circ$.) Voor alle $a, b \in G$ geldt $a \circ b = b \circ a$.

Niels Hendrik Abel, Noors wiskundige, 1802–1829

Een *eindige groep* is een groep met slechts eindig veel elementen.

Op één verzameling G kan men vaak vele bewerkingen definiëren, en verschillende hiervan kunnen een groep opleveren. Om een groep aan te duiden is het in principe dus niet voldoende alleen de verzameling G te geven: men moet er ook de bewerking bij vermelden. Tegen deze regel zullen we vaak zondigen; meestal is wel duidelijk welke bewerking bedoeld is.

Opmerking 1.3. In de literatuur komt men ook begrippen tegen waarbij niet aan alle hierboven genoemde voorwaarden hoeft te zijn voldaan. Zo noemt men een verzameling M die is voorzien van een bewerking zo dat aan (G1) en (G2) is voldaan (maar niet noodzakelijk aan (G3)) een *monoïde*.

Voorbeeld 1.4. Laat $G = \mathbb{R}$, met $\circ$ gedefinieerd door $a \circ b = a + b$, de gewone optelling in $\mathbb{R}$. Het is welbekend dat deze bewerking voldoet aan (G1), (G2) (met $e = 0$), (G3) (met $a^* = -a$) en (G4). Dus $\mathbb{R}$ is een abelse groep, de *additieve groep der reële getallen*.

Ook in de *additieve groep der gehele getallen* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ en in de *additieve groep der rationale getallen* $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$ wordt de groepsbewerking door de gewone optelling gegeven. De gewone optelling geeft geen groepsstructuur op $\mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, \ldots\}$, want aan (G3) is niet voldaan. In plaats van $\mathbb{Z}$, $\mathbb{Q}$ en $\mathbb{R}$ schrijven we ook wel $\mathbb{Z}^+$, $\mathbb{Q}^+$ en $\mathbb{R}^+$, om aan te geven dat de optelling de groepsbewerking is.

Voorbeeld 1.5. Laat $G = \mathbb{R} - \{0\}$, de verzameling der reële getallen ongelijk aan nul, en zij $\circ$ gedefinieerd door $a \circ b = ab$, de gewone vermenigvuldiging in $\mathbb{R}$. Dit is een welgedefinieerde bewerking op G, want het product van twee reële getallen ongelijk aan nul is weer ongelijk aan nul. Opnieuw is voldaan aan (G1), (G2) (met $e = 1$), (G3) (met $a^* = a^{-1}$) en (G4), dus $\mathbb{R} - \{0\}$ is een abelse groep ten opzichte van de vermenigvuldiging, de *multiplicatieve groep der reële getallen* (ongelijk aan nul), notatie: $\mathbb{R}^*$. Merk op dat we de nul moesten weglaten, omdat nul geen inverse bezit.

Op dezelfde manier definieert men de multiplicatieve groep der rationale getallen $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, met de gewone vermenigvuldiging als bewerking. Maar $\mathbb{Z} - \{0\}$ is geen groep ten opzichte van de gewone vermenigvuldiging: aan (G3) is niet voldaan.

Voorbeeld 1.6. Een *complex getal* is een uitdrukking van de vorm

$$a + bi, \qquad \text{met } a, b \in \mathbb{R}.$$

Voorbeelden van complexe getallen zijn

$$1+2i\,, \qquad 3-2i \quad (=3+(-2)i)\,, \qquad i \quad (=0+1i)\,.$$

We spreken af dat twee complexe getallen $a+bi$ en $a'+b'i$ (met $a,b,a',b' \in \mathbb{R}$) gelijk zijn dan en slechts dan als $a=a'$ en $b=b'$. We noemen a het *reële deel* van $a+bi$, notatie: $\mathrm{Re}(a+bi)$, en b het *imaginaire deel* van $a+bi$, notatie: $\mathrm{Im}(a+bi)$. De verzameling van alle complexe getallen wordt met $\mathbb{C}$ aangegeven. We beschouwen $\mathbb{R}$ als deelverzameling van $\mathbb{C}$ door $a=a+0i$, voor $a \in \mathbb{R}$.

Twee complexe getallen worden opgeteld door

$$(a+bi)+(c+di)=(a+c)+(b+d)i.$$

Het is eenvoudig te controleren dat $\mathbb{C}$, met de optelling als bewerking, aan (G1) t/m (G4) voldoet. Dus $\mathbb{C}$ is een abelse groep, de *additieve groep der complexe getallen.* Deze groep zullen we ook wel met $\mathbb{C}^+$ aangeven.

Twee complexe getallen worden vermenigvuldigd door

$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i\,.$$

(Dit vindt men door het product uit te werken en het regeltje $i^2=-1$ toe te passen.) Het is duidelijk dat dit een welgedefineerde bewerking is op de verzameling $\mathbb{C}$. De verificatie van de associatieve wet (G1) verloopt wat moeizamer: er geldt

$$\begin{aligned}((a+bi)\cdot(c+di))\cdot(f+gi) &= ((ac-bd)+(ad+bc)i)\cdot(f+gi)\\ &= ((ac-bd)f-(ad+bc)g)+((ac-bd)g+(ad+bc)f)i\\ &= (acf-bdf-adg-bcg)+(acg-bdg+adf+bcf)i\end{aligned}$$

en

$$\begin{aligned}(a+bi)\cdot((c+di)\cdot(f+gi)) &= (a+bi)\cdot((cf-dg)+(cg+df)i)\\ &= (a(cf-dg)-b(cg+df))+(a(cg+df)+b(cf-dg))i\\ &= (acf-bdf-adg-bcg)+(acg-bdg+adf+bcf)i,\end{aligned}$$

dus de vermenigvuldiging van complexe getallen is inderdaad associatief. Voorwaarde (G2) is ook vervuld: neem $e=1=1+0i$. Aan (G3) is echter niet voldaan, want $0=0+0i$ heeft geen inverse; immers, voor alle $c+di$ geldt $0\cdot(c+di)=0$, dus is er geen complex getal $c+di$ met $0\cdot(c+di)=1$.

Net als in Voorbeeld 1.5 laten we de nul nu weg, en we beschouwen de verzameling $\mathbb{C}-\{0\}$. We moeten voor $\mathbb{C}-\{0\}$ nu wel controleren dat deze verzameling gesloten is onder vermenigvuldiging; m.a.w., we moeten bewijzen: als $a+bi$ en $c+di$ complexe getallen ongelijk aan nul zijn, dan is ook hun product $(a+bi)(c+di)$ ongelijk aan nul. Hiertoe merken we op dat

$$(a-bi)(a+bi)(c+di)(c-di)=(a^2+b^2)(c^2+d^2)$$

en als $a+bi$ en $c+di$ ongelijk aan nul zijn dan is het rechterlid een positief reëel getal, dus $(a+bi)(c+di)$ kan niet gelijk zijn aan nul.

Het is duidelijk dat de vermenigvuldiging op de verzameling $\mathbb{C} - \{0\}$ nog steeds associatief is (deze eigenschap gaat uiteraard niet verloren als we ons beperken tot een deelverzameling) en dat nog steeds aan (G2) is voldaan, want 1 is een element van $\mathbb{C} - \{0\}$. Nu is aan (G3) wel voldaan, want voor $a + bi \neq 0$ geldt

$$a^2 + b^2 \neq 0,$$

en als inverse van $a + bi$ kunnen we nemen

$$\frac{a}{d} - \frac{b}{d}i, \qquad \text{met } d = a^2 + b^2.$$

Dit complexe getal geven we aan met $(a + bi)^{-1}$. We hebben nu bewezen dat $\mathbb{C} - \{0\}$ ten opzichte van de vermenigvuldiging een groep vormt, de *multiplicatieve groep der complexe getallen*, notatie $\mathbb{C}^*$. Men ziet gemakkelijk dat $\mathbb{C}^*$ abels is.

De *complex geconjugeerde* $\overline{\alpha}$ van een complex getal $\alpha = a + bi$ is gedefinieerd door

$$\overline{\alpha} = a - bi.$$

Men gaat eenvoudig na dat geldt:

$$\overline{\overline{\alpha}} = \alpha\,, \quad \overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}\,, \quad \overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$$

voor $\alpha, \beta \in \mathbb{C}$. Als $\alpha = a + bi$ dan is $\alpha \cdot \overline{\alpha} = \overline{\alpha} \cdot \alpha = a^2 + b^2$. Voor $\alpha \neq 0$ is de inverse α^{-1} dus het getal $\overline{\alpha}/(a^2 + b^2)$.

Stelling 1.7. *Laat G een groep zijn. Dan geldt:*

(a) *Er is precies één eenheidselement in G.*

(b) *Elk element van G heeft precies één inverse.*

(c) *Geven we, voor $a \in G$, de inverse van a met a^{-1} aan, dan geldt*

$$(a^{-1})^{-1} = a\,, \quad (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \qquad \textit{(let op de volgorde!)}$$

voor alle $a, b \in G$.

Bewijs. (a) Stel dat $e, e' \in G$ allebei eenheidselementen zijn. Dan $e' = e' \cdot e$ (want e is een eenheidselement), maar ook $e = e' \cdot e$ (want e' is een eenheidselement). Dus $e = e'$.

(b) Laat $a \in G$, en stel dat $b, c \in G$ allebei inversen van a zijn. Dan geldt

$$b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c,$$

dus a heeft niet meer dan één inverse. Wegens (G3) heeft a *minstens* één inverse. Dus a heeft precies één inverse.

(c) Omdat a^{-1} maar één inverse heeft (wegens (b)), en omdat geldt

$$a \cdot a^{-1} = a^{-1} \cdot a = e,$$

is a de inverse van a^{-1}, voor $a \in G$. Verder geldt, voor $a, b \in G$:

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

en op dezelfde wijze

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e.$$

Omdat $a \cdot b$ maar één inverse heeft (wegens (b)) volgt hieruit $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Hiermee is 1.7 bewezen. □

Wegens 1.7(a) en (b) kunnen we in het vervolg over *het* eenheidselement van een groep en *de* inverse van een groepselement spreken.

Opmerking 1.8. In het vervolg zullen we voor groepen vaak de *multiplicatieve* schrijfwijze hanteren, d.w.z. we schrijven $a \cdot b$ of ab in plaats van $a \circ b$, we noemen dit het *product* van de *factoren* a en b, en we zeggen dat ab verkregen wordt door a en b te *vermenigvuldigen*; verder schrijven we a^{-1} in plaats van a^*.

In andere voorbeelden zullen we de *additieve* schrijfwijze gebruiken, waarin we $a + b$ in plaats van $a \circ b$ schrijven. Deze schrijfwijze is gereserveerd voor abelse groepen.

Voor verdere terminologie en notaties zie onderstaande tabel.

Multiplicatief	Additief
ab of $a \cdot b$	$a + b$
product	som
factoren	termen
vermenigvuldigen	optellen
a^{-1}	$-a$
inverse (of omgekeerde)	tegengestelde
e (of 1)	0
eenheidselement	nulelement
ab^{-1}	$a - b$ $(= a + (-b))$
delen	aftrekken

In de voorbeelden hierboven zijn we alleen nog abelse groepen tegengekomen. We gaan nu voorbeelden bekijken waarbij ook niet-abelse groepen optreden.

Voorbeeld 1.9. De *quaternionen* van Hamilton

Sir William Rowan Hamilton, Engels-Iers wiskundige, 1805–1865.

Quaternionen zijn uitdrukkingen van de vorm

$$a + bi + cj + dk, \qquad \text{met } a, b, c, d \in \mathbb{R}.$$

Twee quaternionen $a + bi + cj + dk$ en $a' + b'i + c'j + d'k$ zijn gelijk dan en slechts dan als $a = a'$, $b = b'$, $c = c'$ en $d = d'$. We geven de verzameling der quaternionen aan met $\mathbb{H}$, en beschouwen $\mathbb{C}$ als deelverzameling van $\mathbb{H}$ door $a + bi = a + bi + 0j + 0k$, voor $a, b \in \mathbb{R}$.

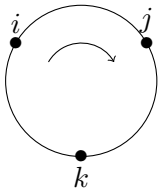
Quaternionen worden componentsgewijs opgeteld:

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k,$$

voor $a, b, c, d, a', b', c', d' \in \mathbb{R}$. Deze optelling maakt $\mathbb{H}$ tot een abelse groep, de *additieve groep der quaternionen*, notatie $\mathbb{H}$ of $\mathbb{H}^+$.

De vermenigvuldiging van quaternionen berust op de regeltjes

$$\begin{aligned} &i^2 = j^2 = k^2 = -1, \\ &ij = k, \quad ji = -k, \\ &jk = i, \quad kj = -i, \\ &ki = j, \quad ik = -j \end{aligned}$$



met de klok mee: $+$
tegen de klok in: $-$

Uitgewerkt levert dit

$$\begin{aligned} (a + bi + cj + dk) \cdot (a' + b'i + c'j + d'k) = \quad & (aa' - bb' - cc' - dd') \\ & + (ab' + ba' + cd' - dc')\, i \\ & + (ac' - bd' + ca' + db')\, j \\ & + (ad' + bc' - cb' + da')\, k. \end{aligned}$$

Evenals bij de complexe getallen kan men nu rechtstreeks verfiëren dat deze vermenigvuldiging associatief is. Deze verificatie wordt aanzienlijk bekort als men quaternionen niet met vier reële coëfficiënten a, b, c, d beschrijft, maar met twee complexe coëfficiënten $\alpha = a + bi$ en $\beta = c + di$:

$$a + bi + cj + dk = \alpha + \beta j \qquad (\text{want } ij = k).$$

De vermenigvuldiging krijgt dan de volgende gedaante:

$$(\alpha + \beta j) \cdot (\gamma + \delta j) = (\alpha\gamma - \beta\overline{\delta}) + (\alpha\delta + \beta\overline{\gamma})\, j$$

voor $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, waarbij $\bar{}$ complexe conjucatie aangeeft (zie 1.6).

Het element $1 \in \mathbb{H}$ is een neutraal element voor de vermenigvuldiging, en elke quaternion $a + bi + cj + dk$ ongelijk nul heeft een inverse

$$\frac{a}{n} - \frac{b}{n}i - \frac{c}{n}j - \frac{d}{n}k, \qquad \text{met } n = a^2 + b^2 + c^2 + d^2 > 0.$$

Net als bij de complexe getallen leidt men hieruit af dat $\mathbb{H}^* = \mathbb{H} - \{0\}$ ten opzichte van de vermenigvuldiging een groep is, de *multiplicatieve groep der quaternionen*. Dit is een voorbeeld van een groep die niet commutatief is, want

$$i \cdot j = k \neq -k = j \cdot i.$$

Voorbeeld 1.10. *Vectoren.* Laat $n \in \mathbb{Z}_{>0}$, en zij $\mathbb{R}^n$ de verzameling n-tallen reële getallen:

$$\mathbb{R}^n = \left\{(a_1, a_2, \ldots, a_n) \;\middle|\; a_i \in \mathbb{R} \ (1 \leq i \leq n)\right\}.$$

Dergelijke n-tallen worden componentsgewijs opgeteld:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Het is eenvoudig na te gaan dat zo een commutatieve groep verkregen wordt. Er geldt $\mathbb{R}^1 = \mathbb{R}$, de groep $\mathbb{R}^2$ is 'dezelfde' groep als $\mathbb{C}^+$, en $\mathbb{R}^4$ is 'dezelfde' als $\mathbb{H}^+$ (de precieze betekenis van 'dezelfde' is 'isomorf', zie Hoofdstuk 2).

Voorbeeld 1.11. *Matrices.* Een 2×2-*matrix* met reële coëfficiënten is een viertal reële getallen gerangschikt in een vierkant:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad a, b, c, d \in \mathbb{R}.$$

Het product van 2×2-matrices is als volgt gedefinieerd:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} g & h \\ i & j \end{pmatrix} = \begin{pmatrix} ag + bi & ah + bj \\ cg + di & ch + dj \end{pmatrix}.$$

Deze vermenigvuldiging is associatief, en heeft als neutraal element de *eenheidsmatrix*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

De *determinant* van een matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

wordt gedefinieerd door $\det(A) = ad - bc$. Er geldt

$$\det(A \cdot B) = \det(A) \cdot \det(B),$$

zoals men gemakkelijk narekent. Als de matrix A een inverse heeft, dan vinden we, als we $B = A^{-1}$ nemen: $\det(A) \cdot \det(B) = \det(AB) = \det(I) = 1$, dus $\det(A) \neq 0$. Omgekeerd, als $\det(A) \neq 0$, dan blijkt een inverse van A gegeven te worden door

$$A^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}, \qquad \text{met } \Delta = \det(A).$$

We concluderen: A heeft een inverse $\iff \det(A) \neq 0$. Laat

$$\mathrm{GL}(2, \mathbb{R}) = \left\{A \;\middle|\; A \text{ is een } 2 \times 2\text{-matrix met reële coëfficiënten, en } \det(A) \neq 0\right\}.$$

Het is nu eenvoudig na te gaan dat $\mathrm{GL}(2,\mathbb{R})$, met als bewerking de matrixvermenigvuldiging, een groep is (zie Opgave 1.17), de groep van *inverteerbare* of *niet-singuliere* 2×2-matrices over $\mathbb{R}$. De groep is niet commutatief, er geldt bijvoorbeeld

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\cdot\begin{pmatrix}1&0\\1&1\end{pmatrix}=\begin{pmatrix}2&1\\1&1\end{pmatrix}\neq\begin{pmatrix}1&1\\1&2\end{pmatrix}=\begin{pmatrix}1&0\\1&1\end{pmatrix}\cdot\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

Lezers die lineaire algebra kennen zullen onmiddelijk inzien dat het bovenstaande ook voor $n\times n$-matrices geldt, waarbij n een willekeurig positief geheel getal is. Is A een $n\times n$-matrix met reële coëfficiënten, dan geldt:

$$A \text{ heeft een inverse } \iff \det(A)\neq 0,$$

en de verzameling

$$\mathrm{GL}(n,\mathbb{R})=\{A \mid A \text{ is een } n\times n\text{-matrix met reële coëfficiënten, en } \det(A)\neq 0\}$$

vormt een groep ten opzichte van de matrixvermenigvuldiging. Deze groep is alleen abels als $n=1$ (merk op: $\mathrm{GL}(1,\mathbb{R})=\mathbb{R}^*$). Vervangen we in bovenstaande definitie "reële" door "rationale" of "complexe", dan vinden we de groepen $\mathrm{GL}(n,\mathbb{Q})$ en $\mathrm{GL}(n,\mathbb{C})$. Al deze groepen worden wel de *algemene lineaire* groepen genoemd; "GL" betekent "general linear".

Voorbeeld 1.12. *De viergroep van Klein.*

Felix Klein, Duits wiskundige, 1849–1925.

Laat $V_4=\{e,a,b,c\}$ (vier verschillende elementen), en laat xy, voor $x,y\in V_4$, door de volgende tabel gedefinieerd zijn:

x \ y	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Samengevat: e is neutraal element; $xx=e$ voor alle x; en het product van twee verschillende elementen uit $\{a,b,c\}$ is gelijk aan het derde element.

Een tabel als boven heet een *vermenigvuldigingstafel*, of, als de vermenigvuldiging aan (G1) t/m (G3) voldoet, een *groepentabel*. Aan de vermenigvuldigingstafel kan men in één oogopslag zien of aan (G2), (G3) en (G4) voldaan is. Met (G1) (de associatieve wet) ligt dat in het algemeen minder eenvoudig (zie J. Vuillemin, Comment vérifier l'associativité d'une table de groupe, Theor. Comp. Sci.

4 (1977), 77–82), maar voor V_4 zijn er slechts enkele gevallen te onderscheiden; we laten dit aan de lezer over (zie ook Opgave 1.8).

De conclusie is dat V_4 een eindige abelse groep is, de *viergroep van Klein*. Voor alle $x \in V_4$ geldt $x^{-1} = x$. Groepen met deze eigenschap zijn altijd abels (zie Opgave 1.14).

Merk op dat elk element van V_4 in elke kolom en in elke rij van de groepentabel precies éénmaal voorkomt. Uit Stelling 1.23 beneden volgt dat elke groepentabel deze eigenschap heeft.

Een ander groep van vier elementen is $\{1, i, -1, i\} \subset \mathbb{C}^*$, waarbij de vermenigvuldiging die der complexe getallen is. In deze groep geldt *niet* dat $x = x^{-1}$ voor alle x, dus het is niet 'dezelfde' groep als V_4.

Voorbeeld 1.13. *De quaternionengroep Q.* Laat $Q = \{1, i, j, k, -1, -i, -j, -k\} \subset \mathbb{H}^*$, en laten de elementen van Q vermenigvuldigd worden als quaternionen (zie 1.9). Dit levert een eindige niet-abelse groep van acht elementen.

Voorbeeld 1.14. *De restklassengroep $\mathbb{Z}/n\mathbb{Z}$.* Laat n een willekeurig positief geheel getal zijn. In dit voorbeeld gaan we een groep van n elementen construeren. Een *restklasse* modulo n is de verzameling van alle gehele getallen die bij deling door n een gegeven rest hebben. Omdat er n verschillende resten kunnen optreden bij delingen door n, namelijk $0, 1, 2, \ldots, n-1$, zijn er precies n verschillende restklassen modulo n. Voor $n = 3$ zijn dit bijvoorbeeld

$$\begin{aligned}
&\{\ldots, -6, -3, 0, 3, 6, 9, \ldots, 1002, \ldots\} && \text{(de 3-vouden)},\\
&\{\ldots, -5, -2, 1, 4, 7, 10, \ldots, 583, \ldots\} && \text{(de 3-vouden plus 1)},\\
&\{\ldots, -7, -4, -1, 2, 5, 8, \ldots, 419, \ldots\} && \text{(de 3-vouden plus 2)}.
\end{aligned}$$

De n restklassen modulo n zijn paarsgewijs disjunct, en hun vereniging is $\mathbb{Z}$. Voor $a \in \mathbb{Z}$ geeft men de restklasse waar a in zit aan met $a + n\mathbb{Z}$, of met $a \bmod n$, of, als n vast is, met $\overline{a}$. Dus er geldt:

$$\begin{aligned}
\overline{a} = \overline{b} &\iff a \text{ en } b \text{ hebben dezelfde rest bij deling door } n\\
&\iff a - b \text{ is deelbaar door } n\\
&\iff n \mid a - b.
\end{aligned}$$

Als $\overline{a} = \overline{b}$ dan zegt men wel dat a en b *congruent* zijn modulo n, notatie: $a \equiv b \mod n$. (Congruentie modulo n is een equivalentierelatie, waarvan de equivalentieklassen precies de restklassen modulo n zijn.)

De verzameling restklassen modulo n geeft men aan met $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned}
\mathbb{Z}/n\mathbb{Z} &= \{0 \bmod n\,, 1 \bmod n\,, \ldots\,, (n-1) \bmod n\}\\
&= \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}\\
&= \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n}\} \qquad (\text{want } \overline{n} = \overline{0}).
\end{aligned}$$

Voorbeeld: als $n = 3$ dan $\overline{0} = \overline{3} = \overline{1002}$, $\overline{1} = \overline{7} = \overline{583}$, $\overline{-1} = \overline{2} = \overline{419}$,

$$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\} = \{\overline{-1}, \overline{0}, \overline{1}\}.$$

We definiëren een operatie + op $\mathbb{Z}/n\mathbb{Z}$ door

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

waarbij de + rechts in $\mathbb{Z}$ genomen is. We moeten wel controleren dat $\overline{a+b}$ niet van de keuze van a en b afhangt, d.w.z. als $\overline{a_1} = \overline{a_2}$ en $\overline{b_1} = \overline{b_2}$ dan moeten we nagaan dat $\overline{a_1+b_1} = \overline{a_2+b_2}$. Dat is niet moeilijk: uit $\overline{a_1} = \overline{a_2}$ en $\overline{b_1} = \overline{b_2}$ volgt $n \mid a_1 - a_2$ en $n \mid b_1 - b_2$, en dan geldt ook $n \mid (a_1-a_2)+(b_1-b_2) = (a_1+b_1)-(a_2+b_2)$, dus $\overline{a_1+b_1} = \overline{a_2+b_2}$.

Voorbeeld: als $n = 3$ dan is $\overline{1} = \overline{583}$ en $\overline{2} = \overline{419}$. Tellen we op dan vinden we

$$\overline{1} + \overline{2} = \overline{3}\,, \qquad \overline{583} + \overline{419} = \overline{1002}$$

en inderdaad is $\overline{3} = \overline{1002}$. Als $n = 15$, dan is $\overline{3} + \overline{12} = \overline{0}$ en $\overline{11} + \overline{11} = \overline{7}$.

De verzameling $\mathbb{Z}/n\mathbb{Z}$ met de bewerking + is een eindige abelse groep met n elementen. Bewijs hiervan: (G1) volgt direct uit de associativiteit van + in $\mathbb{Z}$:

$$\begin{aligned}(\overline{a} + \overline{b}) + \overline{c} &= \overline{(a+b)} + \overline{c} \\ &= \overline{(a+b)+c} = \overline{a+(b+c)} \\ &= \overline{a} + \overline{(b+c)} = \overline{a} + (\overline{b} + \overline{c});\end{aligned}$$

(G2): neem $e = \overline{0}$; (G3): neem $\overline{a}^* = \overline{-a}$ (dus, in de additieve notatie: $-\overline{a} = \overline{-a}$); (G4) volgt uit de commutativiteit van + in $\mathbb{Z}$. De groep $\mathbb{Z}/n\mathbb{Z}$ wordt ook wel met $(\mathbb{Z}/n\mathbb{Z})^+$ aangegeven.

De constructie van $\mathbb{Z}/n\mathbb{Z}$ is een special geval van de constructie van een *factorgroep* die we in Hoofdstuk 4 zullen behandelen.

De groep $\mathbb{Z}/n\mathbb{Z}$ wordt ook wel de cyclische groep met n elementen genoemd (zie gevolg 3.8).

Voorbeeld 1.15. *De multiplicatieve restklassengroep* $(\mathbb{Z}/n\mathbb{Z})^*$. Laat weer $n \in \mathbb{Z}$ met $n > 0$. We definiëren op $\mathbb{Z}/n\mathbb{Z}$ een operatie $\cdot$ door

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

waarbij $\cdot$ rechts de gewone vermenigvuldiging in $\mathbb{Z}$ aangeeft. Net als bij de optelling moeten we nagaan dat deze definitie niet van de keuze van de representanten a en b afhangt. Inderdaad: als $\overline{a_1} = \overline{a_2}$ en $\overline{b_1} = \overline{b_2}$ dan $n \mid a_1 - a_2$ en $n \mid b_1 - b_2$, dus ook $n \mid (a_1 - a_2) \cdot b_1 + a_2 \cdot (b_1 - b_2) = a_1 b_1 - a_2 b_2$, d.w.z. $\overline{a_1 b_1} = \overline{a_2 b_2}$, zoals verlangd.

Voorbeeld: als $n = 15$, dan

$$\overline{2} \cdot \overline{2} = \overline{4}\,, \qquad \overline{3} \cdot \overline{7} = \overline{6}\,, \qquad \overline{9} \cdot \overline{10} = \overline{0}\,, \qquad \overline{-4} \cdot \overline{8} = \overline{-2} = \overline{13}\,.$$

Het is gemakkelijk na te gaan dat $\mathbb{Z}/n\mathbb{Z}$ met $\cdot$ voldoet aan (G1), (G2) (met $e = \overline{1}$) en (G4). Maar (G3) is niet vervuld (voor $n > 1$) omdat de vergelijking

$$\overline{x} \cdot \overline{a} = \overline{1} \tag{1.15.1}$$

bijvoorbeeld voor $\overline{a} = \overline{0}$ geen oplossing heeft; immers, voor alle x geldt $\overline{x} \cdot \overline{0} = \overline{x \cdot 0} = \overline{0} \neq \overline{1}$.

Om toch een groep te krijgen beperken we ons tot de deelverzameling van alle $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ waarvoor de vergelijking (1.15.1) wèl een oplossing heeft:

$$(\mathbb{Z}/n\mathbb{Z})^* = \big\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \;\big|\; \text{er is een } \overline{x} \in \mathbb{Z}/n\mathbb{Z} \text{ zo dat } \overline{x} \cdot \overline{a} = \overline{1}\big\}.$$

Om deze verzameling beter te begrijpen, merken we op dat voor $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ geldt:

$$\begin{aligned} &\text{er is een } \overline{x} \in \mathbb{Z}/n\mathbb{Z} \text{ zo dat } \overline{x} \cdot \overline{a} = \overline{1} \\ &\quad \iff \text{er bestaan } x, y \in \mathbb{Z} \text{ zodanig dat } x \cdot a + y \cdot n = 1 \\ &\quad \iff \mathrm{ggd}(a, n) = 1\,, \end{aligned}$$

waarbij de laatste equivalentie volgt uit 0.12. Er geldt derhalve:

$$(\mathbb{Z}/n\mathbb{Z})^* = \big\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \;\big|\; \mathrm{ggd}(a, n) = 1\big\}.$$

(Hierbij dienen we op te merken dat $\mathrm{ggd}(a, n)$ enkel afhangt van de restklasse van a modulo n; zie Opgave 1.5.) Voorbeelden:

$$(\mathbb{Z}/1\mathbb{Z})^* = \{\overline{1}\}\,, \qquad (\mathbb{Z}/2\mathbb{Z})^* = \{\overline{1}\}\,, \qquad (\mathbb{Z}/3\mathbb{Z})^* = \{\overline{1}, \overline{2}\}\,, \qquad (\mathbb{Z}/6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}\,,$$

en

$$(\mathbb{Z}/15\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}\,.$$

Als p een priemgetal is, dan is $(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$.

Uit de definitie gaat men gemakkelijk na dat de deelverzameling $(\mathbb{Z}/n\mathbb{Z})^* \subset (\mathbb{Z}/n\mathbb{Z})$ gesloten is onder de vermenigvuldiging van restklassen. We laten het eenvoudige bewijs dat $(\mathbb{Z}/n\mathbb{Z})^*$ met $\cdot$ een abelse groep vormt aan de lezer over (vgl. Opgave 1.17). Deze groep heet de *multiplicatieve* restklassengroep modulo n. Het aantal elementen van $(\mathbb{Z}/n\mathbb{Z})^*$ wordt aangegeven met $\varphi(n)$; men noemt φ de *φ-functie van Euler*.

Leonhard Euler, Zwitsers wiskundige, 1707–1783

Dus:

$$\varphi(n) = \#\big\{a \in \mathbb{Z} \;\big|\; 1 \le a \le n, \mathrm{ggd}(a, n) = 1\big\}\,.$$

Voorbeelden:

$$\varphi(1) = \varphi(2) = 1\,, \quad \varphi(3) = \varphi(6) = 2\,, \quad \varphi(15) = 8\,, \quad \varphi(5186) = \varphi(5187) = \varphi(5188) = 2592$$

en $\varphi(p) = p - 1$ als p priem is. Bij het vak Ringen en Lichamen zullen we zien dat

$$\varphi(n) = n \cdot \prod_{p|n,\ p \text{ priem}} \left(1 - \frac{1}{p}\right).$$

Om de inverse van een element $\overline{a}$ in de groep $(\mathbb{Z}/n\mathbb{Z})^*$ te berekenen dienen we (1.15.1) op te lossen. Dit kunnen we doen met de methode uit Hoofdstuk 0. Voorbeeld: we berekenen $\overline{22}^{-1} \in (\mathbb{Z}/101\mathbb{Z})^*$ als volgt:

$$\begin{aligned}
\overline{0} \cdot \overline{22} &= \overline{101} \\
\overline{1} \cdot \overline{22} &= \overline{22} && \text{(deze 4}\times\text{ van de vorige aftrekken)} \\
\overline{-4} \cdot \overline{22} &= \overline{13} && \text{(deze 1}\times\text{)} \\
\overline{5} \cdot \overline{22} &= \overline{9} && \text{(deze 1}\times\text{)} \\
\overline{-9} \cdot \overline{22} &= \overline{4} && \text{(deze 2}\times\text{)} \\
\overline{23} \cdot \overline{22} &= \overline{1},
\end{aligned}$$

dus $\overline{22}^{-1} = \overline{23}$. Inderdaad geldt $23 \cdot 22 = 506 = 1 + 5 \cdot 101 \equiv 1 \mod 101$.

Voorbeeld 1.16. *Groepen van afbeeldingen.* Als X een verzameling is, en $f\colon X \to X$ en $g\colon X \to X$ zijn twee afbeeldingen, dan is de *samenstelling* $f \circ g$ van f en g de afbeedling $X \to X$ gedefinieerd door

$$(f \circ g)(x) = f\big(g(x)\big) \qquad (x \in X),$$

dus $(f \circ g)$ krijgen we door "eerst g toe te passen, dan f". Samenstellen van afbeeldingen is associatief, d.w.z.

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

als $f, g, h\colon X \to X$ afbeeldingen zijn. Immers voor elke $x \in X$ geldt

$$\begin{aligned}
\big(f \circ (g \circ h)\big)(x) &= f\big((g \circ h)(x)\big) = f\big(g(h(x))\big) \\
&= \big(f \circ g\big)(h(x)) = \big((f \circ g) \circ h\big)(x),
\end{aligned}$$

dus inderdaad $f \circ (g \circ h) = (f \circ g) \circ h$.

Als men wil bewijzen dat een bepaalde verzameling afbeeldingen $X \to X$ een groep vormt met als bewerking het samenstellen van afbeeldingen dan is het dus niet meer nodig voorwaarde (G1) (associativiteit) te controleren: deze is automatisch vervuld.

De verzameling van *alle* afbeeldingen $X \to X$ vormt geen groep met de samenstelling als bewerking (behalve als $\#X \leq 1$): immers, voor het neutrale element komt alleen de identieke afbeelding $\mathrm{id}_X\colon X \to X$, gedefinieerd door $\mathrm{id}_X(x) = x$ voor alle $x \in X$, in aanmerking (vergelijk het bewijs van 1.7(a)), maar niet elke afbeelding $X \to X$ heeft een inverse, dus aan (G3) is niet voldaan.

Beperkt men zich tot die afbeeldingen $X \to X$ die wel een inverse bezitten, d.w.z. de *bijectieve* afbeeldingen, dan verkrijgt men wel een groep. Deze groep wordt aangegeven met $S(X)$:

$$S(X) = \big\{ f\colon X \to X \;\big|\; f \text{ is bijectief} \big\}.$$

Het is gemakkelijk te controleren dat $S(X)$, met als bewerking het samenstellen van afbeeldingen, een groep vormt. Als $X = \{1, 2, \ldots, n\}$, met $n \in \mathbb{Z}_{>0}$, dan schrijft men wel S_n in plaats van $S(X)$. De elementen van S_n heten *permutaties*, en S_n heet de *symmetrische groep* op n elementen.

Lemma 1.17. *De groep S_n heeft $n! = n \cdot (n-1) \cdots 2 \cdot 1$ elementen.*

Bewijs. Stel $\sigma \in S_n$ dan zijn er n mogelijkheden voor $\sigma(1)$. Voor $\sigma(2)$ zijn er $n-1$ mogelijkheden want $\sigma(1) \neq \sigma(2)$ omdat σ injectief is. Voor $\sigma(3)$ zijn er $n-2$ mogelijkheden enz. In totaal zijn er dus $n! = n \cdot (n-1) \cdots 2 \cdot 1$ mogelijkheden om σ te kiezen. □

Een permutatie kan weergegeven worden als een matrix met twee rijen. In de bovenste rij staan de elementen $\{1, \ldots, n\}$ en daaronder hun beelden: $\left(\begin{smallmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{smallmatrix}\right)$. Dit is echter nogal omslachtig, daarom worden permutaties meestal in de cykelnotatie weergegeven.

Een permutatie $\sigma \in S_n$ heet een *cykel* of een *cyclische permutatie* van lengte k als er k verschillende elementen $a_1, a_2, \ldots, a_k \in X$ bestaan zodanig dat

$$\sigma(x) = \begin{cases} a_{i+1} & \text{als } x = a_i,\ 1 \leq i < k \\ a_1 & \text{als } x = a_k \\ x & \text{als } x \in X \setminus \{a_1, \ldots, a_k\} \end{cases}$$

We schrijven dan $\sigma = \big(a_1\ a_2\ \ldots\ a_k\big)$.

Bijvoorbeeld: $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{smallmatrix}\right) = \big(1\ 3\ 4\big) = \big(3\,4\,1\big)$ is een cyclische permutie van lengte 3, maar $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right) = \big(1\ 3\big) \circ \big(2\ 4\big)$ is niet cyclisch.

Een cykel van lengte 2 heet een *verwisseling* of *transpositie*. Twee cykels $\big(a_1\ a_2\ \ldots\ a_k\big)$ en $\big(b_1\ b_2\ \ldots\ b_l\big)$ heten *disjunct* als de verzamelingen $\{a_1, a_2, \ldots, a_k\}$ en $\{b_1, b_2, \ldots, b_l\}$ disjunct zijn, d.w.z. als $a_i \neq b_j$ voor alle i en j met $1 \leq i \leq k$ en $1 \leq j \leq l$. Een belangrijke opmerking is dat disjuncte cykels onderling commuteren: als $\sigma = \big(a_1\ a_2\ \ldots\ a_k\big)$ en $\tau = \big(b_1\ b_2\ \ldots\ b_l\big)$ disjunct zijn dan is $\sigma \circ \tau = \tau \circ \sigma$, zoals men gemakkelijk nagaat.

Stelling 1.18. *Elke permutatie σ van X kan geschreven worden als product van een aantal paarsgewijs disjuncte cykels. Deze schrijfwijze is eenduidig bepaald, op de volgorde van de factoren en op cykels van lengte* 1 *na.*

Bewijs. Met volledige inductie naar $n = \#X$. Als $n = 1$ dan geldt $\sigma = (1)$ (een cykel van lengte één). Laat nu $n > 1$, en kies $x \in X$. Beschouw de elementen

$$x\,, \quad \sigma(x)\,, \quad \sigma^2(x)\,, \quad \sigma^3(x)\,, \quad \ldots$$

van X, waarbij natuurlijk $\sigma^2 = \sigma \circ \sigma$ en $\sigma^3 = \sigma \circ \sigma \circ \sigma$, etcetera (zie 1.24). Omdat X eindig is, bestaan er ℓ en m met $\ell < m$ en $\sigma^\ell(x) = \sigma^m(x)$. Pas hierop $\sigma^{-\ell}$ toe, dan vinden we $x = \sigma^{m-\ell}(x)$. Er is dus een $k > 0$ met $\sigma^k(x) = x$. Kiezen we k zo klein mogelijk, dan zijn bovendien de elementen

$$x\,, \quad \sigma(x)\,, \quad \sigma^2(x)\,, \quad \sigma^3(x)\,, \quad \ldots\,, \quad \sigma^{k-1}(x)$$

alle verschillend. Het effect van σ op de deelverzameling $\{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)\} \subset X$ wordt dan gegeven door de cykel van lengte k

$$\sigma_1 = \big(x\ \sigma(x)\ \sigma^2(x)\ \sigma^3(x)\ \ldots\ \sigma^{k-1}(x)\big)\,.$$

Laat nu $X' = X \setminus \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)\}$. Dan is $\#X' = n - k$. Als $X' = \emptyset$ dan $\sigma = \sigma_1$, en we zijn klaar. Als $X' \neq \emptyset$, dan wordt het effect van σ op X' gegeven door een permutatie τ van X'. We kunnen nu schrijven $\sigma = \tau \circ \sigma_1 = \sigma_1 \circ \tau$ waarbij we afspreken dat τ als de identiteit op $\{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)\}$ werkt. Omdat X' minder elementen dan X heeft, kunnen we de inductiehypothese op τ toepassen. We vinden dan dat τ geschreven kan worden als $\tau = \sigma_2 \circ \sigma_3 \circ \cdots \circ \sigma_t$ waarbij $\sigma_2, \sigma_3, \ldots, \sigma_t$ paarsgewijs disjuncte cyclische permutaties van X' zijn. Dan geldt $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_t$ waarbij $\sigma_1, \sigma_2, \ldots, \sigma_t$ paarsgewijs disjuncte cykels zijn.

Hiermee hebben we bewezen dat elke permutatie het product van een aantal paarsgewijs disjuncte cykels is. Het bewijs van de eenduidigheid laten we aan de lezer over. □

Er geldt bijvoorbeeld

$$\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 10 & 1 & 5 & 3 & 7 & 9 & 8 & 6 & 2 \end{smallmatrix}\right) = \big(1\ 4\ 5\ 3\big)\,\big(2\ 10\big)\,\big(6\ 7\ 9\big).$$

De cykelnotatie kan ook gebruikt worden om twee permutaties snel samen te stellen:

$$\underbrace{(1\ 3\ 4)(2\ 5)}_{\sigma} \circ \underbrace{(1\ 2\ 3)(4\ 5\ 6)}_{\tau} = (1\ 5\ 6)(2\ 4)$$

want $(\sigma \circ \tau(1) = \sigma(2) = 5$, $\sigma \circ \tau(5) = \sigma(6) = 6$ enz.)

De groep $S(X)$ is niet commutatief als $\#X \geq 3$ want $(12)(13) = (132) \neq (13)(12) = (123)$

Andere interessante groepen verkrijgen we door ons te beperken to bijectieve afbeeldingen $X \to X$ die een bepaalde structuur op X invariant laten. We geven een aantal meetkundige voorbeelden.

Voorbeeld 1.19. In het eerste voorbeeld veronderstellen we enige lineaire algebra bekend. Laat X een n-dimensionale vectorruimte over $\mathbb{R}$ zijn, en zij

$$G = \big\{f\colon X \to X \;\big|\; f \text{ is een bijectieve lineaire afbeelding}\big\}\,.$$

(Ter herinnering: f heet lineair als $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ voor alle $x, y \in X$ en $\lambda, \mu \in \mathbb{R}$.) De verzameling G is een groep met de samenstelling als bewerking. Kiest men een basis van X, dan kan men de elementen van G met behulp van $n \times n$ matrices beschrijven, en men ziet dat G niets anders is dan de groep $\mathrm{GL}(n, \mathbb{R})$ besproken in 1.11.

Voorbeeld 1.20. In het volgende voorbeeld nemen we voor X het gewone (euclidische) platte vlak $\mathbb{R}^2$. Een *congruentie* of *isometrie* van $\mathbb{R}^2$ is een afbeelding $\sigma\colon \mathbb{R}^2 \to \mathbb{R}^2$ met de eigenschap dat voor alle P, $Q \in \mathbb{R}^2$ geldt

$$d(P, Q) = d\big(\sigma(P), \sigma(Q)\big)\,,$$

waarbij $d(P, Q)$ de afstand tussen P en Q aangeeft; dus als $P = (p_1, p_2)$ en $Q = (q_1, q_2)$ dan is $d(P, Q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2}$.

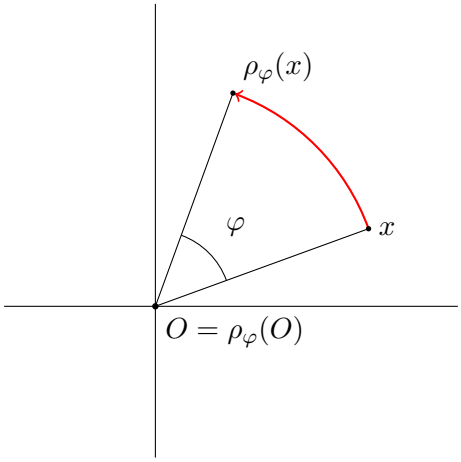
We geven enkele voorbeelden van congruenties:

(a) *Translaties.* Is $P = (p_1, p_2)$, dan is de afbeelding $t_P \colon \mathbb{R}^2 \to \mathbb{R}^2$ gegeven door $(x_1, x_2) \mapsto (x_1 + p_1, x_2 + p_2)$ een congruentie die we translatie over P noemen. Translaties zijn bijectief en er gelden de rekenregels

$$t_O = \mathrm{id}_{\mathbb{R}^2}\,, \quad t_Q \circ t_P = t_{P+Q}\,, \quad (t_P)^{-1} = t_{-P}\,,$$

waarbij $O = (0, 0)$ de oorsprong aangeeft en waarbij we voor $P = (p_1, p_2)$ en $Q = (q_1, q_2)$ schrijven $P + Q = (p_1 + q_1, p_2 + q_2)$ en $-P = (-p_1, -p_2)$.

(b) *Rotaties rond de oorsprong.* Voor $\varphi \in \mathbb{R}$ is ρ_φ de rotatie die het vlak over een hoek φ om de oorsprong draait (tegen de klok in):



Deze rotatie is een inverteerbare *lineaire* transformatie van $\mathbb{R}^2$ die wordt gegeven door de matrix

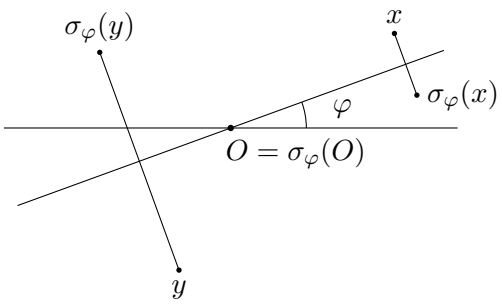
$$\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix},$$

en er gelden de rekenregels

$$\rho_0 = \mathrm{id}_{\mathbb{R}^2}\,, \quad \rho_\varphi \circ \rho_\psi = \rho_\psi \circ \rho_\varphi = \rho_{\varphi+\psi}\,.$$

Verder geldt dat $\rho_\varphi = \rho_\psi$ dan en slechts dan als de hoeken φ en ψ een geheel veelvoud van 2π van elkaar verschillen. Om alle rotaties te krijgen hoeven we dus slechts de hoeken met $0 \leq \varphi < 2\pi$ te beschouwen.

(c) *Spiegelingen in een lijn door de oorsprong.* Voor $\varphi \in \mathbb{R}$ is σ_φ de spiegeling in de lijn door de oorsprong die een hoek φ maakt met de x-as:



Ook deze spiegeling is een inverteerbare lineaire transformatie van $\mathbb{R}^2$ die wordt gegeven door de matrix

$$\begin{pmatrix} \cos(2\varphi) & \sin(2\varphi) \\ \sin(2\varphi) & -\cos(2\varphi) \end{pmatrix},$$

en er geldt

$$\sigma_\varphi \circ \sigma_\psi = \rho_{2(\varphi-\psi)}\,, \quad (\sigma_\varphi)^{-1} = \sigma_\varphi\,.$$

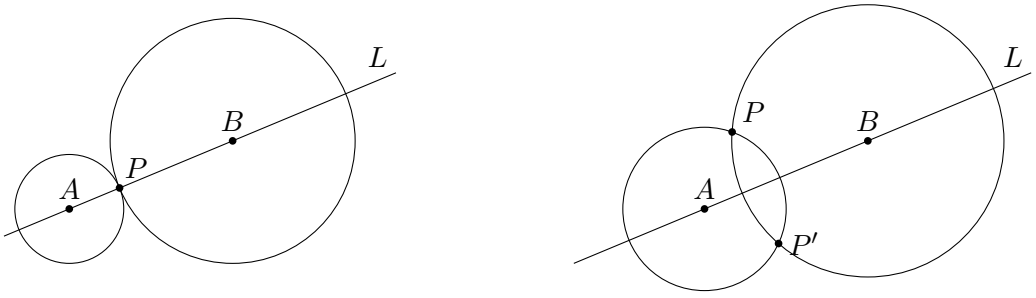
Merk op dat spiegelingen (in tegenstelling tot rotaties) dus niet onderling commuteren: $\sigma_\varphi \circ \sigma_\psi = (\sigma_\psi \circ \sigma_\varphi)^{-1}$ en in het algemeen is dit niet hetzelfde als $\sigma_\psi \circ \sigma_\varphi$. Er geldt $\sigma_\varphi = \sigma_\psi$ dan en slechts dan als φ en ψ een geheel veelvoud van π verschillen.

Door translaties, rotaties en spiegelingen te combineren krijgen we algemenere congruenties van $\mathbb{R}^2$; zo is bijvoorbeeld een samenstelling $t_P \circ \sigma_\varphi$ een spiegeling in een lijn die (voor $P \neq O$) niet door de oorsprong gaat. (Een dergelijke congruentie is dus niet een lineaire transformatie van $\mathbb{R}^2$, aangezien de oorsprong niet op zichzelf wordt afgebeeld.) Het is niet moeilijk om na te gaan dat, voor $P \in \mathbb{R}^2$ en φ, $\psi \in \mathbb{R}$, de volgende regels gelden:

$$\rho_\varphi \circ t_P = t_{\rho_\varphi(P)} \circ \rho_\varphi\,, \qquad \rho_\varphi \circ \sigma_\psi = \sigma_{\psi+\frac{1}{2}\varphi}\,,$$
$$\sigma_\varphi \circ t_P = t_{\sigma_\varphi(P)} \circ \sigma_\varphi\,, \qquad \sigma_\psi \circ \rho_\varphi = \sigma_{\psi-\frac{1}{2}\varphi}\,.$$

We zullen bewijzen dat *elke* congruentie van $\mathbb{R}^2$ te schrijven is als $t_P \circ \rho_\varphi$ of $t_P \circ \sigma_\varphi$ voor zekere $P \in \mathbb{R}^2$ en $\varphi \in \mathbb{R}$. (Merk op dat we voor $P = O$ geldt $t_P \circ \rho_\varphi = \rho_\varphi$ en $t_P \circ \sigma_\varphi = \sigma_\psi$.) Een direct gevolg hiervan is dat congruenties automatisch bijectief zijn (iets dat niet bij voorbaat duidelijk was), dat ze lijnen in lijnen overvoeren, en hoeken behouden. Als we eenmaal weten dat congruenties bijectief zijn, dan gaan we gemakkelijk na dat de verzameling congruenties een groep is, met als bewerking het samenstellen van afbeeldingen (zoals steeds in deze voorbeelden). We zullen voor deze groep de notatie $\mathrm{E}(\mathbb{R}^2)$ gebruiken.

Om in te zien dat elke congruentie van de gestelde vorm is, tonen we eerst aan dat een congruentie $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ die twee verschillende punten A en B vastlaat, ofwel de identieke afbeelding is, of de spiegeling in de lijn L door A en B. Als $P \in \mathbb{R}^2$, laat $a = d(A,P)$ en $b = d(B,P)$. Omdat f een congruentie is met $f(A) = A$ en $f(B) = B$, voert f de cirkel C_1 met middelpunt A en straal a over in zichzelf; evenzo voert f de cirkel C_2 met middelpunt B en straal b over in zichzelf. Als P op L ligt, dan is P het unieke snijpunt van deze twee cirkels, dus $f(P) = P$. Als P niet op L ligt, dan snijden C_1 en C_2 elkaar in precies twee punten, namelijk P en het spiegelbeeld van P in de lijn L (dat in de figuur hieronder aangegeven wordt met P').



Als er tenminste één punt $P \notin L$ is met $f(P) = P$ dan kunnen we het voorgaande ook toepassen met A en B vervangen door P en een willekeurige $Q \in L$; in dat geval vinden we dat $f = \mathrm{id}_{\mathbb{R}^2}$. De enige andere mogelijkheid is dat f de spiegeling is in de lijn L.

Laat nu $g\colon \mathbb{R}^2 \to \mathbb{R}^2$ een willekeurige congruentie zijn. Nemen we $P = g(O)$, dan is $h = t_{-P} \circ g$ een congruentie met de eigenschap dat $h(O) = O$. Het beeld van het punt $Q = (1, 0)$ onder h is een punt op de eenheidscirkel, dus er is een hoek φ zo dat $h(Q) = \rho_\varphi(Q)$. Dan is $f = \rho_{-\varphi} \circ h = \rho_{-\varphi} \circ t_{-P} \circ g$ een congruentie die de punten O en Q vastlaat, en vanwege het resultaat dat we zojuist hebben bewezen, volgt dat f de identiteit is of de spiegeling σ_0 in de x-as. Dit betekent precies dat

$$g = t_P \circ \rho_\varphi\,, \quad \text{of} \quad g = t_P \circ \rho_\varphi \circ \sigma_0 = t_P \circ \sigma_{\frac{1}{2}\varphi}\,,$$

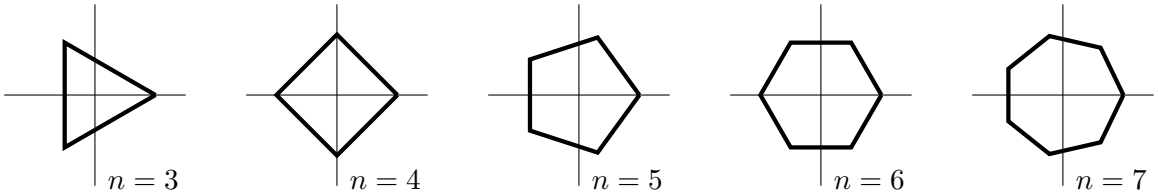
zoals te bewijzen was.

Beperken we ons tot congruenties van $\mathbb{R}^2$ die de oorsprong vastlaten, dan vinden we de zogeheten *orthogonale groep*

$$\mathrm{O}_2(\mathbb{R}) = \left\{\text{congruenties } f\colon \mathbb{R}^2 \to \mathbb{R}^2 \text{ met } f(O) = O\right\}.$$

Uit de voorgaande discussie volgt dat $\mathrm{O}_2(\mathbb{R})$ bestaat uit twee soorten elementen: de rotaties ρ_φ en de spiegelingen σ_ψ. Bovendien kunnen we, dankzij de hierboven gegeven rekenregels, elke spiegeling schrijven in de vorm $\rho_\varphi \circ \sigma$, waarbij $\sigma = \sigma_0$ (de spiegeling in de x-as). Met behulp van de rekenregels $\rho_\varphi \circ \sigma = \sigma \circ \rho_{-\varphi}$ en $\sigma^2 = \mathrm{id}_{\mathbb{R}^2}$ kunnen we samenstellingen eenvoudig weer in standaardvorm schrijven; zo geldt bijvoorbeeld $(\rho_\varphi \circ \sigma) \circ \rho_\psi = \rho_\varphi \circ \rho_{-\psi} \circ \sigma = \rho_{\varphi-\psi} \circ \sigma$ en daarmee $(\rho_\varphi \circ \sigma) \circ (\rho_\psi \circ \sigma) = \rho_{\varphi-\psi}$.

Voorbeeld 1.21. De *diëdergroep* D_n (voor $n \in \mathbb{Z}, n \geq 2$) kan men nu definiëren als de verzameling van die congruenties van het platte vlak, die een gegeven regelmatige n-hoek in zichzelf overvoeren.



Nemen we de oorsprong in het midden van de n-hoek, en kiezen we de n-hoek zo dat deze het punt $(1, 0)$ als een van zijn hoekpunten heeft, dan vinden we:

$$D_n = \{\rho_0, \rho_{2\pi/n}, \rho_{4\pi/n}, \ldots, \rho_{(2n-2)\pi/n}\} \cup \{\sigma_0, \sigma_{\pi/n}, \sigma_{2\pi/n}, \ldots, \sigma_{(n-1)\pi/n}\}.$$

Gemakshalve schrijven we $\sigma = \sigma_0$ en $\rho = \rho_{2\pi/n}$. Verder schrijven we $\rho^k = \rho \circ \rho \circ \cdots \circ \rho$ (k factoren) en $\rho^0 = \mathrm{id}_X$; dan is $\rho_{2k\pi/n} = \rho^k$ en $\sigma_{k\pi/n} = \rho^k \circ \sigma$ (zie 1.20). Daarmee vinden we

$$D_n = \left\{\rho^k \;\middle|\; 0 \leq k < n\right\} \;\cup\; \left\{\rho^k \circ \sigma \;\middle|\; 0 \leq k < n\right\}.$$

De rekenregels zijn

$$\begin{aligned} \rho^n &= \mathrm{id}_X \quad (= \rho^0), \\ \sigma^2 &= \mathrm{id}_X, \\ \sigma\rho^k &= \rho^{n-k}\sigma. \end{aligned}$$

De diëdergroep D_n is inderdaad een groep, en heeft $2n$ elementen. Voor $n > 2$ is D_n niet commutatief, want $\sigma\rho = \rho^{n-1}\sigma \neq \rho\sigma$.

1.22 Linksaxioma's. In de definitie van een groep kunnen de voorwaarden (G2) en (G3) worden afgezwakt tot:

(G2') (Bestaan van een *links-eenheidselement.*) Er is een $e \in G$ zodanig dat

$$e \circ a = a$$

voor alle $a \in G$;

(G3') (Bestaan van een *links-inverse.*) Voor elke $a \in G$ bestaat er een element $a^* \in G$ zodanig dat

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

Deze voorwaarden heten de *linksaxioma's.* Vervangt men $e \circ a$ door $a \circ e$ en $a^* \circ a$ door $a \circ a^*$ dan krijgt men de *rechtsaxioma's* (G2") en (G3").

Om te zien dat (G2), (G3) uit de zwakkere axioma's (G2'), (G3') volgen, als men (G1) aanneemt, bewijst men eerst dat een links-inverse a^* van a ook een rechts-inverse van a is:

$$\begin{aligned} aa^* &= e \cdot (aa^*) = (ea) \cdot a^* \\ &= ((a^{**} \cdot a^*) \cdot a) \cdot a^* && (a^{**} = \text{links-inverse van } a^*) \\ &= (a^{**} \cdot (a^* \cdot a)) \cdot a^* \\ &= (a^{**} \cdot e) \cdot a^* = a^{**} \cdot (e \cdot a^*) = a^{**} \cdot a^* \\ &= e, \end{aligned}$$

en dan dat een links-eenheidselement ook een rechts-eenheidselement is:

$$ae = a(a^*a) = (aa^*)a = ea = a.$$

Dus (G2) en (G3) kunnen inderdaad door de linksaxioma's (G2') en (G3') vervangen worden. Op dezelfde wijze ziet men in dat ze ook door de rechtsaxioma's (G2") en (G3") vervangen kunnen worden. Evenwel niet door (G2'), (G3"), zoals het voorbeeld uit Opgave 1.15 laat zien.

Stelling 1.23. *Laat G een groep zijn, en $a, b \in G$. Dan is er precies één $x \in G$ met $ax = b$, namelijk $x = a^{-1}b$. Bovendien is er precies één $y \in G$ met $ya = b$, namelijk $y = ba^{-1}$.*

Bewijs. Er geldt $a \cdot (a^{-1}b) = (aa^{-1}) \cdot b = e \cdot b = b$, dus $x = a^{-1}b$ voldoet aan de vergelijking $ax = b$. Maar het is ook de enige oplossing van die vergelijking, want omgekeerd volgt uit $ax = b$ dat $x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b$. Dit bewijst het eerste deel van 1.23. Het tweede deel gaat op analoge wijze. □

Voor de groepentabel van G (zie 1.12) betekent 1.23, dat elk element van G precies één keer in elke kolom en elke rij voorkomt. We kunnen 1.23 ook zó formuleren: voor elke $a \in G$ zijn de afbeeldingen

$$\lambda_a \colon G \to G \quad \text{en} \quad \rho_a \colon G \to G$$

gedefinieerd door

$$\lambda_a(x) = ax\,, \qquad \rho_a(x) = xa \qquad (x \in G)$$

("linksvermenigvuldiging" en "rechtsvermenigvuldiging" met a) *bijectief.*

1.24 Producten van meer factoren. Als $a_1, a_2, \ldots, a_n$ elementen van een groep G zijn, $n \geq 2$, dan definiëren we het product $a_1 a_2 \cdots a_n$ met volledige inductie naar n door

$$\begin{aligned} a_1 a_2 &= \text{het product van } a_1 \text{ en } a_2 \text{ in de groep} && (n = 2), \\ a_1 a_2 \cdots a_n &= (a_1 a_2 \cdots a_{n-1}) \cdot a_n && (n > 2). \end{aligned}$$

Bijvoorbeeld $abcde = (((ab)c)d)e$. Met volledige inductie naar n leidt men gemakkelijk uit de associatieve wet (G1) af:

$$(a_1 a_2 \cdots a_k) \cdot (a_{k+1} \cdots a_n) = a_1 a_2 \cdots a_n \qquad (1 \leq k \leq n-1)$$

en uit 1.7(c):

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}.$$

Als G abels is, schrijft men in plaats van $a_1 a_2 \cdots a_n$ wel $\prod_{i=1}^{n} a_i$. Wanneer alle factoren a_i gelijk zijn, $a_i = a$, schrijft men

$$a^n = a_1 a_2 \cdots a_n.$$

Voorts zetten we

$$a^1 = a\,, \quad a^0 = e \quad \text{en} \quad a^{-n} = (a^{-1})^n \quad \text{voor } n \in \mathbb{Z}_{>0}.$$

Dus nu hebben we a^n gedefinieerd voor alle $a \in G$ en $n \in \mathbb{Z}$. De kleinste $n > 0$ waarvoor $a^n = e$ wordt ook wel de *orde van* a genoemd en aangeduid met orde(a). Op dit concept komen we later terug in hoofdstuk 3.

Eenvoudig gaat men de volgende eigenschappen na:

$$\begin{aligned} a^{n+m} &= a^n \cdot a^m, \\ a^{nm} &= (a^n)^m, \end{aligned}$$

voor alle $a \in G$, $n, m \in \mathbb{Z}$. Bovendien

$$(ab)^n = a^n b^n \quad \text{als } G \textit{ abels} \text{ is,}$$

voor alle $a, b \in G$, $n \in \mathbb{Z}$. Als G *niet* abels is geldt deze laatste eigenschap *niet*, zie Opgave 1.19.

In het bovenstaande zijn we er van uitgegaan dat de groep multiplicatief genoteerd is. Wordt de *additieve* schrijfwijze gehanteerd, dan schrijft men

$$\begin{aligned} a_1 + a_2 + \cdots + a_n \quad &\text{in plaats van} \quad a_1 a_2 \cdots a_n, \\ \sum_{i=1}^{n} a_i \quad &\text{in plaats van} \quad \prod_{i=1}^{n} a_i, \\ na \text{ of } n \cdot a \quad &\text{in plaats van} \quad a^n. \end{aligned}$$

De rekenregels luiden in additieve notatie:

$$\begin{aligned} 1a &= a, \\ 0a &= 0, \\ (n+m)a &= na + ma, \\ n(ma) &= (nm)a, \\ n(a+b) &= na + nb, \end{aligned}$$

voor $n, m \in \mathbb{Z}$ en $a, b \in G$, waarbij we er ten behoeve van de laatste regel van uitgaan dat G abels is.

Opgaven

1.1 Laat G een groep zijn, en laat $x, y, a \in G$. Neem aan dat $ax = ay$ geldt. Laat zien: $x = y$.

1.2 De *geconjugeerde* $\overline{x}$ van een quaternion $x = a+bi+cj+dk$ is gedefinieerd door $\overline{x} = a-bi-cj-dk$, voor $a, b, c, d \in \mathbb{R}$. De *norm* $N(x)$ van x is gedefinieerd door $N(x) = x\overline{x}$.

(a) Bewijs:

$$\begin{aligned} \overline{x+y} &= \overline{x} + \overline{y}, \\ \overline{xy} &= \overline{y} \cdot \overline{x}, \\ N(xy) &= N(x)N(y) \end{aligned}$$

voor alle $x, y \in \mathbb{H}$.

(b) Laat V de verzameling gehele getallen n zijn die geschreven kunnen worden als

$$n = a^2 + b^2 + c^2 + d^2, \text{ met } a, b, c, d \in \mathbb{Z}.$$

Bewijs: als $n \in V$ en $m \in V$, dan $n \cdot m \in V$.

1.3

(a) Laat A een 2×2-matrix met coëfficiënten uit $\mathbb{Z}$ zijn. Bewijs: A heeft een inverse die ook coëfficiënten in $\mathbb{Z}$ heeft $\iff \det(A) = \pm 1$.

(b) Bewijs dat de verzameling

$$\mathrm{GL}(2, \mathbb{Z}) = \left\{ A \;\middle|\; A \text{ is een } 2 \times 2\text{-matrix met coëfficiënten uit } \mathbb{Z}, \text{ en } \det(A) = \pm 1 \right\}$$

met de matrixvermenigvuldiging een groep vormt.

(c) Generaliseer (a) en (b) voor $n \times n$-matrices, waarbij n een willekeurig positief geheel getal is.

1.4 Laat $x \in Q$ met $x \neq \pm 1$. Bewijs: $x^2 = -1$.

1.5 Zij n een positief geheel getal.

(a) Als a en b gehele getallen zijn die congruent zijn modulo n, dus $a \equiv b \bmod n$, laat zien dat $\mathrm{ggd}(a, n) = \mathrm{ggd}(b, n)$. Zodoende is $\mathrm{ggd}(\overline{a}, n)$, voor $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, welgedefinieerd.

(b) Als $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, laat zien dat $\mathrm{ggd}(\overline{a} \cdot \overline{b}, n) = \mathrm{ggd}(\overline{b}, n)$ voor alle $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$.

1.6 Laat $\overline{a} = (a \mod 157) \in \mathbb{Z}/157\mathbb{Z}$, voor $a \in \mathbb{Z}$, en beschouw:

$$\overline{17}\,, \quad \overline{-768}\,, \quad \overline{51}\,, \quad \overline{1744}\,, \quad \overline{100}\,, \quad \overline{-57}\,.$$

Hoeveel verschillende elementen van $\mathbb{Z}/157\mathbb{Z}$ staan hier?

1.7 Bepaal $\overline{100}^{-1} \in (\mathbb{Z}/257\mathbb{Z})^*$.

1.8 Maak een groepentabel van $(\mathbb{Z}/12\mathbb{Z})^*$ en vergelijk deze met de groepen tabel van V_4 (zie 1.12). Gebruik de gelijkenis om de associativiteit van de op V_4 gedefinieerde bewerking snel te bewijzen.

1.9 Laat $n \in \mathbb{Z}_{>0}$ en $a \in \mathbb{Z}$.

(a) Bewijs: $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^* \iff \overline{-a} \in (\mathbb{Z}/n\mathbb{Z})^*$.

(b) Bewijs: als n oneven is, dan

$$\overline{a} = \overline{-a} \iff \overline{a} = \overline{0}$$

en als n even is, dan

$$\overline{a} = \overline{-a} \iff \overline{a} = \overline{0} \text{ of } \overline{n/2}.$$

(c) Bewijs: als $n > 2$ dan is $\varphi(n)$ *even*.

1.10 Maak een groepentabel van D_2. Is D_2 abels? Laat zien dat D_2 "dezelfde" groep is als V_4.

1.11 Maak een groepentabel van D_3 en D_4.

1.12 Bewijs dat er 48 congruenties (= transformaties die alle afstanden gelijk laten) van de driedimensionale ruimte zijn die een gegeven kubus op zichzelf afbeelden. Vormen deze een groep? Een abelse groep? Hoeveel congruenties van de driedimensionale ruimte voeren een gegeven regelmatig twintigvlak in zichzelf over?

1.13 Stel dat in een groep G geldt

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

voor alle $a, b \in G$. Bewijs dat G abels is.

1.14 Stel dat in een groep G geldt

$$x^{-1} = x$$

voor alle $x \in G$. Bewijs dat G abels is.

1.15 Zij V een verzameling met $\#V \geq 2$, en definieer op V een bewerking $\circ$ door $a \circ b = b$, voor alle $a, b \in V$. Bewijs dat V, met deze bewerking, voldoet aan (G1), (G2'), (G3"), maar niet een groep is.

1.16 Zij G een verzameling met een bewerking $\circ$, die voldoet aan (G2') en zo dat voor alle a, b, $c \in G$ geldt: $(a \circ b) \circ c = a \circ (c \circ b)$. Bewijs dat voldaan is aan (G1), (G2) en (G4) (dus dat G een "commutatieve monoïde" is).

1.17

(a) Laat G met de bewerking $\circ$ een monoïde zijn (zie Opmerking 1.3 voor de definitie). Bewijs dat

$$G^* = \left\{ a \in G \;\middle|\; \text{er is een } x \in G \text{ met } x \circ a = a \circ x = e \right\}$$

met de bewerking $\circ$ een groep is.

(b) Gebruik het resultaat van (a) om aan te tonen dat $\mathrm{GL}(2, \mathbb{R})$ en $(\mathbb{Z}/n\mathbb{Z})^*$ (zie 1.11 en 1.15) groepen zijn.

1.18 Geef precieze bewijzen van de in 1.24 gedane beweringen.

1.19 Laat G een groep zijn. Bewijs: er geldt

$$(ab)^2 = a^2 b^2 \quad \text{voor alle } a, b \in G$$

dan en slechts dan als G abels is.

1.20 Laat G een groep zijn, en $n \in \mathbb{Z}$. Bewijs: er geldt

$$(ab)^n = a^n b^n \quad \text{voor alle } a, b \in G$$

dan en slechts dan als

$$(ab)^{1-n} = a^{1-n} b^{1-n} \quad \text{voor alle } a, b \in G.$$

1.21 Laat G bestaan uit de 27 uitdrukkingen

$$\alpha^i \beta^j \gamma^k, \text{ met } i, j, k \in \{0, 1, 2\},$$

en laat op G een vermenigvuldiging gedefinieerd zijn door

$$(\alpha^i \beta^j \gamma^k) \cdot (\alpha^l \beta^m \gamma^n) = \alpha^{i+l+km} \beta^{j+m} \gamma^{k+n},$$

waarbij de exponenten modulo 3 genomen worden.

(a) Bewijs dat G, met deze vermenigvuldiging, een niet-commutatieve groep is.

(b) Bewijs dat $x^3 = e$ voor elke $x \in G$.

1.22 Construeer een niet-abelse groep G met de eigenschap (Hint: gebruik de voorgaande oefeningen)

$$(ab)^{-2} = a^{-2}b^{-2} \quad \text{voor alle } a, b \in G.$$

1.23 Ga in elk van de volgende zeven gevallen na of '$\circ$' een bewerking is op G en aan welke van de voorwaarden (G1), (G2), (G3), (G4) voldaan is.

(a) $G = \mathbb{Z}_{>0}$ met $a \circ b = a^b$.

(b) $G = \mathbb{R}$ met $a \circ b = (a^2 + 1) \cdot \log\big(|b| + 1\big)$.

(c) $G = \mathbb{R}_{>1}$ met $a \circ b = a^{\log b}$.

(d) $G = \{-1, 0, 1\}$ met $a \circ b = a + b$ (gewone optelling).

(e) $G = \mathbb{Z}_{>0}$ met $a \circ b = \max\{a, b\}$.

(f) $G = \mathbb{R}$ met $a \circ b = a + b - 3$.

(g) $G = \{0, 1, 2, 3, 4, 5\}$ met $a \circ b$ gegeven door de volgende tabel:

a \ b	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	4	5	2
2	2	3	0	5	1	4
3	3	4	5	0	2	1
4	4	5	1	2	0	3
5	5	2	4	1	3	0

1.24 (a) Schrijf elk van de volgende permutaties als product van disjuncte cykels, en doe hetzelfde voor hun inversen:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 1 & 2 & 3 \end{pmatrix}.$$

(b) Schrijf de permutaties

$$(1\ 4\ 5\ 2)(2\ 3\ 4) \quad \text{en} \quad (2\ 3\ 4)(1\ 4\ 5\ 2)$$

als product van disjuncte cykels.

1.25 Bewijs: $(a_1\ a_2\ \ldots\ a_k)^{-1} = (a_k\ a_{k-1}\ \ldots\ a_1)$.

1.26 Laat $\sigma, \tau \in S_n$.

(a) Stel dat $a \in \{1, 2, \ldots, n\}$ door τ op $a' \in \{1, 2, \ldots, n\}$ wordt afgebeeld. Bewijs dat $\sigma(a)$ door $\sigma\tau\sigma^{-1}$ op $\sigma(a')$ wordt afgebeeld.

(b) Leid uit (a) af: als de ontbinding van τ in disjuncte cykels wordt gegeven door

$$\tau = (a_1\ a_2\ \ldots\ a_k)(b_1\ b_2\ \ldots\ b_\ell)\cdots(g_1\ g_2\ \ldots\ g_q)$$

dan wordt de ontbinding van $\sigma\tau\sigma^{-1}$ in disjuncte cykels gegeven door

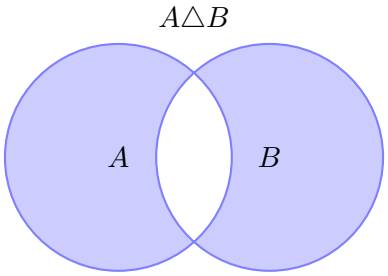
$$\sigma\tau\sigma^{-1} = \big(\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_k)\big)\ \big(\sigma(b_1)\ \sigma(b_2)\ \ldots\ \sigma(b_\ell)\big)\cdots\big(\sigma(g_1)\ \sigma(g_2)\ \ldots\ \sigma(g_q)\big)\,.$$

(c) Laat $\alpha, \beta \in S_n$. Stel dat $\alpha\beta$ het product is van t disjuncte cykels van lengtes $k_1, k_2, \ldots, k_t$. Bewijs dat $\beta\alpha$ ook het product is van t disjuncte cykels van lengtes $k_1, k_2, \ldots, k_t$.

1.27 Laat $\tau = (123\ldots n) \in S_n$ en $\sigma \in S_n$ Bewijs dat $\sigma\tau = \tau\sigma \iff \sigma = \tau^i$ voor een $i \in \mathbb{Z}$ met $0 \le i < n$.

1.28 Zij X een verzameling, en $P(X)$ de verzameling van alle deelverzamelingen van X. Voor $A, B \in P(X)$ is het *symmetrisch verschil* $A\triangle B$ gedefinieerd door

$$A\triangle B = (A \cup B) - (A \cap B).$$



(a) Bewijs dat $P(X)$ met de bewerking $\triangle$ een abelse groep is.

(b) Laat $\#X = 2$. Bewijs dat $P(X)$ "dezelfde" groep is als V_4.

1.29 Laat G een groep zijn met bewerking $\circ$, en X een niet-lege verzameling. Met G^X geven we de verzameling van alle functies $f\colon X \to G$ aan. Voor $f_1, f_2 \in G^X$ definiëren we $f_1 \cdot f_2 \in G^X$ door

$$(f_1 \cdot f_2)\big(x\big) = f_1(x) \circ f_2(x) \quad (x \in X).$$

(a) Bewijs dat G^X met deze bewerking een groep is.

(b) Bewijs: G^X is abels $\iff$ G is abels.

1.30 Laat $G \subset \mathbb{R}$ een *eindige* deelverzameling zijn waarvoor geldt dat $0 \in G$ en dat voor alle $a \in G$ ook $-a \in G$. Voor $a, b \in G$ zij $a \circ b$ het element van G dat het dichts bij $a+b$ ligt, waarbij in geval van twijfel—d.w.z., als er *twee* elementen van G het dichtst bij $a+b$ liggen—het element met de grootste waarde gekozen wordt.

(a) Bewijs dat aan (G2), (G3) en (G4) voldaan is.

(b) Bewijs: als x het grootste element van G is en y het kleinste, dan geldt $(x \circ x) \circ y = 0$, $x \circ (x \circ y) = x$.

(c) Bewijs dat G een groep is met de bewerking $\circ$ dan en slechts dan als $G = \{0\}$.

(d) Is het redelijk om te verwachten dat de optelling op een rekenmachine een associatieve bewerking is?

1.31 Zij G een groep, en a, b elementen van G die voldoen aan

$$aba^{-1} = b^2, \quad bab^{-1} = a^2.$$

Bewijs $a = b = e$.

1.32 Kies een alfabet met n letters $X = \{x_1, \ldots, x_n\}$. Een woord is een uitdrukking

$$a_1^{m_1} \ldots a_k^{m_k}$$

waarbij $k \in \mathbb{N}$, $a_i \in X$ en $m_i \in \mathbb{Z}$. We zeggen dat een woord gereduceerd is als $a_i \neq a_{i+1}$ en alle $m_i \neq 0$ Een niet gereduceerd woord kan men reduceren door $a_i^{m_i} a_{i+1}^{m_{i+1}}$ te vervangen door $a_i^{m_i+m_{i+1}}$ als $a_i = a_{i+1}$ en alle $a_i^{m_i}$ te schrappen waarvoor $m_i = 0$. De verzameling van alle gereduceerde woorden, inclusief het lege woord, duiden we aan met F_n of $F(X)$. Op deze verzameling definiëren we een product door twee woorden aan elkaar te plakken en dan te reduceren.

$$a_1^{m_1} \ldots a_k^{m_k} \star b_1^{n_1} \ldots b_l^{n_l} := \text{Reduceer}(a_1^{m_1} \ldots a_k^{m_k} b_1^{n_1} \ldots b_l^{n_l})$$

Toon aan dat $F_n, \star$ een groep is met het lege woord als eenheidselement. Deze groep wordt de *vrije groep met n letters genoemd*.

1.33 De *octonionen* of *octaven* van Cayley (1845; Arthur Cayley, Engels wiskundige en jurist, 1821–1895) zijn uitdrukkingen van de vorm

$$\alpha + \beta\ell$$

met $\alpha, \beta \in \mathbb{H}$. Octaven worden opgeteld en vermenigvuldigd door middel van de regeltjes

$$(\alpha + \beta\ell) + (\gamma + \delta\ell) = (\alpha + \gamma) + (\beta + \delta)\ell,$$
$$(\alpha + \beta\ell) \cdot (\gamma + \delta\ell) = (\alpha\gamma - \overline{\delta}\beta) + (\delta\alpha + \beta\overline{\gamma})\ell$$

voor $\alpha, \beta, \gamma, \delta \in \mathbb{H}$, waarbij $\bar{\ }$ is als in Opgave 1.2. Verder definiëren we

$$\overline{\alpha + \beta\ell} = \overline{\alpha} - \beta\ell \qquad (\alpha, \beta \in \mathbb{H}),$$
$$N(x) = x\overline{x}.$$

(a) Bewijs dat de octonionen met de bewerking + een abelse groep vormen.

(b) Bewijs dat de octonionen ongelijk aan nul met de bewerking $\cdot$ voldoen aan (G2) en (G3), maar niet aan (G1), (G4).

(c) Bewijs dat voor elk tweetal octonionen x, y geldt:

$$\begin{aligned} \overline{x+y} &= \overline{x} + \overline{y}, \quad \overline{xy} = \overline{y} \cdot \overline{x}, \\ N(xy) &= N(x) \cdot N(y), \\ (x \cdot x) \cdot y = x \cdot (x \cdot y), &\quad (x \cdot y) \cdot x = x \cdot (y \cdot x), \quad (y \cdot x) \cdot x = y \cdot (x \cdot x). \end{aligned}$$

(d) Bewijs: als a, b octonionen ongelijk aan nul zijn, dan zijn er eenduidig bepaalde octonionen x, y waarvoor geldt:

$$a \cdot x = b, \qquad y \cdot a = b.$$

Literatuur hierover: N. Bourbaki, Algèbre, Ch. III, appendice.

Hoofdstuk 2

Ondergroepen, homomorfismen, directe producten

Definitie 2.1. Laat H een deelverzameling van een groep G zijn. Dan heet H een *ondergroep* van G als aan de volgende drie voorwaarden voldaan is:

(H0) H is niet leeg;

(H1) voor alle $a, b \in H$ geldt $ab \in H$;

(H2) voor alle $a \in H$ geldt $a^{-1} \in H$.

Voorbeelden 2.2. De groep $\mathbb{Q}^+$ is een ondergroep van $\mathbb{R}^+$. De quaterniongroep Q is een ondergroep van de multiplicatieve groep $\mathbb{H}^*$ (zie 1.13). De verzameling $2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\} = \{\text{even gehele getallen}\}$ is een ondergroep van $\mathbb{Z}^+$. De verzameling $\mathbb{R}_{>0}$ is niet een ondergroep van de additieve groep $\mathbb{R}^+$ (aan (H2), additief geschreven, is niet voldaan), maar wel van de multiplicatieve groep $\mathbb{R}^*$.

In de rij

$$D_n \subset \mathrm{O}_2(\mathbb{R}) \subset \mathrm{E}(\mathbb{R}^2) \subset S(\mathbb{R}^2)$$

(zie 1.20 en 1.21; $S(\mathbb{R}^2)$ is de groep van alle permutaties van de verzameling $\mathbb{R}^2$) is elke groep een ondergroep van de volgende.

Stelling 2.3. *Laat H een ondergroep van een groep G zijn. Dan is H, met de op G gedefinieerde werking, zelf een groep.*

Bewijs. Neem aan dat (H0), (H1), (H2) gelden. Voorwaarde (H1) drukt uit dat H gesloten is onder de bewerking op G; deze bewerking beperkt derhalve tot een bewerking op H. We bewijzen nu dat H met deze bewerking voldoet aan de groepsaxioma's (G1), (G2) en (G3).

(G1) De associatieve wet $a(bc) = (ab)c$ geldt voor alle $a, b, c \in G$, dus zeker voor alle $a, b, c \in H$.

(G2) Wegens (H0) bestaat er een $x \in H$. Wegens (H2) dan ook $x^{-1} \in H$, en (H1) levert nu $e = xx^{-1} \in H$. Dus $e \in H$, en $ea = ae = a$ voor alle $a \in H$ (zelfs voor alle $a \in G$).

(G3) Dit volgt direct uit (H2).

Hiermee is 2.3 bewezen. De omkering van 2.3 is ook waar, zie Opgave 2.1. □

De volgende stelling laat zien dat voorwaarden (H1) en (H2) gecombineerd kunnen worden:

Stelling 2.4. *Laat H een deelverzameling van een groep G zijn. Dan is H een ondergroep van G dan en slechts dan als aan* (H0) *en* (H1') *voldaan is:*

(H0) *H is niet leeg;*

(H1') *voor alle $a, b \in H$ geldt $ab^{-1} \in H$.*

Bewijs. Het is duidelijk dat (H1') uit (H1) en (H2) volgt. Omgekeerd, neem (H1') aan; we bewijzen (H1) en (H2).

(H2): Laat $a \in H$. Dan $e = aa^{-1} \in H$ wegens (H1') (met $b = a$) en $a^{-1} = ea^{-1} \in H$, opnieuw wegens (H1') (toegepast op e en a). Dit bewijst (H2).

(H1): Laat $a, b \in H$. Dan $b^{-1} \in H$, dus $ab = a(b^{-1})^{-1} \in H$ wegens (H1') (toegepast op a en b^{-1}). Dit bewijst (H1).

Hiermee is 2.4 bewezen. □

Elke groep G heeft *triviale ondergroepen*: G zelf, en $\{e\}$.

Stelling 2.5. *Laat $(H_i)_{i\in I}$ een collectie ondergroepen van een groep G zijn. Dan is de doorsnede $\cap_{i\in I} H_i$ ook een ondergroep van G. In het bijzonder is $H_1 \cap H_2$ een ondergroep van G als H_1 en H_2 ondergroepen van G zijn.*

Bewijs. We controleren (H0), (H1') voor $H = \cap_{i\in I} H_i$.

(H0): Voor elke $i \in I$ geldt $e \in H_i$, omdat H_i een ondergroep is (zie het bewijs van 2.3). Dus $e \in \cap_{i\in I} H_i = H$, en $H \neq \emptyset$.

(H1'): Laat $a, b \in H$. Dan $a, b \in H_i$, voor alle $i \in I$, en omdat H_i een ondergroep is, volgt hieruit $ab^{-1} \in H_i$, voor alle $i \in I$. Dus $ab^{-1} \in \cap_{i\in I} H_i = H$.

Hiermee is 2.5 bewezen. □

In de volgende stelling bepalen we alle ondergroepen van $\mathbb{Z}$ en van $\mathbb{Z}/n\mathbb{Z}$.

Stelling 2.6. (a) *Elke ondergroep van $\mathbb{Z}$ is van de vorm*

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$$

voor een $n \in \mathbb{Z}_{\geq 0}$. Omgekeerd is voor elke $n \in \mathbb{Z}$ de verzameling $n\mathbb{Z}$ een ondergroep van $\mathbb{Z}$.

(b) *Laat $n \in \mathbb{Z}_{>0}$. Dan is elke ondergroep van $\mathbb{Z}/n\mathbb{Z}$ van de vorm*

$$\{\overline{d}, \overline{2d}, \ldots, \overline{n-d}, \overline{n}\},$$

waarbij d een deler van n is.

Bewijs. (a) Laat $H \subset \mathbb{Z}$ een ondergroep zijn. Als $H = \{0\}$ dan geldt $H = n\mathbb{Z}$ met $n = 0$. Veronderstel $H \neq \{0\}$. Dan bevat H een positief element, want als $a \in H$, dan ook $-a \in H$, wegens (H2) (additief!). Laat n het kleinste positieve element van H zijn. We beweren dat geldt: $n\mathbb{Z} = H$.

Bewijs van $\subset$: uit $n \in H$ volgt $2n = n + n \in H$, wegens (H1), $3n = 2n + n \in H$, en met volledige inductie naar x vinden we $xn \in H$ voor alle $x \in \mathbb{Z}_{>0}$. Dan hebben we ook $(-x) \cdot n = -xn \in H$, voor $x > 0$, en $0 \cdot n = 0 \in H$. Dus inderdaad $n\mathbb{Z} \subset H$.

Bewijs van $\supset$: Laat $a \in H$. Met behulp van Stelling 0.1 schrijven we $a = qn + r$, met $q \in \mathbb{Z}$, $r \in \{0, 1, 2, \ldots, n-1\}$. Dan geldt $r = a - qn$, met $a \in H$ en $qn \in n\mathbb{Z} \subset H$, dus wegens (H1') geldt $r \in H$. Als $r \neq 0$, dan zou r een positief element van H kleiner dan n zijn, in tegenspraak met de keuze van n. Dus we hebben $r = 0$, en $a = qn \in n\mathbb{Z}$, zoals verlangd.

Hiermee hebben we de eerste bewering van 2.6(a) bewezen. Het eenvoudige bewijs dat $n\mathbb{Z}$ een ondergroep van $\mathbb{Z}$ is, voor elke $n \in \mathbb{Z}$, laten we aan de lezer over.

(b) Laat $H \subset \mathbb{Z}/n\mathbb{Z}$ een ondergroep zijn. Definieer $K \subset \mathbb{Z}$ door

$$K = \big\{ a \in \mathbb{Z} \;\big|\; \overline{a} \in H \big\}.$$

Met behulp van Stelling 2.4 controleren we dat K een ondergroep van $\mathbb{Z}$ is:

(H0): uit $\overline{n} = \overline{0} \in H$ volgt $n \in K$ (en $0 \in K$), dus $K \neq \emptyset$.

(H1'): als $a, b \in K$, dan $\overline{a}, \overline{b} \in H$, dus $\overline{a} - \overline{b} \in H$, en omdat de groepswerking in $\mathbb{Z}/n\mathbb{Z}$ zó is gedefinieerd dat geldt $\overline{a} - \overline{b} = \overline{a - b}$, volgt hieruit dat $a - b \in K$.

We concluderen dat K een ondergroep van $\mathbb{Z}$ is. Uit (a) vinden we dus dat $K = d\mathbb{Z}$ voor zekere $d \in \mathbb{Z}_{\geq 0}$:

$$K = \{\ldots, -3d, -2d, -d, 0, d, 2d, 3d, \ldots\}.$$

Er geldt $n \in K = d\mathbb{Z}$, dus d is een deler van n. Verder

$$\begin{aligned} H &= \big\{ \overline{a} \;\big|\; a \in K \big\} \\ &= \big\{ \ldots, \overline{-3d}, \overline{-2d}, \overline{-d}, \overline{0}, \overline{d}, \overline{2d}, \overline{3d}, \ldots \big\} \\ &= \big\{ \overline{d}, \overline{2d}, \overline{3d}, \ldots, \overline{n} \big\}. \end{aligned}$$

Hiermee is 2.6 bewezen. □

Definitie 2.7. Laten G_1 en G_2 groepen zijn. Een afbeelding $f\colon G_1 \to G_2$ heet een *homomorfisme* of een *groepshomomorfisme* als geldt

$$f(ab) = f(a)f(b) \qquad \text{voor alle } a, b \in G_1. \tag{*}$$

De verzameling van alle homomorfismen van G_1 naar G_2 wordt aangegeven met $\mathrm{Hom}(G_1, G_2)$. Een *isomorfisme* is een bijectief homomorfisme. Als er een isomorfisme $G_1 \to G_2$ bestaat, heten G_1 en G_2 *isomorf*, notatie: $G_1 \cong G_2$. Laat vervolgens G een groep zijn. Een bijectief homorfisme van G naar zichzelf heet een *automorfisme*. De verzameling automorfismen van G wordt aangegeven met $\mathrm{Aut}(G)$.

Opmerking 2.8. In (*) vindt de vermenigvuldiging van a met b, in het linkerlid, plaats in de groep G_1, maar die van $f(a)$ met $f(b)$, in het rechterlid, in G_2. Hiermee moet men rekening houden als de groepsbewerkingen van G_1 en G_2 op een andere wijze genoteerd worden. Bijvoorbeeld, als $\circ$ de bewerking in G_1 is, en G_2 additief geschreven wordt, dan moet men (*) vervangen door

$$f(a \circ b) = f(a) + f(b) \text{ voor alle } a, b \in G_1.$$

Voorbeelden 2.9. (a) Neem $G_1 = G_2 = \mathbb{R}^*$ en $f(x) = x^2$. Dit is een homomorfisme van $\mathbb{R}^*$ naar zichzelf. Het is geen automorfisme van $\mathbb{R}^*$. Een voorbeeld van een automorfisme van $\mathbb{R}^*$ is de functie $g\colon \mathbb{R}^* \to \mathbb{R}^*$ gedefinieerd door $g(x) = x^3$.

(b) Zij $f\colon \mathbb{C} \to \mathbb{R}$ gedefineerd door $f(z) = \mathrm{Im}(z)$ (het imaginaire deel van z, zie 1.6). Uit $\mathrm{Im}(z_1+z_2) = \mathrm{Im}(z_1) + \mathrm{Im}(z_2)$ zien we dat dit een homomorfisme is. Het is geen isomorfisme.

(c) Beschouw de afbeelding $\log\colon \mathbb{R}_{>0} \to \mathbb{R}^+$ (met $\mathbb{R}_{>0}$ de *multiplicatieve* groep). Uit $\log(xy) = \log(x) + \log(y)$ zien we dat log een groepshomomorfisme is. Het is zelfs een isomorfisme; de inverse afbeelding wordt gegeven door $x \mapsto e^x$.

(d) Zij $f\colon \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^*$ de afbeelding gegeven door $f(A) = \det(A)$ (zie 1.11). De regel $\det(AB) = \det(A)\det(B)$ drukt precies uit dat f een homomorfisme is. Analoog voor $\mathrm{GL}(n,\mathbb{R})$, met n een willekeurig positief geheel getal.

(e) De afbeelding $f\colon Q \to V_4$ (zie 1.12 en 1.13) gedefinieerd door

$$f(\pm 1) = e\,, \qquad f(\pm i) = a\,, \qquad f(\pm j) = b\,, \qquad f(\pm k) = c$$

is een homomorfisme.

(f) Laat G een groep zijn, en $a \in G$ een vast gekozen element. Definieer $f\colon \mathbb{Z} \to G$ door $f(n) = a^n$. Uit het regeltje $a^{n+m} = a^n \cdot a^m$ (zie 1.24) zien we dat f een homomorfisme is.

(g) Is $H \subset G$ een ondergroep, dan is de afbeelding $f\colon H \to G$ gegeven door $f(x) = x$ een homomorfisme. (We noemen deze afbeelding ook wel de *inclusie-afbeelding.*)

(h) Als $\sigma \in S_n$ een permutatie is dan definiëren we de permutatiematrix $P(\sigma)$ als de $n \times n$-matrix

$$P(\sigma)_{ij} = \begin{cases} 1 & j = \sigma(i) \\ 0 & j \neq \sigma(i) \end{cases}$$

M.a.w. $P(\sigma)$ permuteert de kolommen van de eenheidsmatrix volgens de permutatie σ. De afbeelding $P : S_n \to \mathrm{GL}_n(n,\mathbb{R}) : \sigma \mapsto P(\sigma)$ is een injectief groepsmorfisme.

In 2.10 t/m 2.15 nemen we aan dat G_1, G_2 groepen zijn, en $f\colon G_1 \to G_2$ een groepshomomorfisme. Met e_1 geven we het eenheidselement van G_1 aan, met e_2 dat van G_2.

Stelling 2.10. *Er geldt*

(a) $f(e_1) = e_2$*;*

(b) $f(a^{-1}) = f(a)^{-1}$ *voor alle* $a \in G_1$*.*

Bewijs. (a) Er geldt $f(e_1)f(e_1) = f(e_1e_1) = f(e_1)$, en ook $f(e_1)e_2 = f(e_1)$. Omdat $f(e_1)x = f(e_1)$ maar één oplossing x in G_2 heeft (Stelling 1.23) volgt hieruit $f(e_1) = e_2$.

(b) Er geldt $f(a)f(a^{-1}) = f(aa^{-1}) = f(e_1) = e_2$, dus $f(a^{-1)} = f(a)^{-1}$. Dit bewijst 2.10. □

Opmerking 2.11. Als G_1 additief, en G_2 multiplicatief genoteerd wordt, ziet 2.10(b) er zó uit: $f(-a) = f(a)^{-1}$, voor $a \in G_1$.

Definitie 2.12. De *kern* van $f\colon G_1 \to G_2$, notatie $\mathrm{Ker}(f)$, is gedefinieerd door

$$\mathrm{Ker}(f) = \big\{x \in G_1 \;\big|\; f(x) = e_2\big\}.$$

Stelling 2.13. *Zij $f\colon G_1 \to G_2$ een groepshomomorfisme. Dan is $\mathrm{Ker}(f)$ is een ondergroep van G_1.*

Bewijs. We controleren (H0) en (H1') voor $\mathrm{Ker}(f)$ (zie Stelling 2.4).

(H0): Er geldt $f(e_1) = e_2$ wegens 2.10(a), dus $e_1 \in \mathrm{Ker}(f)$, dus $\mathrm{Ker}(f) \neq \emptyset$.

(H1'): Als $a, b \in \mathrm{Ker}(f)$, dan $f(a) = f(b) = e_2$, en daarom $f(ab^{-1}) = f(a)f(b)^{-1} = e_2 e_2^{-1} = e_2$, dus $ab^{-1} \in \mathrm{Ker}(f)$. Dit bewijst 2.13. □

Aan de kern van f kunnen we direct zien of f injectief is:

Stelling 2.14. *Het homomorfisme $f\colon G_1 \to G_2$ is injectief dan en slechts dan als $\mathrm{Ker}(f) = \{e_1\}$.*

Bewijs. Stel f is injectief, en $x \in \mathrm{Ker}(f)$. Dan $f(x) = e_2 = f(e_1)$, dus de injectiviteit levert $x = e_1$. Hieruit volgt $\mathrm{Ker}(f) = \{e_1\}$.

Omgekeerd, stel $\mathrm{Ker}(f) = \{e_1\}$, en $f(x) = f(y)$. Dan $f(xy^{-1}) = f(x)f(y)^{-1} = e_2$, dus $xy^{-1} \in \mathrm{Ker}(f) = \{e_1\}$. We concluderen dat $xy^{-1} = e_1$, d.w.z. $x = y$. Hieruit volgt dat f injectief is. Dit bewijst 2.14. □

Het *beeld* van f, genoteerd $f[G_1]$ of $f(G_1)$ of $\mathrm{Im}(f)$, is gedefinieerd als in de verzamelingenleer:

$$f[G_1] = \big\{f(x) \;\big|\; x \in G_1\big\} \subset G_2.$$

Stelling 2.15. *Zij $f\colon G_1 \to G_2$ een groepshomomorfisme. Dan is het beeld $f[G_1]$ een ondergroep van G_2.*

Bewijs. We gaan na dat (H0) en (H1') gelden voor het beeld.

(H0): Er geldt $e_2 = f(e_1) \in f[G_1]$, dus $f[G_1] \neq \emptyset$.

(H1'): Als $a, b \in f[G_1]$, dan zijn er $x, y \in G_1$ met $f(x) = a$, $f(y) = b$. Dan $f(xy^{-1}) = f(x)f(y)^{-1} = ab^{-1}$, dus $ab^{-1} \in f[G_1]$. Dit bewijst 2.15. □

Opmerking 2.16. Zoals we aan Voorbeeld 2.9(g) zien is elke ondergroep H van een groep G het beeld van een geschikt gekozen homomorfisme. De overeenkomstige uitspraak voor kernen is niet waar: niet elke ondergroep is de kern van een homomorfisme; voor een nodige en voldoende voorwaarde, zie 4.12.

Stelling 2.17. *Laten $f\colon G_1 \to G_2$ en $g\colon G_2 \to G_3$ groepshomomorfismen zijn. Dan is $g \circ f\colon G_1 \to G_3$ een groepshomomorfisme. Zijn f en g beide isomorfismen, dan is $g \circ f$ ook een isomorfisme.*

Bewijs. Voor $a, b \in G_1$ geldt

$$\begin{aligned}(g \circ f)(ab) &= g(f(ab)) = g(f(a)f(b)) \\ &= g(f(a))g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b),\end{aligned}$$

dus $g \circ f$ is een homomorfisme. Zijn f en g allebei bijectief, dan is $g \circ f$ dit ook. Dit bewijst 2.17. □

Voorbeeld 2.18. In 2.9 hebben we twee groepsmorfismen gezien: $P : S_n \to \mathrm{GL}(n,\mathbb{R})$ en det : $\mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}^*$. De samenstelling van die twee morfismen $\varepsilon := \det \circ P$ noemen we de tekenafbeelding en $\varepsilon(\tau)$ het teken van τ.

Stelling 2.19. (a) *Is σ een verwisseling, dan $\varepsilon(\sigma) = -1$.*

(b) *Is σ een cykel van lengte k, dan $\varepsilon(\sigma) = (-1)^{k-1}$.*

(c) *Is σ het product van ℓ cykels van lengtes $k_1, k_2, \ldots, k_\ell$, dan $\varepsilon(\sigma) = (-1)^{k_1+k_2+\cdots+k_\ell-\ell}$*

(d) *Elke $\sigma \in S_n$ kan geschreven worden als product van een aantal verwisselingen; is σ even, dan is dit aantal even, en is σ oneven, dan is dit aantal oneven.*

Bewijs. De determinant wisselt van teken als je twee kolommen omwisselt. Omdat $P(i\ j)$ de eenheidsmatrix is met de kolommen i en j omgewisseld is $\varepsilon(i\ j) = -1$. Daarnaast is

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)\,(a_2\ a_3)\,\cdots\,(a_{k-2}\ a_{k-1})\,(a_{k-1}\ a_k)\,. \tag{2.19.1}$$

dus

$$\varepsilon\big((a_1\ a_2\ \ldots\ a_k)\big) = \varepsilon(a_1\ a_2)\cdot\varepsilon(a_2\ a_3)\cdots\varepsilon(a_{k-2}\ a_{k-1})\cdot\varepsilon(a_{k-1}\ a_k) = (-1)^{k-1}$$

Ook (c) en (d) volgen direct uit het feit dat ε een groepsmorfisme is. □

Het beeld van ε is dus $\{1,-1\}$. Als $\varepsilon(\sigma) = 1$ noemen we σ *even*, als $\varepsilon(\sigma) = -1$ *oneven*. We zeggen ook wel dat de *pariteit* van σ even of oneven is.

Definitie 2.20. De *alternerende groep* A_n is de verzameling even permutaties in S_n.

Opmerking 2.21. Per definitie is $A_n = \mathrm{Ker}(\varepsilon)$, dus A_n is inderdaad een ondergroep van S_n (Stelling 2.13). Laat $n \geq 2$, en $\sigma = (1\ 2)$. Dan bestaat $\sigma A_n = \{\sigma\tau \mid \tau \in A_n\}$ geheel uit oneven permutaties, en elke oneven permutatie υ komt ook in σA_n voor, want we kunnen schrijven $\upsilon = \sigma\cdot(\sigma^{-1}\upsilon)$ met $\sigma^{-1}\upsilon \in A_n$. Dus we zien dat er evenveel oneven permutaties als even permutaties zijn. Hieruit volgt: $\#A_n = \frac{n!}{2}$.

Stelling 2.22. *Laat $f\colon G_1 \to G_2$ een isomorfisme van groepen zijn. Dan is $f^{-1}\colon G_2 \to G_1$ ook een isomorfisme.*

Bewijs. Merk op dat f^{-1} bestaat, omdat f bijectief is. Laat $a, b \in G_2$. Dan geldt:

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

Omdat f injectief is volgt hieruit

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

Dus f^{-1} is een homomorfisme. Bovendien is f^{-1} bijectief, want het is de inverse van een bijectieve afbeelding. Hiermee is 2.5 bewezen. □

Uit 2.17 en 2.22 zien we:

- als $G_1 \cong G_2$ en $G_2 \cong G_3$, dan is $G_1 \cong G_3$,
- als $G_1 \cong G_2$ dan is $G_2 \cong G_1$,

terwijl natuurlijk ook geldt

- $G_1 \cong G_1$.

Dus $\cong$ is een equivalentierelatie op de klasse van alle groepen. Men kan isomorfe groepen in groepentheoretisch opzicht als 'dezelfde' beschouwen; het enige eventuele verschil bestaat in de schrijfwijze die men voor de elementen en de bewerking van de groep hanteert (vergelijk 1.10).

Voorbeelden 2.23. We geven hier enkele voorbeelden van isomorfismen. Zie ook 2.9(c).

(a) De groepentabel van $(\mathbb{Z}/8\mathbb{Z})^*$ is

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

Afgezien van de keuze der symbolen is dit dezelfde tabel als voor V_4 (zie 1.12). Dus er is een isomorfisme $f\colon V_4 \to (\mathbb{Z}/8\mathbb{Z})^*$, gegeven door $f(e) = \overline{1}$, $f(a) = \overline{3}$, $f(b) = \overline{5}$, $f(c) = \overline{7}$.

(b) Een isomorfisme $f\colon \mathbb{R}^2 \to \mathbb{C}$ wordt gegeven door $f((a,b)) = a + bi$. Evenzo is de afbeelding $f\colon \mathbb{R}^4 \to \mathbb{H}$ gegeven door $f((a_1,a_2,a_3,a_4)) = a_1 + a_2 i + a_3 j + a_4 k$ een isomorfisme.

(c) De afbeelding $f\colon \mathbb{Z}/4\mathbb{Z} \to \{1, i, -1, -i\}$ (vgl. het eind van 1.12), $f(a \mod 4) = i^a$, is een isomorfisme.

(d) De groep D_3 is gedefinieerd als de groep van alle congruenties van het platte vlak die een gegeven gelijkzijdige driehoek in zichzelf overvoeren (zie 1.16). Iedere dergelijke congruentie permuteert de drie hoekpunten van de driehoek. Nummeren we de hoekpunten $1, 2, 3$ en geven we met S_3 de verzameling permutaties van $\{1, 2, 3\}$ aan (zie 1.16), dan krijgen we een afbeelding $f\colon D_3 \to S_3$, die aan elke congruentie in D_3 de bijbehorende permutatie van de hoekpunten toevoegt. Men ziet direct in dat f een groepshomomorfisme is. Omdat een element van D_3 volledig vastligt door de wijze waarop het de hoekpunten permuteert, is f injectief. Maar D_3 en S_3 hebben allebei zes elementen (zie 1.17 voor S_3), dus f moet ook surjectief zijn. We concluderen dat f een isomorfisme is, en dat D_3 en S_3 isomorf zijn.

(e) Laat G een groep zijn, en $g \in G$ een vast gekozen element. Definieer

$$f\colon G \to G$$

door

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

Uit

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

zien we dat f een homomorfisme van G naar zichzelf is. Bovendien is f bijectief, want de afbeelding

$$h\colon G \to G, \qquad h(x) = g^{-1}xg,$$

is een tweezijdige inverse van f, d.w.z. $f \circ h = h \circ f = \mathrm{id}_G$. We concluderen dat f een automorfisme van G is. Een zo geconstrueerd automorfisme van G heet *inwendig*; voor meer informatie zie Hoofdstuk 7.

Definitie 2.24. Als G_1 en G_2 groepen zijn, dan is het *directe product* van G_1 en G_2 de verzameling

$$G_1 \times G_2 = \big\{(g_1, g_2) \;\big|\; g_1 \in G_1, g_2 \in G_2\big\}$$

met de bewerking

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1h_1, g_2h_2) \qquad (g_1, h_1 \in G_1, g_2, h_2 \in G_2)$$

('componentsgewijs vermenigvuldigen'). Notatie: $G_1 \times G_2$. Als G_1 en G_2 abels zijn schrijven we in plaats van $G_1 \times G_2$ ook wel $G_1 \oplus G_2$, en spreken dan van de *directe som* van G_1 en G_2.

Stelling 2.25. *Het directe product $G_1 \times G_2$ van twee groepen G_1 en G_2 is, met de boven gedefinieerde bewerking, een groep.*

Bewijs. Dit is eenvoudig na te gaan aan de hand van de groepsaxioma's. Het eenheidselement van $G_1 \times G_2$ is (e_1, e_2), waar e_1 het eenheidselement van G_1 aangeeft en e_2 dat van G_2, en er geldt $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$, voor $g_1 \in G_1, g_2 \in G_2$. Dit bewijst 2.25. □

Voorbeelden 2.26. (a) Het platte vlak $\mathbb{R}^2$ (additief) is het directe product van $\mathbb{R}^+$ en $\mathbb{R}^+$.

(b) De groep $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is isomorf met de viergroep van Klein V_4 (zie 1.12), door

$$(\overline{0}, \overline{0}) \mapsto e\,, \qquad (\overline{1}, \overline{0}) \mapsto a\,, \qquad (\overline{0}, \overline{1}) \mapsto b\,, \qquad (\overline{1}, \overline{1}) \mapsto c\,.$$

$+$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$

Het nemen van directe producten is commutatief in de zin dat

$$G_1 \times G_2 \cong G_2 \times G_1,$$

met een isomorfisme gegeven door

$$(g_1, g_2) \mapsto (g_2, g_1)$$

en associatief in de zin dat

$$(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3),$$

met een isomorfisme gegeven door

$$((g_1, g_2), g_3) \mapsto (g_1, (g_2, g_3)) \qquad (g_i \in G_i),$$

voor willekeurige groepen G_1, G_2 en G_3. Bij herhaalde producten $G_1 \times G_2 \times \ldots \times G_n$ zullen we dan ook geen haakjes schrijven.

Als $G = G_1 \times G_2$, dan is $H_1 = G_1 \times \{e_2\} = \big\{(g_1, e_2) \;\big|\; g_1 \in G_1\big\}$ een ondergroep van G die isomorf is met G_1, met een isomorfisme gegeven door $(g_1, e_2) \mapsto g_1$. Op dezelfde wijze ziet men dat $H_2 = \{e_1\} \times G_2$ een ondergroep van G is die isomorf is met G_2. Men gaat eenvoudig na dat de ondergroepen H_1 en H_2 van G de volgende drie eigenschappen hebben:

(a) $h_1 h_2 = h_2 h_1$ voor alle $h_1 \in H_1$ en $h_2 \in H_2$;

(b) $H_1 \cap H_2 = \{e\}$;

(c) elk element $g \in G$ is te schrijven als $g = h_1 h_2$, met $h_1 \in H_1$ en $h_2 \in H_2$.

De volgende stelling zegt dat deze drie eigenschappen omgekeerd ook impliceren dat men G als direct product van H_1 en H_2 kan opvatten:

Stelling 2.27. *Laat G een groep zijn, en $H_1, H_2 \subset G$ ondergroepen die aan de voorwaarden* (a)*,* (b) *en* (c) *voldoen. Dan geldt $G \cong H_1 \times H_2$.*

Bewijs. Definieer $f\colon H_1 \times H_2 \to G$ door $f((h_1, h_2)) = h_1 h_2$.

(i) *f is een groepshomomorfisme*: immers, voor $h_1, h_1' \in H$ en $h_2, h_2' \in H_2$ geldt

$$\begin{aligned} f((h_1, h_2) \cdot (h_1', h_2')) &= f((h_1 h_1', h_2 h_2')) \\ &= h_1 h_1' h_2 h_2' \\ &= h_1 h_2 h_1' h_2' \qquad \text{(hier gebruiken we (a): } h_1' h_2 = h_2 h_1') \\ &= f((h_1, h_2)) \cdot f((h_1', h_2')). \end{aligned}$$

(ii) *f is injectief*: als $(h_1, h_2) \in \mathrm{Ker}(f)$ dan $h_1 h_2 = e$ dus $h_1 = h_2^{-1}$. Dan geldt $h_1 \in H_1 \cap H_2$ dus $h_1 = e$ wegens (b), en $h_2 = h_1^{-1} = e$. Dus $\mathrm{Ker}(f)$ bestaat alleen uit het eenheidselement (e, e) van $H_1 \times H_2$. Volgens 2.14 is f nu injectief.

(iii) *f is surjectief*: dit is precies voorwaarde (c).

Uit (i), (ii) en (iii) blijkt dat f een bijectief homomorfisme, dus een isomorfisme, van $H_1 \times H_2$ naar G is. Dit bewijst 2.27. □

Voorbeelden 2.28. Neem $G = \mathbb{R}^*$, $H_1 = \{\pm 1\}$, $H_2 = \mathbb{R}_{>0}$. Aan (a), (b), (c) is voldaan, dus $\mathbb{R}^* \cong \{\pm 1\} \times \mathbb{R}_{>0}$. Bovendien $\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$, door $\overline{0} \mapsto 1$ en $\overline{1} \mapsto -1$, en $\mathbb{R}_{>0} \cong \mathbb{R}^+$ door $x \mapsto \log x$ (zie 2.9(c)). We concluderen dat $\mathbb{R}^* \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{R}^+$.

Stelling 2.29 (Chinese reststelling, moderne versie)**.** *Laten n en m twee onderling ondeelbare positieve gehele getallen zijn. Dan is er een groepsisomorfisme*

$$\mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

Bewijs. In dit bewijs gebruiken we de notaties

$$\overline{a} = (a \mod nm), \qquad \tilde{a} = (a \mod n), \qquad \hat{a} = (a \mod m).$$

Definieer $f\colon \mathbb{Z}/nm\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ door

$$f(\overline{a}) = (\tilde{a}, \hat{a}).$$

Dit is een goede definitie: als $\overline{a} = \overline{a'}$, dan $nm \mid a - a'$, dus zeker $n \mid a - a'$, dus $\tilde{a} = \widetilde{a'}$; en evenzo $\hat{a} = \widehat{a'}$.

Voorbeeld van f: neem $n = 3$ en $m = 5$.

	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$
$\tilde{0}$	$\overline{0}$	$\overline{6}$	$\overline{12}$	$\overline{3}$	$\overline{9}$
$\tilde{1}$	$\overline{10}$	$\overline{1}$	$\overline{7}$	$\overline{13}$	$\overline{4}$
$\tilde{2}$	$\overline{5}$	$\overline{11}$	$\overline{2}$	$\overline{8}$	$\overline{14}$

waarbij

$$\begin{array}{ccc} & & \hat{i} \\ & & | \\ \tilde{j} & - & \overline{k} \end{array}$$

aangeeft dat $f(\overline{k}) = \left(\hat{i}, \tilde{j}\right)$, dus: $k \equiv i \bmod 3$ en $k \equiv j \bmod 5$.

We gaan bewijzen dat f een isomorfisme is.

(a) f is een homomorfisme:

$$\begin{aligned} f(\overline{a} + \overline{b}) = f(\overline{a+b}) &= (\widetilde{a+b}, \widehat{a+b}) = (\tilde{a} + \tilde{b}, \hat{a} + \hat{b}) \\ &= (\tilde{a}, \hat{a}) + (\tilde{b}, \hat{b}) = f(\overline{a}) + f(\overline{b}). \end{aligned}$$

Hier hebben we $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ additief geschreven.

(b) f is injectief. Als $\overline{a} \in \mathrm{Ker}(f)$ dan $(\tilde{a}, \hat{a}) = (\tilde{0}, \hat{0})$, dus $n \mid a$ en $m \mid a$, en hieruit volgt $\mathrm{kgv}(n, m) \mid a$. Omdat n en m onderling ondeelbaar zijn, geldt $\mathrm{kgv}(n, m) = nm$. Dus $nm \mid a$, en $\overline{a} = \overline{0}$. We hebben hiermee bewezen dat $\mathrm{Ker}(f) = \{\overline{0}\}$. Wegens 2.14 is f nu injectief.

(c) f is surjectief. Omdat f injectief is, bestaat het beeld van f:

$$f[\mathbb{Z}/nm\mathbb{Z}] = \{f(\overline{0}), f(\overline{1}), \ldots, f(\overline{nm-1})\}$$

uit nm *verschillende* elementen. Maar $f[\mathbb{Z}/nm\mathbb{Z}]$ is een deelverzameling van de verzameling $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, die zelf ook nm elementen heeft. Er blijft dus geen mogelijkheid over dan $f[\mathbb{Z}/nm\mathbb{Z}] = (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, m.a.w. f is surjectief.

Uit (a), (b), (c) volgt dat f een isomorfisme is. Hiermee is 2.29 bewezen. □

De bijectiviteit van de functie f kan ook als volgt geformuleerd worden:

Stelling 2.30 (Chinese reststelling, antieke versie)**.** *Laten n en m onderling ondeelbare positieve gehele getallen zijn, en $b, c \in \mathbb{Z}$. Dan bestaat er een $a \in \mathbb{Z}$ met*

$$a \equiv b \mod n,$$

$$a \equiv c \mod m.$$

Bovendien is a eenduidig bepaald modulo nm.

Bewijs. Met de notaties uit het bewijs van 2.29, zegt deze stelling dat er voor elke $(\tilde{b}, \hat{c}) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ precies één $\overline{a} \in \mathbb{Z}/nm\mathbb{Z}$ is met $f(\overline{a}) = (\tilde{b}, \hat{c})$. Met andere woorden: f is bijectief, en dat hebben we boven bewezen. Dit bewijst 2.30. □

De Stellingen 2.29 en 2.30 kunnen voor meer dan twee getallen gegeneraliseerd worden:

Stelling 2.31. *Laten $n_1, n_2, \ldots, n_t$ positieve gehele getallen zijn, zo dat voor alle indices $i \neq j$ geldt dat* $\gcd(n_i, n_j) = 1$. *Laat $N = \prod_{i=1}^{t} n_i$. Dan geldt:*

$$\mathbb{Z}/N\mathbb{Z} \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_t\mathbb{Z}).$$

Bovendien bestaat er voor elk stelsel van t gehele getallen $a_1, a_2, \ldots, a_t$ een geheel getal a waarvoor

$$\begin{aligned} a &\equiv a_1 \mod n_1 \\ a &\equiv a_2 \mod n_2 \\ &\vdots \\ a &\equiv a_t \mod n_t \end{aligned}$$

en deze a is eenduidig bepaald modulo $N = \prod_{i=1}^{t} n_i$.

Bewijs. Dit laten we aan de lezer over. Men kan de argumenten in het bewijs van 2.29 generaliseren, maar men kan de stelling ook, door volledige inductie naar t toe te passen, terugvoeren tot het geval $t = 2$. Tot zover het bewijs van 2.31. □

Ook 2.31 staat bekend onder de naam 'Chinese reststelling', naar de Chinese wiskundige Sun-Tsŭ ($\approx$ 1e eeuw na Chr.) die er een speciaal geval van behandelde. Voor de geschiedenis van de stelling, zie L.E. Dickson, History of the theory of numbers, vol. II, pp. 57ff.

2.32 Er zijn verschillende methoden om, gegeven $n_1, n_2, \ldots, n_t$ en $a_1, a_2, \ldots, a_t$ als in 2.31, een geheel getal a te vinden dat voldoet aan $a \equiv a_i \mod n_i$, voor $1 \leq i \leq t$.

De eerste methode geeft de eenvoudigste formule voor a. Eerst vindt men $x \in \mathbb{Z}$ met

$$xn_2n_3 \ldots n_t \equiv 1 \mod n_1.$$

Omdat $\text{ggd}(n_2n_3 \ldots n_t, n_1) = 1$ kan men een dergelijke x vinden met de methode aangegeven in 1.15 (eind). Het getal $b_1 = xn_2n_3 \ldots n_t$ voldoet nu aan

$$\begin{aligned} b_1 &\equiv 1 \mod n_1, \\ b_1 &\equiv 0 \mod n_j \qquad (2 \leq j \leq t). \end{aligned}$$

Op dezelfde wijze vindt men getallen $b_2, b_3, \ldots, b_t$ die voldoen aan

$$\begin{aligned} b_i &\equiv 1 \mod n_i, \\ b_i &\equiv 0 \mod n_j \qquad (1 \leq j \leq t, \quad j \neq i). \end{aligned}$$

Het getal

$$a = a_1b_1 + a_2b_2 + \ldots + a_tb_t$$

voldoet nu aan de verlangde congruenties.

De tweede methode werkt met kleinere getallen en is in vele omstandigheden beter bruikbaar. De methode werkt met volledige inductie naar t. Stel dat men, voor zekere $u < t$, een geheel getal a kent dat in elk geval voldoet aan de eerste u congruenties:

$$a \equiv a_1 \mod n_1, \qquad a \equiv a_2 \mod n_2, \ldots, \qquad a \equiv a_u \mod n_u.$$

Zo'n getal kent men bijvoorbeeld voor $u = 1$, nl. $a = a_1$. We geven een methode aan om a zodanig te wijzigen dat ook aan de volgende congruentie $a \equiv a_{u+1} \mod n_{u+1}$ wordt voldaan. Hiertoe bepaalt men, opnieuw met de methode van 1.15, een geheel getal x waarvoor geldt

$$xn_1n_2 \ldots n_u \equiv 1 \mod n_{u+1}.$$

Het getal

$$a' = a + (a_{u+1} - a)xn_1n_2 \ldots n_u \qquad (*)$$

voldoet nu aan de eerste $u+1$ congruenties $a' \equiv a_i \mod n_i \qquad (1 \leq i \leq u+1)$. Om met kleine getallen te blijven werken is het verstandig om vóór men (*) uitrekent, de factor $(a_{u+1} - a)x$ te vervangen door zijn rest bij deling door n_{u+1}. Men noemt a' nu weer a. Voert men deze stap $t-1$ keer uit, uitgaande van $a = a_1$, dan heeft men de verlangde a gevonden.

Voorbeelden 2.33. Laat $n_1 = 7, \quad n_2 = 11, \quad n_3 = 13, \quad a_1 = 1, \quad a_2 = 6, \quad a_3 = 3$. Eerste methode: met de algoritme van 1.15 vindt men

$$b_1 = -286, \quad b_2 = 364, \quad b_3 = -77.$$

Dat levert de oplossing

$$a = 1 \cdot -286 + 6 \cdot 364 + 3 \cdot -77 = 1667.$$

Om de kleinste niet-negatieve oplossing te vinden trekt men hier een zo groot mogelijk veelvoud van $\prod_{i=1}^{t} n_i = 7 \cdot 11 \cdot 13 = 1001$ van af. Dat levert

$$a = 1667 - 1 \cdot 1001 = 666.$$

Tweede methode. Eerst zet men $a = a_1 = 1, \quad u = 1$. Als oplossing van $x \cdot n_1 \equiv 1 \mod n_2$ vindt men $x = -3$. In formule (*) vervangen we nu eerste de factor $(a_{u+1} - a) \cdot x = (6 - 1) \cdot -3 = -15$ door zijn rest bij deling door $n_{u+1}(= 11)$, (deze rest is 7), en we vinden dan

$$a' = 1 + 7 \cdot 7 = 50.$$

Dit is onze nieuwe a. Dan zetten we $u = 2$, lossen $x \cdot 7 \cdot 11 \equiv 1 \mod 13$ op (uitkomst $x = -1$), vervangen $(a_{u+1} - a) \cdot x = 47$ door zijn rest (=8) bij deling door n_{u+1} (=13), en vinden tenslotte het antwoord uit (*):

$$50 + 8 \cdot 77 = 666.$$

Deze methode levert vanzelf de kleinste niet-negatieve oplossing.

Opgaven

2.1 Laat G een groep zijn, en $H \subset G$ een deelverzameling die met de bewerking op G een groep vormt. Bewijs dat H een ondergroep van G is.

2.2 Laat G een groep zijn, en $H \subset G$ een *eindige* deelverzameling die voldoet aan (H0) en (H1). Bewijs van H een ondergroep van G is. N.b.: zoals het voorbeeld $\mathbb{Z}_{\geq 0} \subset \mathbb{Z}^+$ laat zien, is de eindigheid van H essentieel!

2.3 (a) Bewijs: $S_3 = \big\{(1)\,,(1\ 2)\,,(2\ 3)\,,(1\ 3)\,,(1\ 2\ 3)\,,(1\ 3\ 2)\big\}$.

(b) Maak een groeptabel voor S_3.

(c) Bewijs dat S_3 precies zes ondergroepen heeft namelijk

$$\big\{(1)\big\}\,, \quad \big\{(1),(1\ 2)\big\}\,, \quad \big\{(1),(2\ 3)\big\}\,, \quad \big\{(1),(1\ 3)\big\}\,, \quad \big\{(1),(1\ 2\ 3),(1\ 3\ 2)\big\}\,, \quad S_3\,.$$

2.4 Welke van de volgende deelverzamelingen zijn ondergroepen?

$$\mathbb{Q}_{>0} \subset \mathbb{Q}^*$$
$$\mathbb{Q}_{>0} \subset \mathbb{C}^+$$
$$\mathbb{C}^* \subset \mathbb{H}^*$$
$$\left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{R}) \;\middle|\; ad - bc > 0 \right\} \subset \mathrm{GL}(2,\mathbb{R})$$
$$\{1, i, j, k\} \subset Q$$
$$\{1, i, -1, -i\} \subset \mathbb{C}^*$$
$$\left\{ x \in \mathbb{C}^* \;\middle|\; |x| = 1 \right\} \subset \mathbb{C}^*$$
$$\left\{ a + bi \in \mathbb{C}^* \;\middle|\; a^2 + b^2 \in \mathbb{Q} \right\} \subset \mathbb{C}^*$$
$$2\mathbb{Z}_{\geq 0} \subset \mathbb{Z}$$
$$D_d \subset D_n\,, \qquad \text{waarbij } d, n \in \mathbb{Z}_{>1} \text{ met } d \mid n$$
$$\left\{ x \in \mathbb{Q}^* \;\middle|\; \text{er bestaan } a, b \in \mathbb{Q} \text{ zo dat } x = a^2 + b^2 \right\} \subset \mathbb{Q}^*$$

2.5

(a) Bewijs: een ondergroep van een abelse groep is abels.

(b) Geef een voorbeeld van een niet-abelse groep met een abelse ondergroep.

2.6

(a) Laat G een groep zijn, en $H_1 \subset G$, $H_2 \subset G$ ondergroepen. Bewijs: als $G = H_1 \cup H_2$, dan $G = H_1$ of $G = H_2$.

(b) Bewijs dat V_4 drie ondergroepen H_1, H_2, H_3, allemaal verschillend van V_4, heeft, waarvoor geldt $V_4 = H_1 \cup H_2 \cup H_3$.

2.7

1. Laat X een verzameling zijn, en $Y \subset X$ een deelverzameling. Bewijs dat

$$\left\{ \sigma \in S(X) \;\middle|\; \sigma[Y] = Y \right\} \qquad \text{en} \qquad \left\{ \sigma \in S(X) \;\middle|\; \sigma(y) = y \text{ voor alle } y \in Y \right\}$$

   allebei ondergroepen van $S(X)$ zijn (zie 1.16 voor de definitie van $S(X)$).

2. Neem aan dat X eindig is. Bepaal het aantal elementen van bovenstaande ondergroepen van $S(X)$.

2.8 Laat $m, n \in \mathbb{Z}$, $n > 0$, en $d = \gcd(m, n)$. Bewijs dat

$$\left\{\overline{a} \;\middle|\; a \in m\mathbb{Z}\right\} \subset \mathbb{Z}/n\mathbb{Z}$$

(met $\overline{a} = a \mod n$) een ondergroep is, en dat deze ondergroep gelijk is aan

$$\left\{\overline{d}, \overline{2d}, \overline{3d}, \ldots, \overline{n}\right\}.$$

2.9 Geef volledige bewijzen van de in 2.9 gedane beweringen.

2.10 Bewijs dat de volgende afbeeldingen groepshomomorfismen zijn. Welke zijn injectief, welke surjectief?

$$\begin{array}{ll}
\mathbb{R}^+ \to \mathbb{C}^*, & x \mapsto e^{2\pi i x}; \\
\mathbb{C}^* \to \mathbb{C}^*, & z \mapsto \overline{z}; \\
\mathbb{C}^* \to \mathbb{R}^*, & z \mapsto z\overline{z}; \\
\mathbb{R}^* \to \mathbb{R}^*, & x \mapsto |x|; \\
\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, & a \mapsto \overline{a} \qquad (n \in \mathbb{Z}_{>0}); \\
\mathbb{C}^* \to \mathrm{GL}(2, \mathbb{R}), & a + bi \mapsto \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \qquad (a, b \in \mathbb{R}); \\
\mathbb{H}^* \to \mathrm{GL}(2, \mathbb{C}), & \alpha + \beta j \mapsto \left(\begin{smallmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{smallmatrix}\right) \qquad (\alpha, \beta \in \mathbb{C}).
\end{array}$$

2.11 Laat $d, n \in \mathbb{Z}_{>0}$ met $d \mid n$.

(a) Bewijs dat er een groepshomomorfisme $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ is waarvoor geldt $f(a \mod n) = (a \mod d)$, voor alle $a \in \mathbb{Z}$. Is f surjectief?

(b) Bewijs dat er een groepshomomorfisme $g\colon (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*$ is waarvoor geldt $g(a \mod n) = (a \mod d)$, voor alle $a \in \mathbb{Z}$ met $\gcd(a, n) = 1$.

(c) Laat $a \in \mathbb{Z}$ voldoen aan $\gcd(a, d) = 1$. Zij t het product van alle priemgetallen die n delen maar a niet. Bewijs: $\gcd(a + td, n) = 1$.

(d) Bewijs dat de afbeelding g uit (b) surjectief is. Geef een voorbeeld, met $d < n$, waar g ook injectief is.

2.12 Zij G een groep. Bewijs dat de afbeelding $f\colon G \to G$ gedefinieerd door $f(x) = x^2$ een endomorfisme van G is dan en slechts dan als G abels is.

2.13 Laten G_1 en G_2 groepen zijn, en veronderstel dat G_2 abels is. Voor $f, g \in \mathrm{Hom}(G_1, G_2)$ definiëren we $f \star g\colon G_1 \to G_2$ door

$$(f \star g)(a) = f(a) \cdot g(a) \quad (a \in G_1).$$

Bewijs dat $f \star g$ een homomorfisme $G_1 \to G_2$ is, en dat $\mathrm{Hom}(G_1, G_2)$ met de bewerking $\star$ een abelse groep is.

2.14 Bepaal de kernen en beelden van de homomorfismen in 2.9(a), (b), (c), (e), (g) en van de eerste vijf homomorfismen in Opgave (2.10).

2.15

(a) Stel dat G_1 en G_2 groepen zijn die elk één element hebben. Bewijs: $G_1 \cong G_2$.

(b) Stel dat G_1 en G_2 groepen zijn die elk twee elementen hebben. Bewijs: $G_1 \cong G_2$. Geldt het ook nog voor drie elementen? En voor vier?

2.16 Bewijs de volgende isomorfismen:

(a) $(\mathbb{Z}/12\mathbb{Z})^* \cong V_4 \cong D_2 \cong P(X)$ (vgl. Opgaven 1.8 en 1.10) waarbij X een verzameling van twee elementen is, en $P(X)$ als in Opgave 1.28 gedefinieerd is.

(b) $\mathbb{R}^2 \cong \mathbb{C}^+$, $\mathbb{R}^4 \cong \mathbb{H}^+$ (vgl. 1.10).

(c) $G \cong \mathbb{R}^+$, waarbij G de groep uit Opgave 1.23(c) is.

(d) $V_4 \cong \big\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\} \subset S_4$.

2.17 Laat $n \geq 3$. Bewijs dat S_n een ondergroep heeft die isomorf is met D_n. Is $D_3 \cong S_3$?

2.18 Bepaal de pariteit van alle elementen van S_3.

2.19 Bewijs: $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$, voor alle $\sigma \in S_n$

2.20 Bereken de tekens van

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}, \quad \text{en} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 1 & 2 & 3 \end{pmatrix}.$$

2.21 (Naar Sam Loyd.)

Sam Loyd, Amerikaans puzzelexpert, 1841-1911

(a) Vijftien blokjes, genummerd van 1 t/m 15, liggen in een doosje zoals hieronder afgebeeld; de zestiende plaats is leeg.

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

Het is de bedoeling dat men zei met de blokjes schuift dat ze in de juiste volgorde komen te liggen (dus met 14 en 15 verwisseld). Kan dit?

(b) Bewijs dat de puzzel oplosbaar is vanuit precies de helft van alle denkbare beginposities.

2.22 Hetzelfde spel als in de vorige opgave wordt nu met letters gespeeld. In de puzzel hieronder moet "wta" gecorrigeerd worden tot "wat". Kan dit?

D	E	N	K
O	F	S	C
H	U	I	F
W	T	A	

2.23 Laat X een verzameling zijn. Definieer

$$\varphi\colon (\mathbb{Z}/2\mathbb{Z})^X \to P(X) \qquad \text{(zie Opgaven 1.28 en 1.29 voor notaties)}$$

door

$$\varphi(f) = \big\{x \in X \;\big|\; f(x) = (1 \mod 2) \in \mathbb{Z}/2\mathbb{Z}\big\} \qquad (f \in (\mathbb{Z}/2\mathbb{Z})^X).$$

Bewijs dat φ een isomorfisme is, en dat de inverse χ van φ wordt gegeven door

$$\chi(A)(x) = \begin{cases} (1 \mod 2) & \text{als } x \in A \\ (0 \mod 2) & \text{als } x \notin A \end{cases} \qquad (A \subset X, x \in X).$$

Men noemt $\chi(A)$ de *karakteristieke functie* van A.

2.24

(a) Bepaal een geheel getal a waarvoor geldt

$$a \equiv 6 \mod 9, \quad a \equiv 24 \mod 41, \quad a \equiv 162 \mod 271.$$

(b) Bepaal een geheel getal a waarvoor geldt

$$a \equiv 6 \mod 7, \quad a \equiv 10 \mod 11, \quad a \equiv 12 \mod 13,$$

$$a \equiv 26 \mod 27, \quad a \equiv 36 \mod 37.$$

2.25 Bewijs de volgende generalisatie van de Chinese reststelling: Laten $a_1, a_2, \ldots, a_t, n_1, n_2, \ldots, n_t$ gehele getallen zijn, met $n_i > 0 \quad (1 \leq i \leq t)$. Dan zijn de volgende twee uitspraken equivalent:

(i) er is een $a \in \mathbb{Z}$ met

$$a \equiv a_1 \mod n_1, \qquad a \equiv a_2 \mod n_2, \ldots, \qquad a \equiv a_t \mod n_t;$$

(ii) voor alle i, j met $1 \leq i < j \leq t$ geldt

$$a_i \equiv a_j \mod \text{ggd}(n_i, n_j).$$

Bovendien is het gehele getal a in (i), als het bestaat, eenduidig bepaald modulo $\text{kgv}(n_1, n_2, \ldots, n_t)$.

2.26 Laat $n, m \in \mathbb{Z}_{>0}$. Bewijs:

$$(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/\text{kgv}(n,m)\mathbb{Z}) \times (\mathbb{Z}/\text{ggd}(n,m)\mathbb{Z}).$$

Aanwijzing: gebruik de isomorfie van 2.31 om het vraagstuk terug te voeren tot het geval waarin n en m allebei machten van een priemgetal p zijn.

2.27 Laat

$$U_1 = \left\{ z \in \mathbb{C} \;\middle|\; |z| = 1 \right\} \subset \mathbb{C}^*.$$

(a) Bewijs dat U_1 een ondergroep is van $\mathbb{C}^*$. Men noemt U_1 de *cirkelgroep*.

(b) Bewijs: $\mathbb{C}^* \cong U_1 \times \mathbb{R}^+$.

2.28 Laat $k, n \in \mathbb{Z}$ met $0 < k < n$. Definieer $H \subset S_n$ door

$$H = \left\{ \sigma \in S_n \;\middle|\; 1 \leq \sigma(i) \leq k \text{ voor alle } i = 1, 2, \ldots, k \right\}.$$

Bewijs dat H een ondergroep van S_n is, en dat H isomorf is met $S_k \times S_{n-k}$.

2.29 Laat K een kubus in de driedimensionale ruimte zijn, met het zwaartepunt in de oorsprong, en zij G de groep congruenties van de ruimte die K in zichzelf laat overvoeren (zie Opgave 1.12). We definiëren $\sigma \in G$ door $\sigma(x) = -x \quad (x \in \mathbb{R}^3)$, en $H_1, H_2 \subset G$ door

$$H_1 = \big\{\mathrm{id}_{\mathbb{R}^3}, \sigma\big\},$$
$$H_2 = \big\{\tau \in G \;\big|\; \det(\tau) = 1\big\}$$

(det = determinant; het is zinvol om over de determinant van τ te spreken, want alle elementen van G zijn lineaire afbeeldingen).

(a) Bewijs dat H_1 een ondergroep van G is, en dat $H_1 \cong \mathbb{Z}/2\mathbb{Z}$.

(b) Bewijs dat H_2 een ondergroep van G is, en dat $H_2 \cong S_4$ (aanwijzing: ga na dat een element van H_2 volledig bepaald is door de wijze waarop het de vier hoofddiagonalen van de kubus permuteert).

(c) Bewijs: $G \cong (\mathbb{Z}/2\mathbb{Z}) \times S_4$.

2.30 Zij $f\colon G_1 \to G_2$ een groepshomomorfisme, en H_i een ondergroep van G_i $(i = 1, 2)$. Bewijs dat $f[H_1]$ een ondergroep van G_2 is, en $f^{-1}[H_2]$ een ondergroep van G_1.

Hoofdstuk 3

Voortbrengers, orde, index.

Laat G een groep zijn en $S \subset G$ een niet-lege deelverzameling. Zij $H \subset G$ de verzameling elementen $a \in G$ die geschreven kunnen worden in de vorm $a = x_1 x_2 \dots x_n$ met $n \in \mathbb{Z}_{>0}$ en met $x_i \in S$ of $x_i^{-1} \in S$ voor elke i, $(1 \leq i \leq n)$. Men gaat gemakkelijk na dat H een ondergroep van G is. We noemen H de door S *voortgebrachte ondergroep*, en we zeggen dat S de ondergroep H voortbrengt, notatie: $H = \langle S \rangle$. Als S eindig is, $S = \{s_1, s_2, \dots s_t\}$, dan schrijven we $H = \langle s_1, s_2, \dots, s_t \rangle$ en zeggen we dat $s_1, \dots, s_t$ voortbrengers zijn voor H.

Als G een groep is, en $x \in G$, dan zien we direct uit de definitie dat

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, e, x, x^2, x^3, \dots\} = \left\{x^n \;\middle|\; n \in \mathbb{Z}\right\}.$$

We noemen G *cyclisch* als G wordt voortgebracht door (een verzameling van) één element, d.w.z., als er een $x \in G$ is met $G = \langle x \rangle$. Een dergelijk element x heet een voortbrenger van G.

Voorbeeld 3.1. Het element 1 is een voortbrenger van de additieve groep $\mathbb{Z}^+$; ook -1 is een voortbrenger van $\mathbb{Z}^+$.Verder is $\overline{1}$ een voortbrenger van $\mathbb{Z}/n\mathbb{Z}$. De groepen $\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$ zijn dus cyclisch. Beneden zullen we zien, dat er op isomorfie na geen andere cyclische groepen bestaan.

Voorbeeld 3.2. De verzameling van alle cykels brengt S_n voort omdat we wegens 1.18 elke permutatie kunnen schrijven als een product van cykels. De verzameling van alle verwisselingen brengt ook S_n voort omdat elke cykel te schrijven is als een product van verwisselingen:

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)\,(a_2\ a_3)\,\cdots\,(a_{k-2}\ a_{k-1})\,(a_{k-1}\ a_k).$$

De alternerende groep wordt voortgebracht door alle 3-cykels, het bewijs van deze observatie vormt het onderwerp van oefening 3.4.

Definitie 3.3. Laat G een groep zijn, en $x \in G$. Als er een positief geheel getal n bestaat waarvoor $x^n = e$, dan heet de kleinste dergelijke n de *orde van* x, notatie: orde(x). Bestaat er niet zo'n n, dan zeggen we dat de orde van x oneindig is, notatie: orde$(x) = \infty$.

Voorbeelden 3.4. (a) Voor het eenheidselement $e \in G$ geldt orde$(e) = 1$. Bovendien is e het enige element van G met orde 1.

(b) Voor $G = \mathbb{R}^*$ geldt orde$(1) = 1$, orde$(-1) = 2$, en orde$(x) = \infty$ voor $x \neq \pm 1$. Voor $G = \mathbb{C}^*$ geldt orde$(i) = 4$. Voor $G = \mathbb{Z}^+$ geldt orde$(x) = \infty$, voor alle $x \neq 0$.

(c) In de additieve groep $\mathbb{Z}/n\mathbb{Z}$ geldt orde$(\overline{1}) = n$. Laat algemener $a \in \mathbb{Z}/n\mathbb{Z}$, met $1 \leq a \leq n$. Dan is orde(a) het kleinste positieve gehele getal m waarvoor

$$\underbrace{\overline{a} + \cdots + \overline{a}}_{m\times} = m \cdot \overline{a} = \overline{ma}$$

gelijk is aan 0 in $\mathbb{Z}/n\mathbb{Z}$, d.w.z. waarvoor ma deelbaar is door n. Omdat ma natuurlijk ook door a deelbaar is, treedt dit voor het eerst op als $ma = \text{kgv}(a, n)$, dus als $m = \text{kgv}(a, n)/a = n/\text{ggd}(a, n)$. We concluderen:

$$\text{orde}(a) = n/\text{ggd}(a, n).$$

In het bijzonder zien we dat orde$(\overline{a})$ een deler is van n, het aantal elementen van de groep. Het zal blijken dat dit een algemene eigenschap is, zie 3.9 en 3.29.

(d) Als $\sigma \in S_n$ een k-cykel is, dan geldt orde$(\sigma) = k$. Als $\sigma \in S_n$ het product van t disjuncte cykels van lengtes $k_1, \ldots, k_t$ is, dan is orde(σ) het kleinste positieve gehele getal dat door elk van de getallen $k_1, k_2, \ldots, k_t$ deelbaar is, dus:

$$\text{orde}(\sigma) = \text{kgv}(k_1, k_2, \ldots, k_t).$$

(Probeer dit zelf te bewijzen).

Laat nu d een positieve deler van n zijn. We beweren: het aantal elementen $a \in \mathbb{Z}/n\mathbb{Z}$ met orde$(a) = d$ is gelijk aan $\varphi(d)$ (zie 1.15 voor de definitie van $\varphi(d)$). Bewijs hiervan: orde$(\overline{a}) = d$ betekent hetzelfde als $\text{ggd}(a, n) = n/d$, en dit is hetzelfde als

$$a = b \cdot \frac{n}{d} \qquad \text{met ggd}(b, d) = 1 \text{ en } 1 \leq b \leq d$$

(ga dit na; we nemen aan dat $1 \leq a \leq n$). Omdat er $\varphi(d)$ zulke b's te vinden zijn, is hiermee het bewijs voltooid.

Laten we d nu over alle delers van n lopen, dan zien we dat er in totaal $\sum_{d|n} \varphi(d)$ elementen in $\mathbb{Z}/n\mathbb{Z}$ zijn ($\sum_{d|n}$ betekent dat gesommeerd wordt over de verzameling positieve delers van n). Anderzijds is het duidelijk, dat het aantal elementen van $\mathbb{Z}/n\mathbb{Z}$ gelijk is aan n. Hiermee hebben we de *formule van Gauss* bewezen:

$$\sum_{d|n} \varphi(d) = n\,.$$

Carl Friedrich Gauss, Duits wiskundige, 1777-1855

.

Stelling 3.5. *Laat G een groep zijn, $x \in G$ en* $\text{orde}(x) = n < \infty$. *Dan geldt voor $m \in \mathbb{Z}$,*

$$x^m = e \iff n \mid m\,.$$

Bewijs. $\Leftarrow$: als $m = qn$, dan $x^m = (x^n)^q = e^q = e$. $\Rightarrow$: Stel $x^m = e$ en schrijf $m = qn + r$ met $q, r \in \mathbb{Z}$ en $0 \leq r < n$ (Stelling 0.1). Als $r = 0$ dan geldt $m = qn$ en zijn we klaar. Stel dus dat $r > 0$ dan is $x^r = x^{m-qn} = x^m(x^n)^{-q} = ee^{-q} = e$. Dus r is een positief getal kleiner dan n zodanig dat $x^n = e$. Maar n was gedefinieerd als het keinste dergelijke getal. Dit is een tegenspraak. □

Gevolg 3.6. *Laat G een groep zijn, en $x \in G$. Dan geldt:*

(a) *Als x oneindige orde heeft, dan $\langle x \rangle \cong \mathbb{Z}$.*

(b) *Als* $\text{orde}(x) = n < \infty$, *dan $\langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$, en $\langle x \rangle$ heeft n elementen.*

Bewijs. (a) Definieer $f\colon \mathbb{Z} \to \langle x \rangle$ door $f(n) = x^n$. Dan is f een homomorfisme (zie 2.9(f)) dat wegens de definitie van $\langle x \rangle$ surjectief is. Omdat x oneindige orde heeft bevat $\text{Ker}(f)$ geen positief geheel getal. Maar als $n \in \text{Ker}(f)$ dan is ook $-n \in \text{Ker}(f)$, dus $\text{Ker}(f)$ bevat ook geen negatief geheel getal. Dus $\text{Ker}(f) = \{0\}$, en f is injectief Stelling 2.14). We concluderen dat f een isomorfisme is.

(b) Definieer $f\colon \mathbb{Z}/n\mathbb{Z} \to \langle x \rangle$ door $f(\overline{a}) \mapsto x^a$. Uit

$$\overline{a} = \overline{b} \iff n \mid a - b \overset{3.5}{\iff} x^{a-b} = e \iff x^a = x^b$$

zien we tegelijk dat f welgedefinieerd is en dat f injectief is. Verder is duidelijk dat f een surjectief groepshomomorfisme is. Dus f is een isomorfisme, en $\#\langle x \rangle = \#(\mathbb{Z}/n\mathbb{Z}) = n$. □

Uit 3.6 zien we dat er voor iedere n, op isomorfie na, maar één cyclische groep van n elementen is. Kortheidshalve geeft men deze vaak met C_n aan in plaats van met $\mathbb{Z}/n\mathbb{Z}$. De groep C_n noteert men dan ook multiplicatief

$$C_n = \{e, \alpha, \alpha^2, \ldots, \alpha^{n-1}\} \text{ met } \alpha^n = e$$

Merk op dat cyclische groepen abels zijn (dit geldt immers voor $\mathbb{Z}/n\mathbb{Z}$).

Gevolg 3.7. *Laat $f\colon G_1 \to G_2$ een groepshomomorfisme zijn. Als $x \in G_1$ eindige orde heeft, dan heeft $f(x) \in G_2$ ook eindige orde, en* $\text{orde}\big(f(x)\big) \mid \text{orde}(x)$. *Als f injectief is, dan geldt* $\text{orde}\big(f(x)\big) = \text{orde}(x)$ *voor alle $x \in G_1$.*

Bewijs. Als $m = \text{orde}(x)$, dan $x^m = e_1$, dus

$$(f(x))^m = f(x^m) = f(e_1) = e_2,$$

waaruit blijkt dat $\text{orde}(f(x))$ eindig is en m deelt wegens 3.5. Indien f injectief is geldt voor alle $n \in \mathbb{Z}$

$$x^n = e_1 \iff f(x^n) = e_2 \iff f(x)^n = e_2$$

dus x en $f(x)$ hebben dezelfde orde. □

Als $f\colon G_1 \to G_2$ een isomorfisme van groepen is, dan geldt $\text{orde}(x) = \text{orde}(f(x))$ voor elke $x \in G_1$ wegens 3.7. Hieruit volgt dat isomorfe groepen evenveel elementen van orde n bezitten, voor elke $n \in \{1, 2, 3, \ldots, \infty\}$. Deze opmerking kan men soms gebruiken om aan te tonen dat bepaalde groepen niet isomorf zijn (Opgave 3.26), maar deze methode werkt niet altijd (Opgave 3.27).

Definitie 3.8. De orde van een groep G is het aantal elementen van G, notatie: $\#G$ of $\text{orde}(G)$. Merk op dat uit 3.6 volgt: $\text{orde}(\langle x \rangle) = \text{orde}(x)$, voor $x \in G$.

Stelling 3.9. *Laat G een eindige abelse groep zijn, en $x \in G$. Dan is de orde van x eindig, en een deler van de orde van G.*

Opmerking 3.10. Zoals we in 3.29 zullen zien is de voorwaarde dat G abels is overbodig. In het abelse geval is er echter een bijzonder eenvoudig bewijs.

Bewijs. Laat $m = \text{orde}(G)$, en laten $g_1, g_2, \ldots, g_m$ de elementen van G zijn. Zij $x \in G$. Wegens 1.23 zijn $xg_1, xg_2, \ldots, xg_m$ dan ook alle elementen van G, alleen misschien in een andere volgorde. Maar omdat G abels is doet bij het vermenigvuldigen de volgorde er niet toe, dus

$$g_1 g_2 \cdots g_m = (xg_1)(xg_2)\cdots(xg_m)\,.$$

Bovendien hebben we, weer omdat G abels is:

$$(xg_1)(xg_2)\cdots(xg_m) = x^m g_1 g_2 \cdots g_m\,.$$

Combineren we beide gelijkheden, dan zien we dat $x^m = e$, dus wegens 3.5 geldt $\text{orde}(x) \mid m = \text{orde}(G)$. □

Gevolg 3.11 (Stelling van Euler)**.** *Laat $a, m \in \mathbb{Z}$ met $m > 0$ en $\text{ggd}(a, m) = 1$. Dan geldt*

$$a^{\varphi(m)} \equiv 1 \bmod m$$

Hier is φ de functie van Euler (zie 1.15).

Bewijs. Wegens $\text{ggd}(a, m) = 1$ geldt $\overline{a} = (a \mod m) \in (\mathbb{Z}/m\mathbb{Z})^*$ (zie 1.15), en 3.9 levert nu $\text{orde}(\overline{a}) \mid \text{orde}((\mathbb{Z}/m\mathbb{Z}) = \varphi(m)$, dus $\overline{a}^{\varphi(m)} = \overline{1}$ d.w.z. $a^{\varphi(m)} = 1 \mod m$. □

Pierre de Fermat, Frans wiskundige, 1601-1665

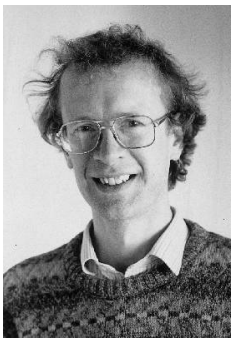
Gevolg 3.12 (Kleine stelling van Fermat)**.** *Laat p een priemgetal zijn, en $a \in \mathbb{Z}$. Dan geldt $a^p = a$* mod p.

Bewijs. Als a deelbaar door p is, geldt $a^p \equiv 0 \equiv a \mod p$. We mogen dus aannemen dat a niet deelbaar door p is. Dan geldt $\text{ggd}(a,p) = 1$ en we kunnen 3.11 toepassen. Omdat p priem is hebben we $\varphi(p) = p - 1$, dus we vinden $a^{p-1} \equiv 1 \mod p$. Na vermenigvuldiging met a levert dit $a^p \equiv a$ mod p. □

Zie 3.33 en Opgave 3.29 voor twee andere bewijzen van 3.12.

Voorbeeld 3.13. Neem $a = 3$ en $p = 7$; dan is $3^7 - 3 = 2184$ en dit is inderdaad een 7-voud.

Opmerking 3.14. Men noemt 3.12 ook wel de kleine stelling van Fermat, om verwarring te voorkomen met de grote (of 'laatste') stelling van Fermat, die zegt dat er voor $n \in \mathbb{Z}$ met $n \geq 3$ geen $x, y, z \in \mathbb{Z} > 0$,



Andrew Wiles, Engels wiskundige

bestaan met $x^n + y^n = z^n$. Fermat claimde dat hij hiervoor een bewijs had maar dat de kantlijn van het boek te klein was om het op te schrijven. Ruim drie eeuwen later, in 1995, vond Andrew Wiles met de hulp van zijn student Richard Taylor een bewijs.

Definitie 3.15. Laat H een ondergroep van een groep G zijn, en $a \in G$. Dan heet de deelverzameling $aH = \{ah \mid h \in H\}$ van G een *linkernevenklasse* (Engels: left coset) van H, en $Ha = \{ha \mid h \in H\}$ een *rechternevenklasse* (right coset) van H.

Wordt G additief geschreven, dan schrijven we $a + H$ en $H + a$ in plaats van aH en Ha.

De verzameling linkernevenklassen van H wordt aangegeven met G/H, en de verzameling rechternevenklassen met $H\backslash G$.

Voorbeelden 3.16. (a) Neem $a = e$. Dan geldt $aH = Ha = H$. Dus H is zowel een linker- als rechternevenklasse van zichzelf. Merk op dat we steeds hebben $aH = Ha = H$ als $a \in H$.

(b) Laat $G = \mathbb{R}^2$ (additief), en H een rechte door de oorsprong. Voor $a \in \mathbb{R}^2$ is de nevenklasse $a + H = H + a$ de rechte door a evenwijdig aan H.

(c) Laat $G = \mathbb{Z}$ (additief) en $H = n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ voor zekere $n \in \mathbb{Z}, n > 0$. De nevenklassen $a+H = H+a$ zijn nu precies de restklassen $a+n\mathbb{Z}$ uit Voorbeeld 1.14. Er zijn dus n verschillende nevenklassen van H in G, en ze zijn twee aan twee disjunct.

(d) In de bovenstaande voorbeelden gold steeds $aH = Ha$. Dit is bij abelse G natuurlijk steeds het geval. Ondergroepen H van G zo dat voor alle $a \in G$ geldt dat $aH = Ha$ zullen in Hoofdstuk 4 een belangrijke rol spelen. In het volgende voorbeeld geldt $aH \neq Ha$: neem $G = S_n$, met $n \geq 3$, en $H = \{\sigma \in S_n \mid \sigma(1) = 1\}$; men gaat gemakkelijk na dat H een ondergroep van S_n is. Voor $a = (1\ 2\ 3)$ geldt nu

$$aH = \{a\sigma \in S_n \mid \sigma(1) = 1\} = \{\tau \in S_n \mid \tau(1) = 2\},$$
$$Ha = \{\sigma a \in S_n \mid \sigma(1) = 1\} = \{\tau \in S_n \mid \tau(3) = 1\}.$$

Zodoende vinden we dat $(1\ 2) \in aH$ terwijl $(1\ 2) \notin Ha$; dus $aH \neq Ha$.

In de voorbeelden (b), (c) en (d) ziet men dat twee verschillende linkernevenklassen van H in G steeds disjunct zijn. De volgende stelling zegt dat dit een algemene eigenschap is:

Stelling 3.17. *Laat G een groep zijn, $H \subset G$ een ondergroep.*

(a) *Voor alle $a, b \in G$ geldt: $aH = bH$ dan en slechts dan als $a^{-1}b \in H$.*

(b) *Voor alle $a, b \in G$ geldt: of $aH = bH$ of $aH \cap bH = \emptyset$.*

(c) *Elke $x \in G$ zit in precies één linkernevenklasse van H.*

Opmerking 3.18. Een analoge stelling geldt voor rechternevenklassen; in (a) moet dan $a^{-1}b$ door ba^{-1} worden vervangen.

Bewijs. (a) $\Rightarrow$: Stel $aH = bH$. Dan $b = be \in bH = aH$, dus er is een $h \in H$ met $b = ah$. Hieruit volgt $a^{-1}b = h \in H$. $\Leftarrow$: Stel $a^{-1}b = h \in H$. Voor elke $h' \subset H$ geldt dan $bh' = (ah)h' = a(hh') \in aH$ (want $hh' \in H$), dus $bH \subset aH$, en omgekeerd $ah' = (bh^{-1})h' = b(h^{-1}h') \in bH$ (want $h^{-1}h' \in H$), dus $aH \subset bH$. We concluderen dat $aH = bH$.

(b) Stel $aH \cap bH \neq \emptyset$; we moeten bewijzen dat $aH = bH$. Laat $x \in aH \cap bH$, dan $x = ah_1$, $x = bh_2$ voor zekere $h_1, h_2 \in H$. Dan $a^{-1}b = h_1h_2^{-1} \in H$, dus $aH = bH$ volgens (a).

(c) Het element x zit zeker in de linkernevenklasse xH van H. Verder kan x niet in meer dan één linkernevenklasse van H zitten, want twee verschillende linkernevenklassen van H zijn volgens (b) disjunct. □

Opmerking 3.19. Nevenklassen kunnen ook met behulp van equivalentierelaties ingevoerd worden: definieer

$$a \sim b \iff a^{-1}b \in H$$

dan is $\sim$ een equivalentierelatie op G, en de equivalentieklassen van $\sim$ zijn volgens Stelling 3.17(a) precies de linkernevenklassen van H.

Stelling 3.20. *Laat G een groep zijn en $H \in G$ een ondergroep. Dan geldt $\#aH = \#Ha = \#H$ voor elke $a \in G$.*

Bewijs. De afbeelding $f\colon H \to aH$ gegeven door $h \mapsto ah$, is duidelijk bijectief, dus $\#H = \#aH$. Evenzo bewijst men $\#H = \#Ha$. □

Definitie 3.21. Laat G een groep zijn en $H \in G$ een ondergroep. Het aantal verschillende linkernevenklassen van H in G heet de *index* van H in G, notatie: $[G : H]$ of index$[G : H]$. Er geldt dus per definitie $[G : H] = \#(G/H)$.

Een *representantensysteem* voor de linkernevenklassen van H in G is een deelverzameling $S \subset G$ die uit elke linkernevenklasse van H in G precies één element bevat. Is S zo'n representantensysteem, dan geldt $\#S = [G : H]$ en G is de disjuncte vereniging van de deelverzamelingen sH:

$$G = \coprod_{s \in S} sH\,.$$

(Het symbool $\coprod$ drukt uit dat dit een disjuncte vereniging is.)

Analoog definieert men een representantensysteem voor de rechternevenklassen van H in G: Uit Opgave 3.31 blijkt dat de index niet verandert als we in 3.21 "linker" door "rechter" vervangen.

Voorbeeld 3.22. De gehele getallen $0, 1, \ldots, n-1$ zijn een representantensysteem voor de linkernevenklassen van $n\mathbb{Z}$ in $\mathbb{Z}$, dus $[\mathbb{Z} : n\mathbb{Z}] = n$.

De diëdergroep D_n heeft een ondergroep $H = \{1, \sigma\}$. De draaiingen vormen samen een representantensysteem voor de linkernevenklassen want in elke nevenklasse zit precies één draaiing en één spiegeling, dus $[D_n : H] = n$. De draaiingen vormen ook een representantensysteem voor de rechternevenklassen, maar let op de linkernevenklassen en rechternevenklassen zijn niet gelijk: $\rho^i H = \{\rho^i\sigma, \rho^i\}$ en $H\rho^i = \{\rho^{n-i}\sigma, \rho^i\}$.

Joseph Louis Lagrange, Frans wiskundige, 1736-1813

Stelling 3.23 (Stelling van Lagrange)**.** *Laat G een groep zijn en H een ondergroep. Dan geldt* $\text{orde}(G) = [G : H] \cdot \text{orde}(H)$.

Bewijs. Er zijn $[G : H]$ verschillende linkernevenklassen van H in G (zie Definitie 3.21), en elke linkernevenklasse bevat precies orde(H) elementen (Stelling 3.20). Omdat elke $x \in G$ tot precies één linkernevenklasse van H behoort (Stelling 3.17(c)) volgt hieruit dat er precies $[G : H] \cdot \text{orde}(H)$ elementen in G zijn. □

Opmerking 3.24. Stelling en bewijs zijn ook geldig als G oneindig is; orde en index moeten dan als kardinaalgetallen geïnterpreteerd worden.

Gevolg 3.25. *Laat H een ondergroep van een eindige groep G zijn. Dan is de orde van H een deler van de orde van G.*

Bewijs. Duidelijk uit 3.23, want $[G : H]$ is een geheel getal. □

Voorbeeld 3.26. Laat $n \in \mathbb{Z} > 0$, en zij d een deler van n. De ondergroep $\{\overline{d}, \overline{2d}, \ldots, \overline{n-d}, \overline{n}\}$ van $\mathbb{Z}/n\mathbb{Z}$ (zie 2.6(b)) heeft orde n/d en index d. Een cyclische groep van orde n heeft dus voor elke deler d van n een ondergroep van index d, en deze ondergroep is eenduidig bepaald volgens 2.6(b).

Voorbeeld 3.27. Laat $k, n \in \mathbb{Z}$ met $0 < k < n$. Volgens Opgave 2.28 bezit de groep S_n (van orde $n!$) een ondergroep van orde $k! \cdot (n-k)!$. Uit 3.25 vinden we dus het bekende feit terug, dat de binomiaalcoëfficiënt $\binom{n}{k} = \frac{n!}{n!(n-k)!}$ een geheel getal is.

Gevolg 3.28. *Laten H_1, H_2 ondergroepen van een eindige groep G zijn, met $H_1 \subset H_2$. Dan geldt*

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

Bewijs. Omdat G eindig is, zijn alle optredende ordes eindig, dus in de formule van 3.23 kunnen we delen door orde(H). Dit levert:

$$[G : H_1] = \frac{\text{orde}(G)}{\text{orde}(H_1)} = \frac{\text{orde}(G)}{\text{orde}(H_2)} \cdot \frac{\text{orde}(H_2)}{\text{orde}(H_1)} = [G : H_2] \cdot [H_2 : H_1] .$$

□

Het volgende gevolg is een verscherping van Stelling 3.9.

Gevolg 3.29. *Laat G een eindige groep zijn, en $x \in G$. Dan is de orde van x een deler van de orde van G.*

Bewijs. Dit volgt uit 3.25 met $H = \langle x \rangle$, want orde$\big(\langle x \rangle\big) =$ orde(x). □

Gevolg 3.30. *Laat G een groep zijn waarvoor* orde$(G) = p$ *een priemgetal is. Dan is G cyclisch, en $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Bewijs. Kies $x \in G$, $x \neq e$, willekeurig. Dan is orde(x) een deler van p, maar orde$(x) \neq 1$ (want $x \neq e$). Omdat p priem is volgt hieruit orde$(x) = p$. Dus $\langle x \rangle$ heeft p elementen, en daarom $\langle x \rangle = G$. Uit 3.6(b) volgt nu $G = \langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$. □

Gevolg 3.31. *Laat G een groep zijn met* orde$(G) \leq 5$. *Dan geldt: G is cyclisch of $G \cong V_4$.*

Bewijs. Als orde$(G) = 2$, 3 of 5 dan is G cyclisch wegens 3.30. Als orde$(G) = 1$ dan $\mathbb{G} = \{e\}$, en $\{e\}$ is kennelijk cyclisch. Laat tenslotte orde$(G) = 4$, zeg $G = \{e, a, b, c\}$, met eenheidselement e. Elk van de elementen a, b en c heeft orde 2 of 4, wegens 3.29. Als er een element is, zeg a, van orde 4 dan is $G = \langle a \rangle$, dus G is cyclisch. Anders hebben a, b en c alledrie orde 2. Dan $a^2 = b^2 = c^2 = e$, dus we kennen het volgende deel van de groepentabel:

	e	a	b	c
e	e	a	b	c
a	a	e	$*$	
b	b		e	
c	c			e

Men ziet nu direct dat voor de zes open gebleven plaatsen geen keus is, omdat geen element twee keer in dezelfde rij of kolom mag voorkomen (Stelling 1.23). Bijvoorbeeld: $* \notin \{e, a\}$ (want deze staan al in dezelfde rij), en $* \neq b$ (want deze staat al in dezelfde kolom), dus $* = c$. Het resultaat is dat G de viergroep van Klein is. □

Uit 3.31 zien we in het bijzonder dat een groep met minder dan zes elementen abels is. Merk op dat S_3 een niet-abelse groep met precies zes elementen is. Behalve de cyclische groep van orde zes is S_3 de enige groep met zes elementen, zie Opgave 3.43.

De volgende tabel geeft alle groepen van orde < 16, op isomorfie na.

orde	abels	niet abels	aantal
1	C_1		1
2	C_2		1
3	C_3		1
4	C_4, $C_2 \times C_2 \cong V_4$		2
5	C_5		1
6	C_6	S_3	2
7	C_7		1
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$	D_4, Q	5
9	C_9, $C_3 \times C_3$		2
10	C_{10}	D_5	1
11	C_{11}		1
12	C_{12}, $C_2 \times C_6$	D_6, A_4, B	5
13	C_{13}		1
14	C_{14}	D_7	2
15	C_{15}		1

Verklaring der symbolen: C_n is de cyclische groep van orde n (zie opmerking voor 3.7); D_n is de diëdergroep van orde $2n$ (zie 1.21); Q de quaterniongroep (zie 1.13); voor S_n en A_n zie 1.16 en 2.20; de groep B bestaat uit de twaalf uitdrukkingen $\alpha^i\beta^j$ met $0 \leq i < 3$ en $0 \leq j < 4$, met vermenigvuldiging gegeven door $\alpha^i\beta^j \cdot \alpha^k\beta^\ell = \alpha^{i+(-1)^j k}\beta^{j+\ell}$ waarbij de exponent bij α modulo 3 en de exponent bij β modulo 4 gerekend wordt.

De volledigheid van de tabel voor ordes 1, 2, 3, 4, 5, 7, 11 en 13 volgt uit 3.30 en 3.31 en voor ordes 6, 9, 10, 14 en 15 uit 7.7 en Opgave 7.12. De gevallen van ordes 8 en 12 laten we als opgave aan de gevorderde lezer over.

Voor het geval van abelse groepen kan men 8.1 toepassen. De laatste stelling van deze paragraaf is een gedeeltelijke omkering van 3.29.

Augustin-Louis Cauchy, Frans wiskundige, 1789-1857

Stelling 3.32 (Stelling van Cauchy)**.** *Laat G een eindige groep zijn, en p een priemgetal dat een deler is van de orde van G. Dan is er een $x \in G$ met* $\text{orde}(x) = p$.

De voorwaarde dat p een priemgetal is kan niet gemist worden: anders zou immers elke groep van orde n een element van orde n bevatten, dus cyclisch zijn, en dat is blijkens de tabel niet voor alle n het geval.

Voor $p = 2$ zegt de stelling van Cauchy dat een eindige groep G van even orde steeds een element van orde 2 bevat. In dit speciale geval is er een erg eenvoudig bewijs. Laat

$$V = \left\{ x \in G \;\middle|\; x \neq x^{-1} \right\}.$$

De elementen van V vallen in groepjes van twee uiteen:

$$V = \{a, a^{-1}\} \cup \{b, b^{-1}\} \cup \cdots$$

(dit is een disjuncte vereniging). Hieruit ziet men dat V een even aantal elementen heeft. Maar ook G heeft een even aantal elementen, dus $G \setminus V$ heeft een even aantal elementen. Dit betekent dat er behalve het eenheidselement e, dat zeker tot $G \setminus V$ behoort, nog minstens één element $x \in G \setminus V$ is. Dan $x = x^{-1}$ en $x \neq e$, dus $\text{orde}(x) = 2$, zoals verlangd.

Het bewijs van 3.32 dat we hieronder geven, kan worden opgevat als generalisering van dit bewijs. Aan het eind van Hoofdstuk 6 zullen we een bewijs van 3.32 geven dat op volkomen andere principes berust.

Voorbeeld 3.33. Om de combinatorische grondgedachte van het bewijs van 3.32 duidelijk te maken geven we eerst een bewijs van de Stelling van Fermat 3.12, waarin hetzelfde idee in een eenvoudiger vorm optreedt.

Zij $a \in \mathbb{Z}_{>0}$, en zij A een verzameling van a elementen. Laat p een priemgetal zijn, en laat

$$B = \underbrace{A \times \cdots \times A}_{p \text{ factoren}} = \left\{ (x_0, x_1, \ldots, x_{p-1}) \;\middle|\; x_i \in A \text{ voor } 0 \leq i < p \right\}.$$

Dan geldt $\#B = (\#A)^p$.

Laat $B_0 \subset B$ de deelverzameling zijn van die elementen waarvan alle coordinaten gelijk zijn:

$$B_0 = \left\{ (x, \ldots, x) \;\middle|\; x \in A \right\}.$$

Het is duidelijk dat $\#B_0 = a$. Met B_1 geven we het complement van B_0 in B aan:

$$B_1 = \left\{(x_0, x_1, \ldots, x_{p-1}) \;\middle|\; x_i \neq x_j \text{ voor zekere } 0 \leq i < j < p\right\}.$$

Er geldt $\#B_1 = \#B - \#B_0 = a^p - a$.

Om te bewijzen dat $a^p \equiv a \bmod p$ is het nu voldoende om aan te tonen dat $\#B_1$ deelbaar door p is. Dit doen we met behulp van de afbeelding "cyclisch opschuiven"

$$\varphi\colon B_1 \to B_1 \qquad \text{gegeven door} \quad (x_0, x_1, \ldots, x_{p-1}) \mapsto (x_1, x_2, \ldots, x_{p-1}, x_0).$$

Passen we deze afbeelding p maal toe dan krijgen we de identiteit: $\varphi^p = \mathrm{id}_{B_1}$. Als we nu kunnen bewijzen dat voor elke $b \in B_1$ de elementen

$$b\,, \quad \varphi(b)\,, \quad \varphi^2(b)\,, \quad \ldots\,, \quad \varphi^{p-1}(b)$$

alle p *verschillend* zijn, dan valt B_1 in groepjes ter grootte p uiteen:

$$B_1 = \left\{b, \varphi(b), \varphi^2(b), \ldots, \varphi^{p-1}(b)\right\} \cup \cdots$$

en dan is het duidelijk dat het aantal elementen van B_1 deelbaar is door p.

Stel dus dat $\varphi^i(b) = \varphi^j(b)$ met $0 \leq i < j \leq p-1$ en $b \in B_1$. Schrijven we $k = j - i$ en passen we φ^k toe dan vinden we $b = \varphi^k(b)$. Passen we hierop weer φ^k toe dan vinden we $\varphi^{2k}(b) = \varphi^k(b) = b$. Algemeen krijgen we, met inductie naar t:

$$b = \varphi^{kt}(b) \qquad \text{voor } t = 1, 2, \ldots.$$

Uit $1 \leq k \leq p-1$ en het feit dat p priem is volgt $\mathrm{ggd}(k, p) = 1$, dus er bestaat t met $kt = 1 \mod p$. Dan geldt $\varphi^{kt} = \varphi$ en dus $\varphi(b) = \varphi^{kt}(b) = b$. Schrijven we $b = (x_0, x_1, \ldots, x_{p-1})$ dan wil dit juist zeggen dat $x_0 = x_1 = \cdots = x_{p-1}$, in tegenspraak met $b \in B_1$. Deze tegenspraak besluit het bewijs.

Merk op, dat we strikt genomen met dit argument 3.12 alleen voor positieve a bewezen hebben. Het algemene geval is hier eenvoudig toe terug te brengen.

Bewijs van van 3.32. We definiëren

$$T = \left\{(x_0, x_1, \ldots, x_{p-1}) \in G^p \;\middle|\; x_0 x_1 \cdots x_{p-1} = e\right\}.$$

Het aantal elementen van T is $(\#G)^{p-1}$; immers, $x_0, x_1, \ldots, x_{p-2}$ kunnen op $\#G \times \cdots \times \#G = \#G^{p-1}$ manieren vrij gekozen worden, en x_{p-1} ligt dan vast door

$$x_{p-1} = (x_0 x_1 \cdots x_{p-2})^{-1}.$$

Omdat $(\#G)^{p-1}$ deelbaar is door p, vinden we in het bijzonder $\#T \equiv 0 \bmod p$.

Laat nu $T_0 \subset T$ de deelverzameling zijn van die elementen, waarvan alle coordinaten gelijk zijn:

$$T_0 = \left\{(x, x, \ldots, x) \in G^p \;\middle|\; x^p = e\right\},$$

en T_1 het complement van T_0 in T:

$$T_1 = \big\{(x_0, x_1, \ldots, x_{p-1}) \in T \;\big|\; x_i \neq x_j \text{ voor zekere } 0 \leq i < j < p\big\}\,.$$

Straks zullen we bewijzen dat het aantal elementen van T_1 deelbaar is door p. Als dit zo is, dan moet ook het aantal elementen van T_0 door p deelbaar zijn, dus behalve het element $(e, e, \ldots, e) \in T_0$ moeten er nog minstens $p-1$ elementen $(x, x, \ldots, x) \in T_0$ zijn. Voor al deze elementen geldt $x^p = e$ en $x \neq e$, dus orde$(x) = p$, zoals verlangd.

Om het bewijs van 3.32 af te maken is het dus voldoende aan te tonen dat $\#T_1 \equiv 0 \bmod p$. Voor $t = (x_0, x_1, \ldots, x_{p-1}) \in T_1$ definiëren we, net als boven,

$$\varphi(t) = \big(x_1, x_2, \ldots, x_{p-1}, x_0\big) \qquad \text{('cyclisch opschuiven').}$$

Er geldt

$$x_1 x_2 \ldots x_{p-1} x_0 = x_0^{-1} x_0 x_1 x_2 \ldots x_{p-1} x_0 = x_0^{-1} e x_0 = e$$

dus $\varphi(t) \in T$, en omdat $x_0, x_1, \ldots x_{p-1}$ niet allemaal gelijk zijn, geldt zelfs $\varphi(t) \in T_1$. Precies zoals we boven voor B_1 gedaan hebben kan men nu bewijzen dat voor elke $t \in T_1$ de elementen

$$t\,, \quad \varphi(t)\,, \quad \varphi^2(t)\,, \quad \ldots\,, \quad \varphi^{p-1}(t)$$

alle p *verschillend* zijn, dus dat T_1 in groepjes ter grootte p uiteenvalt:

$$T_1 = \big\{t, \varphi(t), \varphi^2(t), \ldots, \varphi^{p-1}(t)\big\} \;\cup\; \big\{t', \varphi(t'), \varphi^2(t'), \ldots, \varphi^{p-1}(t')\big\} \;\cup\; \ldots$$

Hieruit blijkt dat $\#T_1 \equiv 0 \bmod p$, zoals verlangd. □

Opgaven

3.1 Bewijs:

$$D_n = \langle \rho, \sigma \rangle\,, \quad \text{(zie 1.21)}\,, \quad Q = \langle i, j \rangle\,, \quad \text{(zie 1.13)}\,,$$

en

$$(\mathbb{Z}/23\mathbb{Z})^* = \langle 5 \bmod 23 \rangle\,.$$

3.2 (a) Laat $1 < a < b \leq n$. Bereken $(1\ a)(1\ b)(1\ a)$.

(b) Bewijs dat elk element van S_n geschreven kan worden als product van een eindig aantal verwisselingen van de vorm $(1\ i)$ met $2 \leq i \leq n$.

3.3 Toon aan dat

$$S_n = \langle (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle.$$

3.4 Toon aan dat de alternerende groep wordt voortgebracht door alle 3-cykels:

$$A_n := \langle (i\ j\ k) | 1 \leq i < j < k \leq n \rangle$$

Hint: toon eerst aan dat A_n wordt voortgebracht door alle mogelijke producten van twee omwisselingen:

$$A_n := \langle (i\ j)(l\ k) | 1 \leq i < j \leq n, 1 \leq k < l \leq n \rangle.$$

Schrijf vervolgens $(i\ j)(k\ l)$ als product van 3-cykels. Maak hierbij onderscheid tussen verschillende gevallen (b.v. $i = l$ etc).

3.5 Bewijs dat elk element van A_n geschreven kan worden als product van een eindig aantal 3-cykels van de vorm $(1\ 2\ i)$ met $3 \leq i \leq n$.

3.6 Laat S een deelverzameling van een groep G zijn. Bewijs dat de door S voortgebrachte ondergroep van G gelijk is aan de doorsnee van alle ondergroepen van G die S omvatten.

3.7 Gebruik de formule van Gauss (zie 3.4(d)) om $\varphi(n)$ uit te rekenen voor alle positieve gehele getallen n die 60 delen.

3.8 Bereken de ordes van alle elementen van de groepen

$$V_4\,, \quad \mathbb{Z}/6\mathbb{Z}\,, \quad S_3\,, \quad S_4\,, \quad Q\,, \quad D_n\,, \quad \mathbb{Z}/18\mathbb{Z}\,.$$

(Zie 1.13 en 1.21 voor de definitie van Q en D_n.)

3.9 Laat G een groep zijn, en a, $b \in G$. Bewijs:

$$\begin{aligned} &\text{orde}(a) = \text{orde}(a^{-1}); \\ &\text{orde}(aba^{-1}) = \text{orde}(b); \\ &\text{orde}(ab) = \text{orde}(ba). \end{aligned}$$

3.10 Geef een ander bewijs van 3.5 door 2.6(a) (en het bewijs daarvan) toe te passen op de volgende ondergroep van $\mathbb{Z}$:

$$\left\{ m \in \mathbb{Z} \;\middle|\; x^m = e \right\}.$$

3.11 Laat $\sigma \in S_n$ voldoen aan $\sigma \neq (1)$, $\sigma^p = (1)$, waarbij p een priemgetal is met in $\frac{n}{2} < p \leq n$. Bewijs dat σ een p-cykel is.

3.12 Stel dat $H \subset S_n$ een ondergroep is die isomorf is met Q (zie 1.13), en laat $\tau \in H$ onder het isomorfisme $H \cong Q$ corresponderen met $-1 \in Q$. Laat $x \in \{1, 2, \ldots, n\}$.

(a) Bewijs: als $\tau(x) \neq x$, dan geldt $\sigma(x) \neq x$ voor alle $\sigma \in H$ met $\sigma \neq (1)$.

(b) Bewijs $n \geq 8$.

3.13 Wat is de kleinste n waarvoor S_n een ondergroep bevat die isomorf is met $\mathbb{Z}/6\mathbb{Z}$?

3.14 Bewijs:

$$S_n = \langle (12), (123\cdots n) \rangle\,, \quad A_5 = \langle (12)(34), (135) \rangle$$

3.15 Beschouw de groep S_{13} van permutaties van de verzameling $\{1, 2, \ldots, 13\}$.

(a) Schrijf het element

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

als een product van disjunkte cykels en bepaal het teken en de orde van σ.

(b) Schrijf de permutatie σ^{-86421} als product van disjunkte cykels.

(c) Geef een element $\tau \in S_{13}$ met $\tau^3 = \sigma$, of bewijs dat zo'n element niet bestaat.

(d) Geef een element $\rho \in S_{13}$ met $\rho^4 = \sigma$, of bewijs dat zo'n element niet bestaat.

3.16 Vind een element $\sigma \in S_{20}$ met $\text{orde}(\sigma) = 280$. Is deze σ even of oneven?

3.17 Laat $\alpha(n) = \max_{\sigma \in S_n} \text{orde}(\sigma)$. Bereken $\alpha(n)$ voor $1 \leq n \leq 8$.

3.18 Laat G een eindige groep zijn, en laat, voor $a \in G$, de afbeelding $\lambda_a \colon G \to G$ gedefinieerd zijn door $\lambda_a(x) = ax$, voor $x \in G$ (zie de opmerking na 1.23, en het bewijs van 6.6).

(a) Bewijs dat λ_a het product is van $[G : \langle a \rangle]$ disjuncte cykels van lengte $\text{orde}(a)$.

(b) Bewijs dat λ_a een oneven permutatie is dan en slechts dan als de orde van G even is, en de orde van a deelbaar is door de hoogste macht van 2 die de orde van G deelt.

(c) Stel dat $\text{orde}(G) = 2k$, met k oneven. Bewijs:

$$\lambda_a \text{ is even} \iff \text{orde}(a) \text{ is oneven.}$$

Leid hieruit af dat in dat geval de elementen van G van oneven orde een ondergroep van index 2 van G vormen.

3.19 Laat m een geheel getal > 1 zijn dat geen priemgetal is en er geen een priemgetal p is met $p^2 \mid m$. Stel dat r de grootste priemfactor van m is. Bewijs dat de groep S_r een orde heeft die deelbaar is door m, terwijl er geen $x \in G$ is van orde m.

3.20 Bewijs:

$$(\mathbb{Z}/23\mathbb{Z})^* \cong \mathbb{Z}/22\mathbb{Z}.$$

3.21 Laat $n \in \mathbb{Z}_{>0}$, en $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Bewijs:

$$\overline{m} \text{ heeft orde } n \iff \langle \overline{m} \rangle = \mathbb{Z}/n\mathbb{Z} \iff \text{ggd}(m, n) = 1.$$

3.22 Laat G een *abelse* groep zijn, en $x, y \in G$ twee elementen van eindige orde.

(a) Bewijs: xy heeft eindige orde, en $\text{orde}(xy) \mid \text{kgv}\big(\text{orde}(x), \text{orde}(y)\big)$.

(b) Als $\text{ggd}\big(\text{orde}(x), \text{orde}(y)\big) = 1$, bewijs dat dan $\text{orde}(xy) = \text{orde}(x) \cdot \text{orde}(y)$.

3.23 Laat G een *abelse* groep zijn, en

$$T(G) = \big\{ x \in G \;\big|\; \text{orde}(x) \text{ is eindig} \big\}.$$

Bewijs dat $T(G)$ een ondergroep van G is. Men noemt $T(G)$ de *torsie-ondergroep* van G.

Het volgende vraagstuk toont aan dat de commutativiteit van G essentieel is.

3.24

(a) Definieer de bijecties $\sigma, \tau \colon \mathbb{Z} \mapsto \mathbb{Z}$ door $\sigma(x) = 1 - x$ en $\tau(x) = -x$, voor $x \in \mathbb{Z}$. Bewijs dat σ en τ in de groep $S(\mathbb{Z})$ allebei orde 2 hebben, en dat $\sigma\tau$ oneindige orde heeft.

(b) Bewijs dat elk element van de groep $\text{O}_2(\mathbb{R})$ (zie 1.20) geschreven kan worden als product van hoogstens twee elementen van orde 2, en dat niet elk element van $\text{O}_2(\mathbb{R})$ eindige orde heeft. Bewijs hetzelfde voor de groep $S(X)$, waar X een oneindige verzameling is.

3.25 Laten G_1, G_2 groepen zijn, en $x_1 \in G_1$ en $x_2 \in G_2$ elementen van eindige orde. Zij $x = (x_1, x_2) \in G_1 \times G_2$. Bewijs: $\text{orde}(x)$ is eindig en gelijk aan $\text{kgv}\big(\text{orde}(x_1), \text{orde}(x_2)\big)$.

3.26 Bewijs:

$$Q \ncong D_4, \quad S_4 \ncong D_{12}, \quad A_4 \ncong S_3 \times C_2.$$

3.27 Vind twee niet-isomorfe groepen van 27 elementen, die elk de eigenschap hebben dat $\text{orde}(x) = 3$ voor alle x verschillend van het eenheidselement. (Aanwijzing: Opgave 1.21.)

3.28

(a) Laat p een priemgetal zijn, $a \in \mathbb{Z}$, en $k \in \mathbb{Z}_{\geq 0}$. Bewijs:

$$a^{k(p-1)+1} \equiv a \mod p.$$

(b) Bewijs: $a^{13} - a$ is deelbaar door 2730, voor alle $a \in \mathbb{Z}$.

3.29 (Alternatief bewijs van 3.12). Laat p een priemgetal zijn. Bewijs:

(a) De binomiaalcoëfficiënt $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is deelbaar door p, voor alle $i \in \{1, 2, \ldots, p-1\}$.

(b) Voor alle $a, b \in \mathbb{Z}$ geldt $(a+b)^p \equiv a^p + b^p \mod p$.

(c) Voor alle $n \in \mathbb{Z}$ geldt $n^p \equiv n \mod p$.

3.30 Bewijs:

$$[\mathbb{R}^* : \mathbb{R}_{>0}] = 2; \quad [G : G] = 1; \quad [G : \{e\}] = \#G.$$

3.31 Laat G een groep zijn en $H \subset G$ een ondergroep. Bewijs:

(a) Voor alle $a, b \in G$ geldt: $aH = bH \iff Ha^{-1} = Hb^{-1}$.

(b) Als S een representantensysteem voor de linkernevenklassen van H in G is, dan is $S^{-1} = \left\{ s^{-1} \;\middle|\; s \in S \right\}$ een representantensysteem voor de rechternevenklassen van H in G.

(c) Er geldt $\#(G/H) = \#(H\backslash G)$.

3.32 Stel dat H_1, H_2 ondergroepen van eindige index van een groep G zijn. Bewijs dat $H_1 \cap H_2$ ook eindige index in G heeft.

3.33 Laten H_1, H_2 ondergroepen van een groep G zijn, met $H_1 \subset H_2$. Zij S_1 een representantensysteem voor de linkernevenklassen van H_1 in H_2, en S_2 voor de linkernevenklassen van H_2 in G. Bewijs dat $S = \left\{ s_2 \circ s_1 \;\middle|\; s_1 \in S_1, s_2 \in S_2 \right\}$ een representantensysteem voor de linkernevenklassen van H_1 in G is, en dat $\#S = \#S_1 \cdot \#S_2$. Leid hieruit af dat de eindigheid van G in 3.28 gemist kan worden.

3.34 Deze opgave heeft betrekking op de tabel groepen van orde < 16 (zie na 3.31).

(a) Controleer dat de na de tabel genoemde verzameling B met de daarop gedefinieerde bewerking een groep vormt.

(b) Bewijs de in de tabel voorkomende isomorfieën, en toon aan dat er geen andere isomorfieën tussen in de tabel voorkomende groepen bestaan.

(c) Met welke groep uit de tabel is $C_3 \times C_4$ isomorf?

3.35 Bewijs dat het aantal elementen van orde 2 in een eindige groep van even orde steeds *oneven* is.

3.36 Laat p een priemgetal zijn, en G een eindige groep waarvan de orde deelbaar is door p. Laat k het aantal elementen $x \in G$ van orde p zijn, en l het aantal ondergroepen $H \subset G$ van orde p. Bewijs:

$$\begin{aligned} k &\equiv -1 \mod p, \\ k &= (p-1) \cdot l. \\ l &\equiv 1 \mod p. \end{aligned}$$

3.37 Laat m een geheel getal > 1 zijn dat geen priemgetal is en p een priemgetal is met $p^2 \mid m$. Bewijs dat de groep $G = C_p \times C_{m/p}$ een orde heeft die deelbaar is door m, terwijl er geen $x \in G$ is van orde m.

3.38

(a) Laat G een eindige groep zijn, en $S \subset G$ een deelverzameling met $\#S > \frac{1}{2} \cdot \#G$. Bewijs: $\langle S \rangle = G$. Bewijs ook dat elke $x \in G$ geschreven kan worden als $x = s_1 \cdot s_2$, met s_1, $s_2 \in S$. (Aanwijzing: gegeven $x \in G$, bewijs dat S en $\left\{ xs^{-1} \;\middle|\; s \in S \right\}$ niet disjunct kunnen zijn.)

(b) Laat G een eindige groep van orde > 1 zijn, en $S \subset G$ een deelverzameling met $\#S > \frac{1}{p} \cdot \#G$, waar p de kleinste priemfactor van de orde van G is. Bewijs: $\langle S \rangle = G$.

3.39 Laat G een groep zijn, en $S \subset G$ een deelverzameling met $\langle S \rangle = G$. Laat $H \subset G$ de verzameling elementen zijn die geschreven kunnen worden in de vorm

$$x_1 x_2 \cdots x_m$$

met m *even* en $x_i \in S \cup S^{-1}$ voor $1 \leq i \leq m$ (hier $S^{-1} = \left\{ s^{-1} \;\middle|\; s \in S \right\}$).

(a) Bewijs dat H een ondergroep van G is, en dat $[G : H] = 1$ of 2.

(b) Bewijs: $H = G \iff$ er bestaan $x_1, x_2, \ldots, x_m \in S \cup S^{-1}$ met m *oneven* en $x_1 x_2 \cdots x_m = e$.

(c) Laat $k \in \mathbb{Z}_{>0}$, en laat $H_k \subset G$ de verzameling elementen van de vorm $x_1 x_2 \cdots x_m$, met m deelbaar door k en $x_i \in S \cup S^{-1}$, zijn. Bewijs: $H_k = G$ als k oneven is, en $H_k = H$ als k even is.

3.40 Laat G een groep zijn, en a, $b \in G$ elementen van orde 2.

(a) Bewijs: $a\,b\,a\,b\,a\,b\,a$ heeft orde $2m$ en hetzelfde geldt voor het product van een oneven aantal factoren die afwisselend a en b zijn.

(b) Bewijs: $\big[\langle a, b \rangle : \langle ab \rangle\big] = 2$ (aanwijzing: gebruik Opgave 3.39 en onderdeel (a)).

(c) Bewijs: als orde$(ab) = n < \infty$, dan $\langle a, b \rangle \cong D_n$ (met $D_1 = C_2$) en als orde$(ab) = \infty$ dan $\langle a, b \rangle \cong \langle \sigma, \tau \rangle$, waar σ, $\tau \in S(\mathbb{Z})$ zijn als in Opgave 3.24(a).

3.41 Laat G een eindige groep zijn van orde $2^t k$, met t, $k \in \mathbb{Z}$, k oneven, en stel dat G een element van orde 2^t bevat. Bewijs dat de elementen van G van oneven orde een ondergroep van orde k en index 2^t van G vormen.

3.42 Laat X een oneindige verzameling zijn, en definieer

$$S'(X) = \left\{ \sigma \in S(X) \;\middle|\; \sigma(x) = x \text{ voor bijna alle } x \in X \right\}.$$

Bewijs dat $S'(X)$ een ondergroep van $S(X)$ is, en dat $S'(X)$ een ondergroep van index 2 bezit.

3.43

(a) Bewijs dat onderstaande tabel niet is af te maken tot de vermenigvuldigtabel van een groep van orde 6.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e				
b	b		c	e		
c	c		e	b		
d	d				f	e
f	f				e	d

(b) Stel dat G een groep van orde 6 is die tenminste twee elementen van orde 2 heeft. Bewijs: $G \cong S_3$ (aanwijzing: Opgave 3.40(c)).

(c) Stel dat G een groep van orde 6 is. Bewijs: G is cyclisch of $G \cong S_3$.

Hoofdstuk 4

Normaaldelers, factorgroepen.

Definitie 4.1. Een ondergroep N van een groep G heet een *normaaldeler* of *normale ondergroep* van G als voor alle $g \in G$ en $h \in N$ geldt dat $ghg^{-1} \in N$.

Men gebruikt de notatie $N \triangleleft G$ om aan te geven dat N een normaaldeler van G is.

Voorbeelden 4.2. (a) Is G abels, dan is *elke* ondergroep van G normaaldeler van G.

(b) Elke groep G heeft de "triviale" normaaldelers $\{e\}$ en G.

(c) De alternerende groep A_n is een normaaldeler van S_n: immers, als $\sigma \in S_n$ en $\tau \in A_n$, dan is $\varepsilon(\sigma\tau\sigma^{-1}) = \varepsilon(\sigma)\varepsilon(\tau)\varepsilon(\sigma)^{-1} = \varepsilon(\sigma)\varepsilon(\sigma)^{-1}\varepsilon(\tau) = \varepsilon(\tau) = 1$, dus $\sigma\tau\sigma^{-1} \in A_n$.

(d) De viergroep van Klein $V_4 = \big\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\}$ (vgl. 6.7) is een normaaldeler van S_4. Bewijs hiervan: Laat $\sigma \in S_4$, $\tau \in V_4$. Dan geldt $\tau \in A_4$, dus $\sigma\tau\sigma^{-1} \in A_4$ wegens 4.2(c). Bovendien volgt uit orde$(\tau) \leq 2$ dat orde$(\sigma\tau\sigma^{-1}) \leq 2$. Maar men gaat gemakkelijk na dat de elementen van A_4 van orde ≤ 2 juist de elementen van V_4 zijn. We concluderen dat $\sigma\tau\sigma^{-1} \in V_4$, zoals verlangd.

(e) Laat G een groep zijn. Het *centrum* $Z(G)$ van G is gedefinieerd door

$$Z(G) = \big\{a \in G \;\big|\; ax = xa \text{ voor alle } x \in G\big\}\,.$$

Men gaat gemakkelijk na dat $Z(G)$ een ondergroep van G is. Het is zelfs een normaaldeler van G, want voor elke $g \in G$ en $h \in Z(G)$ geldt $ghg^{-1} = h \in Z(G)$. Op dezelfde wijze ziet men in dat elke ondergroep H van G waarvoor geldt $H \subset Z(G)$ een normaaldeler van G is.

(f) Laat G een groep zijn. Voor g, $h \in G$ is de *commutator* $[g, h]$ gedefinieerd door

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

De naam "commutator" (= "verwisselaar") wordt erdoor verklaard dat $[g, h]$ het element is waarmee men hg moet vermenigvuldigen om gh te krijgen: $gh = [g, h]hg$.

De *commutatorondergroep* van G, notatie: $[G, G]$ of G', is de door alle commutatoren $[g, h]$, met g, $h \in G$, voortgebrachte ondergroep. Dit is een normaaldeler van G, want voor elke $g \in G$ en

$h \in [G,G]$ geldt $ghg^{-1} = [g,h]h \in [G,G]$ (want $[g,h] \in [G,G]$ en $h \in [G,G]$, en $[G,G]$ is een ondergroep). Evenzo bewijst men dat elke ondergroep H van G waarvoor geldt $[G,G] \subset H$ een normaaldeler van G is. We merken op dat niet elk element van $[G,G]$ een commutator hoeft te zijn, zie Opgave 4.27 en: I. M. Isaacs, Commutators and the commutator subgroup, American Mathematical Monthly *84* (1977), 720–722.

De volgende stelling zegt dat een ondergroep en normaaldeler is dan en slechts dan als de linker- en rechternevenklassen samenvallen.

Stelling 4.3. *Laat N een ondergroep van een groep G zijn. Dan geldt:*

$$N \text{ is een normaaldeler van } G \quad \Longleftrightarrow \quad \text{voor alle } a \in G \text{ geldt } aN = Na.$$

Bewijs. $\Rightarrow$: Stel N is normaaldeler van G, en zij $a \in G$. Dan geldt voor elke $h \in N$:

$$ah = (aha^{-1})a \in Na \qquad (\text{omdat } aha^{-1} \in N),$$

dus $aN \subset Na$, en ook

$$ha = a(a^{-1}ha) \in aN \qquad (\text{omdat } a^{-1}ha \in N),$$

dus $Na \subset aN$. We concluderen dat $aN = Na$, zoals verlangd.

$\Leftarrow$: Stel dat $aN = Na$ voor elke $a \in G$, en laat $g \in G$, $h \in N$. Dan geldt $gh \in gN = Ng$, dus $gh = h'g$ voor zekere $h' \in N$. Dus $ghg^{-1} = h' \in N$. Dit betekent dat N een normaaldeler van G is. Hiermee is 4.3 bewezen. □

Uit Stelling 4.3 en Voorbeeld (e) na 3.15 volgt dat voor $n \geq 3$ de ondergroep

$$H = \left\{\sigma \in S_n \;\middle|\; \sigma(1) = 1\right\} \subset S_n$$

geen normaaldeler van S_n is.

Stelling 4.4. *Laat N een ondergroep van G zijn met $[G:N] = 2$. Dan is N een normaaldeler van G.*

Voor een generalisatie van dit resultaat, zie 6.10.

Bewijs. Laat $g \in G$, $h \in N$. We willen bewijzen dat $ghg^{-1} \in N$ Als $g \in N$ is dit duidelijk, want N is een ondergroep. Veronderstel dus dat $g \notin N$. Dan geldt ook $g^{-1} \notin N$, dus $N \neq g^{-1}N$, en omdat N index 2 heeft volgt hieruit $G = N \cup g^{-1}N$. Voorts $hg^{-1} \notin N$ (want $g^{-1} \notin N$), dus hg^{-1} moet tot $g^{-1}N$ behoren: $hg^{-1} = g^{-1}h'$, met $h' \in N$. Dan $ghg^{-1} = h' \in N$, zoals verlangd. □

Tweede bewijs. $[G:N] = 2$ betekent dat N maar twee linkernevenklassen in G heeft; dit moeten dan N en $G - N$ zijn. Wegens Opgave 3.31 zijn er ook maar twee rechternevenklassen van N in G; dit moeten dan tevens N en $G - N$ zijn. De linkernevenklassen zijn dus dezelfde als de rechternevenklassen, en met 4.3 volgt hieruit dat N een normaaldeler van G is. Hiermee is 4.4 bewezen. □

Voorbeelden 4.5. Met behulp van 4.4 zien we opnieuw in dat A_n een normaaldeler van S_n is. Uit 4.4 volgt ook dat

$$\left\{\rho^i \;\middle|\; 0 \leq i < n\right\} \subset D_n$$

(zie 1.21) een normaaldeler van D_n is.

Stelling 4.6. *Laat $f\colon G_1 \to G_2$ een homomorfisme van een groep G_1 naar een groep G_2 zijn. Dan is* $\mathrm{Ker}(f)$ *een normaaldeler van G_1.*

Bewijs. We weten al dat $\mathrm{Ker}(f)$ een ondergroep van G_1 is (Stelling 2.13). Laat nu $g \in G$ en $h \in \mathrm{Ker}(f)$. Dan geldt $f(h) = e_2$ (= eenheidselement van G_2) dus

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(g^{-1}) = f(g)f(g)^{-1} = e_2,$$

met andere woorden: $ghg^{-1} \in \mathrm{Ker}(f)$. Dus $\mathrm{Ker}(f)$ is een normaaldeler van G_1. Dit bewijst 4.6. □

Stelling 4.6 is vaak de gemakkelijkste methode om aan te tonen dat een gegeven ondergroep een normaaldeler is. Beneden (Gevolg 4.12) zullen we zien dat ook de omkering van 4.6 waar is: elke normaaldeler van een groep is de kern van een geschikt gekozen homomorfisme.

Voorbeelden 4.7. (a) Uit $A_n = \mathrm{Ker}(\varepsilon)$ zien we ten derden male in dat A_n een normaaldeler van S_n is.

(b) Laat

$$\mathrm{SL}(2,\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{R}) \;\middle|\; ad - bc = 1 \right\},$$

dan is $\mathrm{SL}(2,\mathbb{R})$ de kern van $\det\colon \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^*$, dus een normaaldeler van $\mathrm{GL}(2,\mathbb{R})$. Analoog definieert men $\mathrm{SL}(n,\mathbb{R})$, voor $n \in \mathbb{Z}_{>0}$; deze groepen heten de *speciale lineaire groepen.*

(c) De ondergroep $\{\pm 1\} \subset Q$ is een normaaldeler; het is namelijk de kern van het in 2.9(e) gedefinieerde homomorfisme.

4.8 Constructie van de factorgroep. Laat G een groep zijn en N een normaaldeler van G. We gaan op de verzameling G/N van (linker-)nevenklassen van N in G een bewerking definiëren die G/N tot een groep maakt. De definitie is volkomen analoog aan degene die we in het geval $\mathbb{Z}/n\mathbb{Z}$ hebben gegeven (Voorbeeld 1.14), behalve dat daar de additieve schrijfwijze gebruikt is.

Laten we kortheidshalve $\overline{a}$ in plaats van aN schrijven, voor $a \in G$. Dus $G/N = \left\{\overline{a} \;\middle|\; a \in G\right\}$, en $\overline{a} = \overline{b} \iff aN = bN \iff a^{-1}b \in N$. We definiëren nu een multiplicatief geschreven bewerking op G/N door

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

waarbij het product ab (onder de streep) in G uitgerekend is. Net als in het geval $\mathbb{Z}/n\mathbb{Z}$ moeten we controleren dat $\overline{ab}$ niet van de keuze van a en b afhangt. D.w.z. als $\overline{a_1} = \overline{a_2}$ en $\overline{b_1} = \overline{b_2}$ dan moeten we nagaan dat $\overline{a_1 b_1} = \overline{a_2 b_2}$. Dit gaat als volgt: uit $\overline{a_1} = \overline{a_2}$ en $\overline{b_1} = \overline{b_2}$ volgt $a_2 = a_1 h$ en $b_2 = b_1 h'$ voor zekere h, $h' \in N$, dus

$$a_2 b_2 = a_1 h b_1 h' = a_1 b_1 \cdot b_1^{-1} h b_1 \cdot h' = a_1 b_1 \cdot h''$$

met $h'' = b_1^{-1}hb_1 \cdot h' \in N$ (omdat $b_1^{-1}hb_1 \in N$ en $h' \in N$). Hieruit volgt $\overline{a_2b_2} = \overline{a_1b_1}$, zoals verlangd. De bewerking op G/N is dus goed gedefinieerd; alleen hiervoor hebben we nodig dat N een *normale* ondergroep van G is.

We gaan na dat G/N met de gedefinieerde bewerking een groep is:

(G1): Dit volgt onmidellijk uit de associativiteit van de bewerking op G, want $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{abc} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$.

(G2): Voor alle $\overline{a} \in G/N$ geldt $\overline{e} \cdot \overline{a} = \overline{a} \cdot \overline{e} = \overline{a}$, dus $\overline{e}$ is een eenheidselement van G/N.

(G3): Voor alle $\overline{a} \in G/N$ geldt $\overline{a} \cdot \overline{a^{-1}} = \overline{a \cdot a^{-1}} = \overline{e}$, en evenzo $\overline{a^{-1}} \cdot \overline{a} = \overline{e}$, dus $\overline{a^{-1}}$ is inverse van $\overline{a}$.

Hiermee is aangetoond dat G/N en groep is. Merk op: als G abels is, is G/N het ook; de omkering hiervan hoeft niet te gelden.

Het volgt onmidellijk uit de definities dat de orde van G/N gelijk is aan $[G : N]$.

Definitie 4.9. De hierboven geconstrueerde groep heet de *factorgroep* of *quotiëntgroep* van G naar N, uitspraak: 'G modulo N', of 'G uitgedeeld naar N'. De afbeelding $\varphi\colon G \to G/N$ gedefinieerd door $\varphi(a) = aN$ $(= \overline{a})$ heet het *natuurlijke* of canonieke homomorfisme van G naar G/N.

Tegen de constructie van de factorgroep kan men ook op de volgende wat concretere manier aankijken. Laat G een groep zijn, $N \subset G$ een normaaldeler, en kies een representantensysteem S voor de (linker-)nevenklassen van N in G. Dan is elk element van G/N op precies één manier te schrijven als $\overline{s}$ $(= sN)$ met $s \in S$:

$$G/N = \left\{ \overline{s} \;\middle|\; s \in S \right\}$$

en $\overline{s} \neq \overline{t}$ als $s \neq t$ (voor $s, t \in S$). We kunnen de elementen van G/N dus met die van S identificeren. Om, in deze schrijfwijze, twee elementen $\overline{s_1}$ en $\overline{s_2}$ van G/N met elkaar te vermenigvuldigen, vermenigvuldigt men eerst de bijbehorende elementen s_1 en s_2 in G, en vervolgens beschouwt men de nevenklasse s_1s_2N waar dit product in ligt. Omdat S een representantensysteem is, ligt er precies één element s_3 van S in deze nevenklasse, en het bijbehorende element $\overline{s_3}$ van G/N is nu het product van $\overline{s_1}$ en $\overline{s_2}$:

$$\overline{s_1} \cdot \overline{s_2} = \overline{s_3}.$$

Voorbeelden 4.10. De voorbeelden (a), (b) en (c) betreffen *additief* geschreven groepen.

(a) Nemen we $G = \mathbb{Z}^+$ en $N = n\mathbb{Z}$, met n een positief geheel getal, dan vinde we de in 1.14 gedefinieerde groep $\mathbb{Z}/n\mathbb{Z}$ terug. Als representantensysteem kunnnen we $S = \{0, 1, \ldots, n-1\}$ nemen, en dit leidt tot

$$G/N = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$$

met de rekenregels

$$\overline{a} + \overline{b} = \begin{cases} \overline{a+b} & \text{als } a+b < n \\ \overline{a+b-n} & \text{als } a+b \geq n, \end{cases}$$

zoals bekend uit 1.14.

(b) Neem $G = \mathbb{R}$ en $N = \mathbb{Z}$. Laat $S = \{s \in \mathbb{R} \mid 0 \leq s < 1\}$. Een willekeurige nevenklasse van N in G is van de vorm

$$x + \mathbb{Z} = \{x + n \mid n \in \mathbb{Z}\}$$

(let op de additieve notatie!), en men ziet direct in dat voor elk reëel getal x deze verzameling precies één element uit S bevat (neem nl. $n = -\lfloor x \rfloor$, dan $x + n \in S$). Dus S is inderdaad een representantensysteem voor de nevenklassen van $\mathbb{Z}$ in $\mathbb{R}$, en

$$\mathbb{R}/\mathbb{Z} = \{\overline{s} \mid s \in \mathbb{R}, 0 \leq s < 1\}.$$

Voor de groepsbewerking in $\mathbb{R}/\mathbb{Z}$ vindt men

$$\begin{aligned} \overline{s_1} + \overline{s_2} &= \overline{s_1 + s_2} && \text{als } s_1 + s_2 < 1 \\ \overline{s_1} + \overline{s_2} &= \overline{s_1 + s_2 - 1} && \text{als } s_1 + s_2 \geq 1, \end{aligned}$$

als s_1, $s_2 \in S$.

(c) (Voor lezers die lineaire algebra kennen.) Laat V een vectorruimte over $\mathbb{R}$ zijn, en $W \subset V$ een deelvectorruimte. Zij W' een *complement* van W in V, d.w.z. een deelvectorruimte met de eigenschap dat elke $v \in V$ eenduidig geschreven kan worden als $v = w + w'$, met $w \in W$, $w' \in W'$. Dan vormt W' een representantensysteem voor de nevenklassen van W in V, dus

$$V/W = \{\overline{x} \mid x \in W'\}.$$

De groepsbewerking in V/W drukt zich uit in deze schrijfwijze erg eenvoudig uit:

$$\overline{x} + \overline{y} = \overline{x + y} \quad (x, y \in W')$$

omdat met x en y ook $x + y$ in W' ligt. We zien dus dat $V/W \cong W'$. Voor generalisaties, zie Opgaven 4.12 en 4.13.

(d) We geven nu een voorbeeld waarin G *niet* commutatief is. Laat $G = S_4$. In 4.2(d) hebben we gezien dat de viergroep van Klein V_4 en normaaldeler van S_4 is. De factorgroep S_4/V_4 is een groep van orde $[S_4 : V_4] = 6$. Deze groep is niet abels: nemen we $\sigma = (1\ 2)$ en $\tau = (1\ 2\ 3)$, en schrijven we $N = V_4 \triangleleft G$, dan is $\sigma N \cdot \tau N = (\sigma\tau)N = (2\ 3)N$ en $\tau N \cdot \sigma N = (\tau\sigma)N = (1\ 3)N$; omdat $(1\ 3)^{-1}(2\ 3) \notin N$ (ga na), vinden we dat $\sigma N \cdot \tau N \neq \tau N \cdot \sigma N$. Volgens hetgeen we in Hoofdstuk 3 gezien hebben (zie de tabel na 3.31 en Opgave 3.43), moet S_4/V_4 dus wel isomorf zijn met S_3.

Om deze conclusie te bewijzen, vatten we S_3 als ondergroep van S_4 op door

$$S_3 = \{\rho \in S_4 \mid \rho(4) = 4\}.$$

Zodadelijk zullen we controleren dat S_3 een representantensysteem is voor de nevenklassen van V_4 in S_4. Als we dat hebben bewezen, volgt

$$S_4/V_4 = \{\overline{\rho} \mid \rho \in S_3\}$$

waarbij de groepsbewerking de volgende eenvoudige vorm aanneemt:

$$\overline{\rho_1} \cdot \overline{\rho_2} = \overline{\rho_1 \rho_2} \qquad (\rho_1, \rho_2 \in S_3).$$

We conluderen dat een isomorfisme

$$S_4/V_4 \xrightarrow{\sim} S_3$$

verkregen wordt door $\overline{\rho}$ op ρ af te beelden.

We bewijzen nu dat S_3 een representantensysteem voor de nevenklassen van V_4 in S_4 is. Zij $\sigma \in S_4$ willekeurig. Uit de definitie van V_4 als ondergroep van S_4 ziet men dat

$$\left\{\tau(4) \;\middle|\; \tau \in V_4\right\} = \{1, 2, 3, 4\}.$$

We kunnen dus $\tau \in V_4$ kiezen met $\tau(4) = \sigma^{-1}(4)$. Voor $\rho = \sigma\tau$ geldt dan $\rho(4) = \sigma(\tau(4)) = \sigma(\sigma^{-1}(4)) = 4$, dus $\rho \in S_3$, en $\rho = \sigma\tau \in \sigma V_4$. Elke nevenklasse van V_4 in S_4 bevat dus een element van S_3. Omdat er zes nevenklassen van V_4 in S_4 zijn, en ook maar zes elementen in S_3, moet iedere nevenklasse in feite precies één element van S_3 bevatten. Hiermee is het bewijs besloten. Zie Opgave 4.13 voor een generalisatie.

Stelling 4.11. *Laat G een groep zijn en N een normaaldeler van G. Dan is het natuurlijke homomorfisme $\varphi\colon G \to G/N$ een surjectief groepshomomorfisme, en* $\mathrm{Ker}(\varphi) = N$.

Bewijs. Surjectiviteit van φ is duidelijk, en uit

$$\varphi(a)\varphi(b) = \overline{a} \cdot \overline{b} = \overline{ab} = \varphi(ab)$$

zien we dat φ een groepshomomorfisme is. Verder geldt dat

$$a \in \mathrm{Ker}(\varphi) \iff \varphi(a) = \varphi(e) \iff aN = eN \iff a \in N$$

dus $\mathrm{Ker}(\varphi) = N$. Dit bewijst 4.11. □

Gevolg 4.12. *Laat G een groep zijn, en $N \subset G$ een deelverzameling. Dan geldt:*

$$N \text{ is een normaaldeler van } G \iff \begin{array}{c}\text{er is een groepshomomorfisme } f \text{ van } G \text{ naar} \\ \text{een groep } G' \text{ waarvoor geldt } \mathrm{Ker}(f) = N.\end{array}$$

Bewijs. $\Leftarrow$: Dit is juist Stelling 4.6.

$\Rightarrow$: Neem $G' = G/N$, en $f = \varphi$; dan geldt wegens 4.11 inderdaad $N = \mathrm{Ker}(\varphi)$. Hiermee is 4.12 bewezen. □

In de volgende stelling beschrijven we alle ondergroepen van G/N.

Stelling 4.13. *Laat G een groep zijn en N een normaaldeler van G. Zij $H \subset G$ een ondergroep met $H \supset N$. Dan is $H/N = \left\{aN \;\middle|\; a \in H\right\}$ een ondergroep van G/N. Omgekeerd is iedere ondergroep van G/N van deze vorm.*

Bewijs. De eenvoudige verificatie dat H/N een ondergroep van G/N is laten we aan de lezer over. Merk op dat de notatie H/N voor deze ondergroep gerechtvaardigd is, d.w.z.: N is een normaaldeler van H, en de factorgroep H/N valt (inclusief de groepsbewerking!) samen met de hier ter sprake zijnde ondergroep van G/N.

Omgekeerd, zij $X \subset G/N$ een ondergroep. Definieer

$$H = \big\{a \in G \;\big|\; \overline{a} \in X\big\} \qquad (\text{met } \overline{a} = aN).$$

Dan controleert men gemakkelijk dat H een ondergroep van G is met $H \supset N$, en dat $X = H/N$. Dus inderdaad is elke ondergroep van G/N van de beschreven vorm. Dit bewijst 4.13. □

Als G een abelse groep is, dan is G/N natuurlijk ook abels, voor elke normaaldeler $N \subset G$. Omgekerd kan G/N best abels zijn zonder dat G het is; voorbeeld: S_3/A_3 heeft twee elementen, en is dus zeker abels, maar S_3 is het niet (ook S_3/S_3 is natuurlijk abels ...). De volgende stelling beschrijft precies wat er aan de hand is; voor de definitie van de commutatorondergroep $[G, G]$ zie 4.2(f).

Stelling 4.14. *Laat G een groep zijn en $N \subset G$ een normaaldeler. Dan geldt: G/N is abels $\iff$ $[G, G] \subset N$. In het bijzonder is $G/[G, G]$ abels.*

Bewijs. We schrijven weer $\overline{a} = aN$, voor $a \in G$. Er geldt:

$$\begin{aligned} G/N \text{ is abels} \quad &\iff \quad \text{voor alle } a, b \in G \text{ geldt } \overline{a}\overline{b} = \overline{b}\overline{a} \\ &\iff \quad \text{voor alle } a, b \in G \text{ geldt } \overline{a}\overline{b}\overline{a}^{-1}\overline{b}^{-1} = \overline{e} \\ &\iff \quad \text{voor alle } a, b \in G \text{ geldt } aba^{-1}b^{-1} \in N \end{aligned}$$

(hier gebruiken we dat $\overline{a}\overline{b}\overline{a}^{-1}\overline{b}^{-1} = \overline{aba^{-1}b^{-1}}$)

$$\iff \quad [G, G] \subset N,$$

want $[G, G]$ is voortgebracht door elementen van de vorm $aba^{-1}b^{-1}$. Dit bewijst 4.14. □

Als voorbeeld berekenen we de commutatorondergroep van S_n en A_n.

Stelling 4.15. *Laat $n \in \mathbb{Z}$, $n > 0$.*

(a) *Er geldt*

$$[S_n, S_n] = A_n.$$

(b) *Er geldt*

$$\begin{aligned} [A_n, A_n] &= \big\{(1)\big\} \qquad \textit{voor } n = 1,\ 2,\ 3, \\ [A_4, A_4] &= V_4 = \big\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\}, \\ [A_n, A_n] &= A_n \qquad \textit{voor } n \geq 5. \end{aligned}$$

Bewijs. (a) Voor $n \leq 2$ is 4.15(a) duidelijk. Laat dus $n \geq 3$. Omdat S_n/A_n twee elementen heeft en dus abels is, geldt $[S_n, S_n] \subset A_n$ wegens 4.14. Verder geldt voor alle $i, j, k \in \{1, 2, \ldots, n\}$ die onderling verschillend zijn:

$$\big[(i\ j), (i\ k)\big] = (i\ j) \circ (i\ k) \circ (i\ j) \circ (i\ k) = (i\ j\ k).$$

Dus $(i\ j\ k) \in [S_n, S_n]$. Omdat A_n wordt voortgebracht door de 3-cykels $(i\ j\ k)$ (Voorbeeld 3.2 en Opgave 3.4) volgt hieruit $A_n \subset [S_n, S_n]$. Einde bewijs van (a).

(b) Voor $n = 1$ of 2 geldt $A_n = \big\{(1)\big\}$, dus ook $[A_n, A_n] = \big\{(1)\big\}$. Omdat A_3 abels is, hebben we $[A_3, A_3] = \big\{(1)\big\}$. Voor $n = 4$ moeten we bewijzen:

$$[A_4, A_4] = V_4.$$

De inclusie $\subset$ volgt weer uit 4.14, want V_4 is normaaldeler van A_4, en A_4/V_4 heeft orde 3 en is daarom abels (zie 3.30). De inclusie $\supset$ volgt uit

$$\big[(1\ 2\ 3), (1\ 2\ 4)\big] = (1\ 2\ 3) \circ (1\ 2\ 4) \circ (1\ 3\ 2) \circ (1\ 4\ 2) = (1\ 2)(3\ 4)$$

en analoge identiteiten voor de andere elementen van V_4.

Laat tenslotte $n \geq 5$. Uit

$$\big[(1\ 2\ 4), (1\ 3\ 5)\big] = (1\ 2\ 4) \circ (1\ 3\ 5) \circ (1\ 4\ 2) \circ (1\ 5\ 3) = (1\ 2\ 3)$$

zien we dat $(1\ 2\ 3) \in [A_n, A_n]$, en op analoge wijze volgt dat $[A_n, A_n]$ alle 3-cykels $(i\ j\ k)$ bevat. Maar deze brengen A_n voort, dus $[A_n, A_n] = A_n$. Hiermee is 4.15 bewezen. □

Opgaven

4.1 Laat $(N_i)_{i \in I}$ een collectie normaaldelers van een groep G zijn. Bewijs dat $\bigcap_{i \in I} N_i$ een normaaldeler van G is.

4.2 Laat G een groep zijn. Bewijs:

$$G \text{ is abels} \quad \Longleftrightarrow \quad Z(G) = G \quad \Longleftrightarrow \quad [G, G] = \{e\}.$$

4.3 Bepaal $Z(G)$ en $[G, G]$ voor $G = S_3$ en $G = D_4$.

4.4 Laat G een groep zijn, $N \subset G$ een normaaldeler, $H \subset G$ een ondergroep, en

$$NH = \big\{nh \;\big|\; n \in N, h \in H\big\}.$$

Bewijs dat NH een ondergroep van G is. Bewijs: als $H \subset G$ een normaaldeler van G is, is NH dat ook.

4.5 Bepaal alle normaaldelers van S_3 en A_4.

4.6 Laat G een groep zijn, en N en M normaaldelers van G waarvoor geldt $N \cap M = \{e\}$.

(a) Bewijs: voor alle $n \in N$ en $m \in M$ geldt $nm = mn$.

(b) Stel dat G wordt voortgebracht door $N \cup M$. Bewijs:

$$G \cong N \times M$$

(aanwijzing: pas 2.27 toe).

4.7 Bewijs dat alle ondergroepen van Q (zie 1.13) normaaldelers zijn, hoewel Q niet abels is. Dus de omkering van 4.2(a) is niet waar.

4.8

(a) Bepaal alle normaaldelers van D_4.

(b) Geef een voorbeeld van een groep G en ondergroepen $H, N \subset G$ waarvoor geldt:

$$\begin{aligned} &H \subset N \subset G, \\ &N \quad \text{is normaaldeler van } G, \\ &H \quad \text{is normaaldeler van } N, \\ &H \quad \text{is } \textit{niet} \text{ normaaldeler van } G. \end{aligned}$$

4.9 Laat G een groep zijn, en $A \subset G$ een eindige deelverzameling, met $n = \#A$. We definiëren:

$$\begin{aligned} H &= \left\{ g \in G \;\middle|\; \text{voor alle } a \in A \text{ is } gag^{-1} \in A \right\}, \\ N &= \left\{ g \in G \;\middle|\; \text{voor alle } a \in A \text{ is } ga = ag \right\}. \end{aligned}$$

Bewijs dat H een ondergroep van G is, en dat N een normaaldeler van H is. Vind een homomorfisme $f\colon H \to S_n$ waarvoor geldt $N = \mathrm{Ker}(f)$.

4.10 Laat H een ondergroep van een groep G zijn, en definieer $N = \bigcap_{g \in G} gHg^{-1}$, waarbij $gHg^{-1} = \left\{ ghg^{-1} \;\middle|\; h \in H \right\}$. Bewijs dat N een normaaldeler van G is die bevat is in H. Bewijs ook dat N de "grootste" normaaldeler van G is die in H bevat is, d.w.z. dat voor elke andere normaaldeler M van G met $M \subset H$ geldt $M \subset N$.

4.11 Laat $U_1 = \left\{ z \in \mathbb{C}^* \;\middle|\; |z| = 1 \right\}$; dit is een ondergroep van $\mathbb{C}^*$, de zgn. *cirkelgroep* (zie Opgave 2.27). Bewijs dat de afbeelding

$$f\colon \mathbb{R}/\mathbb{Z} \to U_1 \quad \text{gegeven door} \quad f(\overline{s}) = e^{2\pi i s} \qquad (s \in \mathbb{R})$$

welgedefinieerd is en dat f een groepsisomorfisme is.

4.12 Laten G_1 en G_2 groepen zijn. Bewijs dat

$$H_1 = G_1 \times \{e_2\} \qquad (e_2 = \text{ eenheidselement van } G_2)$$

een normaaldeler van $G_1 \times G_2$ is, en dat

$$(G_1 \times G_2)/H_1 \cong G_2.$$

4.13 Laat G een groep zijn, $N \subset G$ een normaaldeler, en stel dat er een ondergroep $H \subset G$ is waarvoor geldt

$$\begin{aligned} &HN = G \qquad (\text{met } HN = \left\{hn \;\middle|\; h \in H, n \in N\right\}), \\ &H \cap N = \{e\}. \end{aligned}$$

Bewijs dat H een representantensysteem voor de nevenklassen van N in G vormt, en dat $G/N \cong H$. (Zie Stelling 5.6 voor een generalisatie.)

4.14 Ga na dat de torsie-ondergroep $T(\mathbb{C}^*)$ van $\mathbb{C}^*$ (zie Opgave 3.23) isomorf is met $\mathbb{Q}/\mathbb{Z}$.

4.15 Zij $\mathrm{E}(\mathbb{R}^2)$ de in 1.20 besproken groep van isometrieën van $\mathbb{R}^2$.

(a) Toon aan dat de deelverzameling van alle rotaties rond de oorsprong $\left\{\rho_\varphi \;\middle|\; \varphi \in \mathbb{R}\right\} \subset \mathrm{E}(\mathbb{R}^2)$ wel een ondergroep is, maar niet een normaaldeler. (N.B.: zoals in 1.20 besproken, geldt $\rho_\varphi = \rho_\psi$ als $\varphi - \psi$ een geheel veelvoud van 2π is.)

(b) Bewijs dat de ondergroep van rotaties isomorf is met de cirkelgroep U_1 uit Opgaven 2.27 en 4.11.

(c) Toon aan dat de deelverzameling van alle translaties $T = \left\{t_P \;\middle|\; P \in \mathbb{R}^2\right\} \subset \mathrm{E}(\mathbb{R}^2)$ een normaaldeler is.

(d) Bewijs dat $\mathrm{E}(\mathbb{R}^2)/T$ isomorf is met de orthogonale groep $\mathrm{O}_2(\mathbb{R})$. (Aanwijzing: gebruik Opgave 4.13.)

4.16 Bepaal de structuur van G/N voor de groepen $G = S_3$, Q, D_4 en A_4 en voor elke normaaldeler $N \triangleleft G$.

4.17 Laat G een eindige groep zijn van orde $2^t k$, met $t, k \in \mathbb{Z}$, k oneven, en stel dat G een element van orde 2^t bevat. Volgens Opgave 3.41 is de verzameling elementen van oneven orde een ondergroep N van G. Bewijs dat N een normaaldeler van G is, en dat $G/N \cong C_{2^t}$.

4.18 Bereken $Z(G)$ en $[G, G]$ voor $G = Q$, C_{12}, D_n $(n \geq 3)$ en S_n.

4.19 Bewijs: $Z(\mathbb{H}^*) = \mathbb{R}^*$.

4.20

(a) Bepaal alle $A \in \mathrm{GL}(2,\mathbb{R})$ waarvoor geldt

$$A\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}A \qquad \text{en} \qquad A\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}A.$$

(b) Bepaal $Z\big(\mathrm{GL}(2,\mathbb{R})\big)$ en $Z\big(\mathrm{SL}(2,\mathbb{R})\big)$. (Zie Voorbeeld (b) na 4.6 voor de definitie van $\mathrm{SL}(2,\mathbb{R})$.)

4.21 Laat $G = \mathrm{GL}(2,\mathbb{R})$.

(a) Bewijs: $[G,G] \subset \mathrm{SL}(2,\mathbb{R})$.

(b) Bereken $\left[\, \left(\begin{smallmatrix}x & 0\\ 0 & x^{-1}\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & y\\ 0 & 1\end{smallmatrix}\right) \,\right]$ voor $x \in \mathbb{R}^*$ en $y \in \mathbb{R}$.

(c) Bewijs dat $\mathrm{SL}(2,\mathbb{R})$ wordt voortgebracht door alle matrices van de vorm $\left(\begin{smallmatrix}1 & z\\ 0 & 1\end{smallmatrix}\right)$ of $\left(\begin{smallmatrix}1 & 0\\ z & 1\end{smallmatrix}\right)$, met $z \in \mathbb{R}$.

(d) Bewijs: $[G,G] = \mathrm{SL}(2,\mathbb{R})$. Bepaal ook $\big[\mathrm{SL}(2,\mathbb{R}), \mathrm{SL}(2,\mathbb{R})\big]$.

4.22 Laat $N\colon \mathbb{H}^* \to \mathbb{R}^*$ gedefinieerd zijn door $N(x) = x\overline{x}$ (zie Opgave 1.2).

(a) Bewijs: $[\mathbb{H}^*, \mathbb{H}^*] \subset \mathrm{Ker}(N)]$.

(b) Bewijs dat er voor elke $x \in \mathbb{H}$ een $y \in \mathbb{H}^*$ is met $yx = \overline{x}y$.

(c) Laat $x \in \mathrm{Ker}(N)$ met $x \neq -1$. Bewijs dat er een $y \in \mathbb{H}^*$ bestaat zo dat

$$x = [1 + \overline{x}, y]\,.$$

(d) Bewijs: $[\mathbb{H}^*, \mathbb{H}^*] = \mathrm{Ker}(N) = \big\{x \in \mathbb{H}^* \;\big|\; x\overline{x} = 1\big\}$.

4.23 Laat G een *abelse* groep zijn. In Opgave 3.23 is de torsie-ondergroep $T(G)$ van G gedefinieerd. Bewijs: $T(G/T(G)) = \{\overline{e}\}$ (hierbij is $\overline{e}$ het eenheidselement van $G/T(G)$).

4.24 Laten G_1 en G_2 groepen zijn, en zij $H \subset G_1 \times G_2$ een ondergroep met de eigenschap

$$\text{voor elke } a \in G_1 \text{ is er een } b \in G_2 \text{ met } (a,b) \in H,$$
$$\text{voor elke } b \in G_2 \text{ is er een } a \in G_1 \text{ met } (a,b) \in H,$$

(d.w.z. de projecties $\pi_i\colon G_1 \times G_2 \to G_i$, beperkt tot H, zijn surjectief voor $i = 1, 2$). Definieer

$$N_1 = \big\{a \in G_1 \;\big|\; (a,e_2) \in H\big\},$$
$$N_2 = \big\{b \in G_2 \;\big|\; (e_1,b) \in H\big\}$$

(e_i is het eenheidselement van G_i). Bewijs dat N_1 en normaaldeler van G_1 is, dat N_2 een normaaldeler van G_2 is, en dat $G_1/N_1 \cong G_2/N_2$, met een isomorfisme dat aN_1 op bN_2 afbeeldt als $(a,b) \in H$. Bewijs verder: H is een normaaldeler van $G_1 \times G_2 \iff [G_1 \times G_2, G_1 \times G_2] \subset H$.

4.25 Laat G een groep zijn, en zij N de ondergroep van G voortgebracht door $\{x^2 \mid x \in G\}$. Bewijs dat N een normaaldeler van G is, en dat $[G, G] \subset N$.

4.26 Laat G een groep zijn met de eigenschap dat $G/Z(G)$ cyclisch is. Bewijs dat G abels is (en dus $Z(G) = G$).

4.27 Zij $H \subset \mathbb{H}^+$ de ondergroep

$$\{bi + cj + dk \mid b, c, d \in \mathbb{R}\}$$

en $Q \subset \mathbb{H}^*$ de quaterniongroep (zie 1.13). Laat G de verzameling $H \times Q$ zijn, en definieer op G een bewerking $+$ door

$$(x, \alpha) * (y, \beta) = (x + \alpha y \alpha^{-1}, \alpha\beta)$$

(x, $y \in H$, α, $\beta \in Q$).

(a) Bewijs dat G met de bewerking $*$ een groep is, en dat

$$Z(G) = \{(0, 1), (0, -1)\},$$
$$[G, G] = \{(x, \alpha) \mid x \in H, \alpha \in \{\pm 1\}\}.$$

(b) Laat zien dat het element $(i + j + k, 1) \in [G, G]$ geen commutator is. (Aanwijzing: stel dat $[(x, \alpha), (y, \beta)] = (z, 1)$; dan kan men zonder z te veranderen bereiken dat $\alpha = 1$ of $\beta = 1$ of $\alpha = \beta$.)

(c) Construeer een groep G_1 van orde 216 met de eigenschap

$$[G_1, G_1] \supsetneq \{[g, h] \mid g, h \in G_1\}$$

(aanwijzing: vervang $\mathbb{R}$ door $\mathbb{Z}/3\mathbb{Z}$).

4.28 Vind een voorbeeld van een groep G met normaaldelers N en N' waarvoor geldt

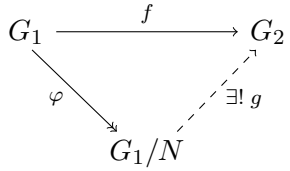
$$N \cong N', \qquad G/N \ncong G/N'.$$

4.29 Bewijs dat $A_n \times C_2 \ncong S_n$, voor $n \geq 3$.

Hoofdstuk 5

Homomorfie- en isomorfiestellingen

Stelling 5.1 (De homomorfiestelling)**.** *Laat $f\colon G_1 \to G_2$ een homomorfisme van een groep G_1 naar een groep G_2 zijn, en $N \subset G_1$ een normaaldeler waarvoor geldt $N \subset \mathrm{Ker}(f)$. Zij $\varphi\colon G_1 \to G_1/N$ het canonieke homomorfisme. Dan is er precies één groepshomomorfisme $g\colon G_1/N \to G_2$ waarvoor geldt $f = g \circ \varphi$. Bovendien geldt $\mathrm{Ker}(g) = \mathrm{Ker}(f)/N \subset G_1/N$.*



Bewijs. We schrijven weer $\overline{a} = aN = \varphi(a)$, voor $a \in G_1$. Definieer $g\colon G_1/N \to G_2$ door $g(\overline{a}) = f(a)$; dit is een goede definitie, want

$$\overline{a_1} = \overline{a_2} \implies a_1^{-1}a_2 \in N \implies a_1^{-1}a_2 \in \mathrm{Ker}(f) \implies f(a_1) = f(a_2)\,.$$

Ook geldt

$$g(\overline{a})g(\overline{b}) = f(a)f(b) = f(ab) = g(\overline{ab}) = g(\overline{a} \cdot \overline{b})$$

dus g is een groepshomomorfisme. Uit

$$g \circ \varphi(a) = g(\varphi(a)) = g(\overline{a}) = f(a) \qquad \text{(voor alle } a \in G_1)$$

blijkt dat $g \circ \varphi = f$. Als ook $g'\colon G_1/N \to G_2$ voldoet aan $g' \circ \varphi = f$, dan

$$g'(\overline{a}) = g'(\varphi(a)) = g' \circ \varphi(a) = f(a) = g(\overline{a}) \qquad \text{(voor alle } a \in G_1)$$

dus $g' = g$. Hieruit blijkt dat g eenduidig bepaald is.

We berekenen tenslotte $\mathrm{Ker}(g)$. Voor $a \in G_1$ geldt

$$\begin{aligned} \overline{a} = aN \in \mathrm{Ker}(g) \quad &\iff \quad g(\overline{a}) = e \in G_2 \\ &\iff \quad f(a) = e \in G_2 \\ &\iff \quad a \in \mathrm{Ker}(f) \\ &\iff \quad aN \in \mathrm{Ker}(f)/N, \end{aligned}$$

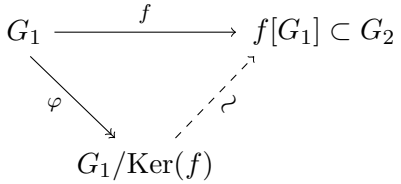
dus $\mathrm{Ker}(g) = \mathrm{Ker}(f)/N$. Dit bewijst 5.1. □

Stelling 5.2 (Eerste isomorfiestelling)**.** *Laat $f\colon G_1 \to G_2$ een homomorfisme van een groep G_1 naar een groep G_2 zijn. Dan geldt*

$$G_1/\mathrm{Ker}(f) \cong f[G_1]$$

met een isomorfie gegeven door

$$a \cdot \mathrm{Ker}(f) \mapsto f(a).$$



Bewijs. We passen Stelling 5.1 toe, met G_2 vervangen door $f[G_1]$ en met $N = \mathrm{Ker}(f)$; dit is inderdaad een normaaldeler van G_1, wegens 4.6. Uit 5.1 volgt dat er een groepshomomorfisme $g\colon G_1/\mathrm{Ker}(f) \to f[G_1]$ is met $g(\overline{a}) = f(a)$, waarbij $\overline{a} = a \cdot \mathrm{Ker}(f)$. Kennelijk is g surjectief. Verder volgt uit 5.1 dat $\mathrm{Ker}(g) = \mathrm{Ker}(f)/N = \mathrm{Ker}(f)/\mathrm{Ker}(f) = \{\overline{e}\} \subset G_1/\mathrm{Ker}(f)$, dus $\mathrm{Ker}(g)$ bestaat alleen uit het eenheidselement van $G_1/\mathrm{Ker}(f)$. Volgens 2.14 is g dus injectief. We concluderen dat g een isomorfisme is. Hiermee is 5.2 bewezen. □

Stelling 5.2 is een van de belangrijkste stellingen uit de groepentheorie. De stelling houdt, slordig gezegd, in, dat het *beeld* van een homomorfisme op isomorfie na door zijn *kern* bepaald is.

Gevolg 5.3. *Laat $f\colon G_1 \to G_2$ een* surjectief *groepshomomorfisme zijn. Dan geldt $G_1/\mathrm{Ker}(f) \cong G_2$.*

Bewijs. Pas 5.2 toe, en merk op dat $f[G_1] = G_2$. Dit bewijst 5.3. □

Voorbeelden 5.4. (a) Definieer $f\colon \mathbb{R} \to \mathbb{C}^*$ door $f(x) = e^{2\pi i x}$. Dit is een groepshomomorfisme, en uit de analyse is bekend dat

$$f[\mathbb{R}] = \big\{ z \in \mathbb{C} \;\big|\; |z| = 1 \big\} \subset \mathbb{C}^*,$$

de cirkelgroep $\mathbb{T}$ (zie Opgave 4.11). Eveneens is uit de analyse bekend dat

$$e^{2\pi i x} = 1 \qquad \Longleftrightarrow \qquad x \in \mathbb{Z}$$

dus $\mathrm{Ker}(f) = \mathbb{Z} \subset \mathbb{R}$. Uit Stelling 5.2 volgt nu $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$, waarmee het resultaat van Opgave 4.11 is teruggevonden.

(b) Zij G een groep, en $x \in G$ een element met $\mathrm{orde}(x) = n < \infty$. Definieer $f\colon \mathbb{Z} \to G$ door $f(m) = x^m$. Dan is g een groepshomomorfisme met

$$f[\mathbb{Z}] = \langle x \rangle \subset G, \qquad \mathrm{Ker}(f) = n\mathbb{Z} \subset \mathbb{Z} \qquad \text{(wegens 3.5)},$$

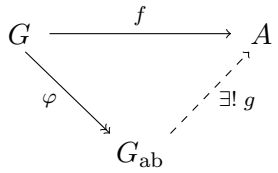
dus 5.2 levert

$$\mathbb{Z}/n\mathbb{Z} \cong \langle x \rangle,$$

zoals we al uit 3.6 wisten.

Met behulp van 5.1 en 5.2 kunnen we een overzicht krijgen over alle homomorfismen van een groep G naar *abelse* groepen. Een voorbeeld van een dergelijk homomorfisme wordt gegeven door de canonieke afbeelding $\varphi\colon G \to G/[G,G]$; men noteert wel $G_{\mathrm{ab}} = G/[G,G]$ en noemt dit de "abels gemaakte G" (vgl. 4.14). De volgende stelling zegt dat *alle* homomorfismen van G naar een abelse groep "via φ lopen".

Stelling 5.5. *Laat G een groep zijn en A een abelse groep. Dan is er voor elk homomorfisme $f\colon G \to A$ een eenduidig bepaald homomorfisme $g\colon G_{\mathrm{ab}} \to A$ waarvoor geldt $f = g \circ \varphi$; hier is $\varphi\colon G \to G_{\mathrm{ab}}$ de canonieke afbeelding.*



Bewijs. Er geldt $G/\mathrm{Ker}(f) \cong f[G]$, en $f[G]$ is, als ondergroep van de abelse groep A, zelf abels. De groep $G/\mathrm{Ker}(f)$ is dus abels, hetgeen volgens 4.14 wil zeggen dat $[G,G] \subset \mathrm{Ker}(f)$. Nu volgen het bestaan en de eenduidigheid van g direct uit Stelling 5.1 (met $N = [G,G]$, $G_1 = G$ en $G_2 = A$). Dit bewijst 5.5. □

Stelling 5.6. *Zij G een groep, $N \subset G$ een normaaldeler, en $H \subset G$ een ondergroep. Dan geldt*

(a) *$H \cap N$ is een normaaldeler van H;*

(b) *$HN = \{hn \mid h \in H, n \in N\}$ is een ondergroep van G;*

(c) (tweede isomorfiestelling): *$H/(H \cap N) \cong HN/N$.*

Bewijs. Laat $\varphi\colon G \to G/N$ de canonieke afbeelding zijn, en zij $\psi\colon H \to G/N$ de beperking van φ tot H; dus $\psi(x) = \varphi(x)$ voor alle $x \in H$. Dan is ψ een groepshomomorfisme, en

$$\mathrm{Ker}(\psi) = \{x \in H \mid \varphi(x) = \overline{e} \in G/N\} = H \cap N.$$

Wegens 4.6 is $H \cap N$ nu een normaaldeler van H. Dit bewijst (a). Bovendien volgt uit 5.2:

$$H/(H \cap N) \cong \psi[H] = \varphi[H]. \qquad (*)$$

Laat $x \in G$. Dan geldt:

$$\begin{aligned} \varphi(x) \in \varphi[H] &\iff \text{er is een } h \in H \text{ met } \varphi(x) = \varphi(h) \\ &\iff \text{er is een } h \in H \text{ met } xh^{-1} \in \mathrm{Ker}(\varphi) = N \\ &\iff \text{er is een } h \in H \text{ met } x \in hN \iff x \in HN\,. \end{aligned}$$

Samenvattend:

$$HN = \{x \in G \mid \varphi(x) \in \varphi[H]\}.$$

Hieruit zien we direct: als x, $y \in HN$, dan ook $xy^{-1} \in HN$. Omdat ook $e \in HN$, volgt nu dat HN een ondergroep van G is (Stelling 2.4). Dit bewijst (b).

Laat $\chi\colon HN \to G/N$ de beperking van φ tot HN zijn. Dan geldt $\mathrm{Ker}(\chi) = N$ en $\chi[HN] = \varphi[H]$. Uit 5.2 volgt dus:

$$HN/N \cong \chi[HN] = \varphi[H].$$

Combineren we dit met (*) dan zien we

$$HN/N \cong \varphi[H] \cong H/(H \cap N).$$

Hiermee is (c) bewezen. Dit bewijst Stelling 5.6. □

Voorbeeld 5.7. Van het resultaat $S_4/V_4 \cong S_3$ uit Hoofdstuk 4 kunnen we met behulp van 5.5 een sneller bewijs geven. Neem $G = S_4$ en laat $H = \{\rho \in S_4 \mid \rho(4) = 4\} = S_3$ en $N = V_4$. Uit $H \cap N = \{(1)\}$ en 5.6(c) volgt dat $S_3/\{(1)\} \cong S_3V_4/V_4$, dus S_4/V_4 bevat een ondergroep (namelijk S_3V_4/V_4) die isomorf met S_3 is. Omdat S_4/V_4 en S_3 beide orde 6 hebben moet deze ondergroep de hele groep zijn, dus $S_4/V_4 \cong S_3$, zoals te bewijzen was. Zie Opgave 5.13 voor een meetkundige interpretatie van de gevonden isomorfie.

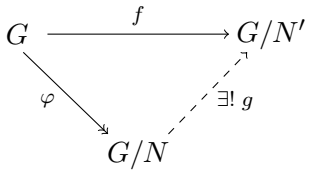
Stelling 5.8. *Laat G een groep zijn en N een normaaldeler van G. Zij $N' \subset G$ een normaaldeler met $N' \supset N$. Dan is N'/N een normaaldeler van G/N. Omgekeerd is iedere normaaldeler van G/N van deze vorm. Tenslotte geldt*

$$(G/N)/(N'/N) \cong G/N'$$

(derde isomorfiestelling).

Bewijs. De eerste twee beweringen van 5.8 worden precies zo bewezen als 4.13, behalve dat men in dit bewijs steeds "normaaldeler" in plaats van "ondergroep" lezen moet.

We geven het bewijs van de isomorfie $(G/N)/(N'/N) \cong G/N'$. Laten $f\colon G \to G/N'$ en $\varphi\colon G \to G/N$ de canonieke afbeeldingen zijn. Omdat $N \subset N' = \mathrm{Ker}(f)$ kunnen we Stelling 5.1 toepassen.



Dit levert een groepshomomorfisme $g\colon G/N \to G/N'$ waarvoor geldt

$$f = g \circ \varphi, \qquad \mathrm{Ker}(g) = \mathrm{Ker}(f)/N = N'/N.$$

Omdat f surjectief is, is g het ook, dus met 5.3 (toegepast op $G_1 = G/N$ en $G_2 = G/N'$, en met g in de plaats van f) vinden we

$$(G/N)/\mathrm{Ker}(g) \cong G/N'.$$

Wegens $\mathrm{Ker}(g) = N'/N$ is hiermee de verlangde isomorfie bewezen. Dit bewijst 5.8. □

Opgaven

5.1 Bewijs $\mathbb{C}^* \cong \mathbb{R}^*_{>0} \times U_1 \cong \mathbb{C}/\mathbb{Z}$. (Ter herinnering U_1 is de cirkelgroep $\{x \in \mathbb{C} || x| = 1\}$).

5.2 Laat G een groep zijn, en N_1, N_2 normaaldelers van G. Definieer $f\colon G \to (G/N_1) \times (G/N_2)$ door $f(a) = (aN_1, aN_2)$.

(a) Bewijs dat f een groepshomomorfisme is, met kern $N_1 \cap N_2$.

(b) Bewijs dat $G/(N_1 \cap N_2)$ isomorf is met een ondergroep van $(G/N_1) \times (G/N_2)$.

5.3 Bewijs $Q/\{1, -1\} \cong V_4$ met behulp van 2.9(e) en 5.3.

5.4 Zij $n \geq 1$ en $G = \{z \in \mathbb{C}^* \mid z^n = 1\}$. Laat zien dat G een normaaldeler in $\mathbb{C}^*$ is, en dat $\mathbb{C}^*/G \cong \mathbb{C}^*$.

5.5 Zij G_1 en G_2 groepen, zij N_1 een normaaldeler van G_1 en zij N_2 een normaaldeler van G_2. Laat zien dat $N_1 \times N_2$ een normaaldeler van $G_1 \times G_2$ is, en dat $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

5.6 Zij G een groep. Zij $x \in G$ van orde $n < \infty$, en $y \in G$ van orde $m < \infty$. Neem aan dat $xy = yx$ en dat $\langle x \rangle \cap \langle y \rangle = \{e\}$. Laat zien dat $\langle x, y \rangle \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. (Hint: beschouw de afbeelding $\mathbb{Z} \times \mathbb{Z} \to G, (a, b) \mapsto x^a y^b$.)

5.7 Laat G, A, n, H, N zijn als in Opgave 4.9. Bewijs dat H/N isomorf is met een ondergroep van S_n.

5.8 Zij G en H groepen en N een normaaldeler in G. Laat zien dat er een bijectie is tussen de verzameling homomorfismen $f\colon G \to H$ met de eigenschap dat $f[N] = \{e\}$, en de verzameling van homomorfismen $G/N \to H$.

5.9 Zij G een groep en A een abelse groep. Laat zien dat er een bijectie is tussen de verzameling van homomorfismen $G \to A$ en de verzameling van homomorfismen $G_{\text{ab}} \to A$.

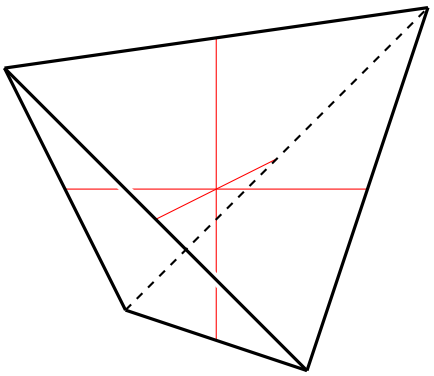
5.10 Bepaal alle groepshomomorfismen $S_n \to \mathbb{C}^*$, voor $n \in \mathbb{Z}$ met $n \geq 2$. Bepaal ook alle groepshomomorfismen $A_n \to \mathbb{C}^*$, voor $n \geq 2$.

5.11 Maak Opgaven 4.12 en 4.13 met behulp van 5.6.

5.12 Vind het isomorfisme $S_4/V_4 \xrightarrow{\sim} S_3$ door Opgaven 4.9 en 5.7 toe te passen met $G = S_4$ en A geschikt gekozen.

5.13 Laat $T \subset \mathbb{R}^3$ een regelmatig viervlak zijn, en zij G de groep van congruenties van $\mathbb{R}^3$ (vlg. 1.16 en Opgave 1.12) die T in zichzelf overvoeren.

(a) Bewijs: $G \cong S_4$. Laat verder X de verzameling zijn waarvan de elementen de drie verbindingslijnstukken van middens van overstaande ribben van T zijn.



(b) Bewijs dat G de elementen van X permuteert, en dat dit aanleiding geeft tot een homomorfisme $f\colon G \to S(X)$.

(c) Bewijs dat f surjectief is en bepaal $\mathrm{Ker}(f)$. Concludeer dat we hiermee een "meetkundige interpretatie" van het isomorfisme $S_4/V_4 \cong S_3$ gevonden hebben.

5.14 Laat $f\colon G_1 \to G_2$ een homomorfisme van groepen zijn, $N_2 \subset G_2$ een normaaldeler en $N_1 = f^{-1}[N_2]$ $(= \{x \in G_1 \mid f(x) \in N_2\})$. Bewijs dat N_1 een normaaldeler van G_1 is. Bewijs verder dat $G_1/N_1 \cong G_2/N_2$ als f surjectief is.

Hoofdstuk 6

Werkingen van groepen

Definitie 6.1. Laat G een groep zijn, en X een verzameling. Een *werking* van G op X is een afbeelding

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

doe voldoet aan

(W0) $e \circ x = x$ voor alle $x \in X$,

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

Opmerking 6.2. In plaats van 'werking' zegt men ook wel 'linkswerking'; een 'rechtswerking' is dan een afbeelding $G \times X \to X$, die we noteren als $(g, x) \mapsto x * g$, waarvoor geldt

$$x * e = x, \quad x * (gh) = (x * g) * h$$

voor alle $x \in X$ en $g, h \in G$. Uit Opgave 6.1 blijkt dat men uit elke rechtswerking op eenvoudige wijze een linkswerking kan verkrijgen. Omgekeerd geeft elke linkswerking aanleiding tot een rechtswerking. Om deze reden beschouwen we verder alleen linkswerkingen.

Als misverstanden uitgesloten zijn schrijft men wel gx in plaats van $g \circ x$.

Voorbeelden 6.3. (a) Laat X een willekeurige verzameling zijn, en $G = S(X)$ (zie 1.16). Dan werkt G op X door $\sigma \circ x = \sigma(x)$, voor $\sigma \in G$, $x \in X$. In het bijzonder werkt S_n op $\{1, 2, \ldots, n\}$, voor $n \in \mathbb{Z}_{>0}$.

(b) Laat G de groep van alle isometrieën van het platte vlak zijn (zie 1.20), en X de verzameling rechthoekige driehoeken in het platte vlak. Een isometrie voert een rechthoekige driehoek weer in een rechthoekige driehoek over, dus G werkt op een voor de hand liggende wijze op X.

(c) Laat G een willekeurige groep zijn. Dan werkt G op zichzelf door $g \circ h = gh$ (de vermenigvuldiging in de groep). Ook werkt G op de verzameling deelverzamelingen van zichzelf door

$$g \circ S = \{gs \mid s \in S\} \qquad \text{voor } S \subset G \text{ en } g \in G.$$

(d) Laat G een groep zijn. Dan werkt G op zichzelf door *conjungatie*:

$$g \circ x = gxg^{-1} \qquad (\text{voor } g,\, x \in G).$$

Het is gemakkelijk na te gaan dat (W0) en (W1) gelden. In dit voorbeeld zou het duidelijk tot misverstanden leiden als we gx in plaats van $g \circ x$ zouden schrijven. De gebruikelijke notatie is

$$^{g}x = gxg^{-1}$$

en (W0), (W1) hebben dan de gedaante:

$$^{e}x = x, \quad ^{gh}x = {}^{g}({}^{h}x) \qquad (\text{voor } g,\, h,\, x \in G).$$

Analoog heeft men de rechtswerking

$$x^{g} = g^{-1}xg$$

van G op zichzelf.

(e) Laat G een groep zijn, $H \subset G$ een ondergroep, en $X = G/H = \{aH \mid a \in G\}$. Dan werkt G op X door

$$g \circ aH = (ga)H \qquad (= \text{de linkernevenklasse van } H \text{ waar } ga \text{ in zit}).$$

Dit is een goede definitie, want als $aH = a'H$, dan geldt $a^{-1}a' \in H$, dus ook $(ga)^{-1} \cdot (ga') = a^{-1}a' \in H$, dus $(ga)H = (ga')H$. Het is gemakkelijk na te gaan dat aan (W0) en (W1) voldaan is. Op analoge wijze definieert men een rechtswerking van G op $H\backslash G$ door $(Ha) * g = H(ag)$.

Stelling 6.4. *Laat de groep G werken op de verzameling X. Dan is voor elke $g \in G$ de afbeelding $\varepsilon_g \colon X \to X$ gegeven door $\varepsilon_g(x) = g \circ x$ bijectief. Bovendien is de afbeelding*

$$f \colon G \to S(X) \qquad \textit{gegeven door } f(g) = \varepsilon_g$$

een groepshomomorfisme.

Bewijs. Er geldt

$$\varepsilon_e(x) = e \circ x = x \qquad \text{voor alle } x \in X$$

wegens (W0); dus $\varepsilon_e = \mathrm{id}_X$. Verder geldt voor alle $g, h \in G$ en $x \in X$:

$$\varepsilon_{gh}(x) = (gh) \circ x = g \circ (h \circ x) = \varepsilon_g\big(\varepsilon_h(x)\big)$$

wegens (W1), dus

$$\varepsilon_{gh} = \varepsilon_g \circ \varepsilon_h. \qquad (*)$$

In het bijzonder geldt

$$\varepsilon_g \circ \varepsilon_{g^{-1}} = \varepsilon_{g^{-1}} \circ \varepsilon_g = \varepsilon_e = \mathrm{id}_X,$$

dus voor elke $g \in G$ heeft ε_g een tweezijdige inverse, d.w.z. is bijectief. Hiermee is de eerste bewering van 6.4 aangetoond.

Omdat ε_g bijectief is geldt $\varepsilon_g \in S(X)$, voor alle $g \in G$. Dus de afbeelding $f \colon G \to S(X)$ gegeven door $f(g) = \varepsilon_g$ is goed gedefinieerd, en $(*)$ drukt precies uit dat f een groepshomomorfisme is.

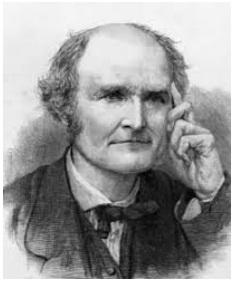
Dit bewijst 6.4. □

Opmerking 6.5. Er geldt ook een omkering van 6.4: is G een groep, X een verzameling, en $f\colon G \to S(X)$ een groepshomomorfisme, dan wordt een werking van G op X gegeven door

$$g \circ x = f(g)\big(x\big)$$

(dit is een zinvolle formule, want $f(g) \in S(X)$, dus $f(g)$ is een afbeelding $X \to X$). Het eenvoudige bewijs laten we aan de lezer over.

Als toepassing van 6.4 bewijzen we de volgende stelling.



Arthur Cayley, Engels wiskundige, 1821-1895

Stelling 6.6 (Stelling van Cayley)**.** *Elke groep G is isomorf met een ondergroep van $S(G)$. Is G een eindige groep, $\#G = n$, dan is G isomorf met een ondergroep van S_n.*

Bewijs. De groep G werkt op zichzelf door $g \circ h = gh$. Wegens 6.4 geeft dit een groepsmorfisme $f : G \to S(G)$. Als $a \in \mathrm{Ker}(f)$, dan is $ah = h$ voor alle $h \in G$ dus in het bijzonder $a = ae = e$, d.w.z. $\mathrm{Ker}(f) = \{e\}$. Volgens 2.14 is f dus injectief.

Het beeld $f[G]$ van f is een ondergroep van $S(G)$ (zie 2.15), en de afbeelding $f\colon G \to f[G]$ is een bijectief homomorfisme. Dus $G \cong f[G]$. Dit bewijst de eerste uitspraak van 6.6. De tweede volgt onmiddellijk, want $S(G) \cong S_n$ als $\#G = n$. □

Voorbeeld 6.7. Passen we de constructie van het bewijs van 6.6 toe op V_4 (zie 1.12), en noemen we de elementen van deze groep 1, 2, 3, 4 in plaats van e, a, b, c dan vinden we

$$V_4 \cong \big\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\} \subset S_4.$$

Dit wordt ook wel als definitie van V_4 genomen.

We kunnen 6.6 ook gebruiken om iets te weten te komen over de normaaldelers van een groep.

Stelling 6.8. *Laat G een groep zijn, en $H \subset G$ een ondergroep van eindige index n. Dan is er een normaaldeler N van G waarvoor geldt:*

$$N \subset H\,, \qquad \mathrm{index}[G : N] \text{ is eindig en deelt } n!.$$

Bewijs. Neem $X = G/H$, en laat G op X werken als in 6.3(e). Merk op dat

$$\#X = \mathrm{index}[G : H] = n,$$

dus $S(X)$ heeft orde $n!$ (Stelling 1.17). Laat $f\colon G \to S(X)$ het groepshomomorfisme uit 6.4 zijn. Dan is $N = \mathrm{Ker}(f)$ een normaaldeler van G (Stelling 4.6). We controleren dat N de verlangde eigenschappen heeft.

Zij $h \in N$ willekeurig. Dan is $f(h)$ het eenheidselement van $S(X)$, d.w.z. $\varepsilon_h = \mathrm{id}_X$, dus $(ha)H = aH$ voor alle $a \in G$. Neem $a = e$; dan zien we $hH = H$, dus $h \in H$. Hiermee is aangetoond dat $N \subset H$.

Aangezien $f[G]$ een ondergroep van $S(X)$ is (Stelling 2.15), met $\#S(X) = n!$, vinden we uit 3.25 dat $\#f[G]$ eindig is en $n!$ deelt. Maar $f[G] \cong G/N$ (Stelling 5.2), dus

$$\#f[G] = \#(G/N) = \mathrm{index}[G : N].$$

Hiermee is 6.8 bewezen. □

Gevolg 6.9. *Laat G een eindige groep zijn, en $H \subset G$ een ondergroep waarvoor geldt*

$$\mathrm{ggd}\big(\#H, (\mathrm{index}[G : H] - 1)!\big) = 1\,.$$

Dan is H een normaaldeler van G.

Bewijs. Volgens 6.8 is er een normaaldeler N van G met $N \subset H$ en $\mathrm{index}[G : N] \mid n!$, waar $n = \mathrm{index}[G : H]$. Er geldt

$$\mathrm{index}[G : N] = \mathrm{index}[G : H] \cdot \mathrm{index}[H : N] = n \cdot \mathrm{index}[H : N].$$

Omdat dit een deler van $n!$ is, volgt dat $\mathrm{index}[H : N]$ een deler is van $(n-1)!$. Ook is $\mathrm{index}[H : N]$ een deler van $\#H$ (Stelling 3.23), dus $\mathrm{index}[H : N]$ deelt $\mathrm{ggd}\big(\#H, (n-1)!\big)$. We concluderen dat $\mathrm{index}[H : N] = 1$; dit wil zeggen dat $N = H$ en H is een normaaldeler van G. Dit bewijst 6.9. □

Gevolg 6.10. *Laat G een eindige groep zijn, en $H \subset G$ een ondergroep waarvoor* $\mathrm{index}[G : H]$ *het kleinste priemgetal is dat $\#G$ deelt. Dan is H een normaaldeler van G.*

Bewijs. Laat $\mathrm{index}[G : H] = p$. Omdat alle priemfactoren van $(p-1)!$ kleiner dan p zijn, is $(p-1)!$ onderling ondeelbaar met $\#G$. Dus zeker $\mathrm{ggd}\big(\#H, (p-1)!\big) = 1$, en uit 6.9 volgt nu dat H een normaaldeler van G is. □

Merk op dat voor eindige groepen, 6.10 een generalisatie is van 4.4.

Laat de groep G werken op de verzameling X. Twee elementen $x, y \in X$ heten *equivalent* onder G, notatie $x \sim_G y$, als er een $g \in G$ is met $g \circ x = y$. De relatie $\sim_G$ is symmetrisch:

$$\begin{aligned} x \sim_G y \quad &\Longrightarrow \quad g \circ x = y \qquad \text{voor een } g \in G \\ &\Longrightarrow \quad x = g^{-1} \circ y \qquad \text{voor een } g \in G \\ &\Longrightarrow \quad y \sim_G x\,. \end{aligned}$$

De relatie is ook reflexief, want $x = e \circ x$, en ze is transitief:

$$\begin{aligned} x \sim_G y \quad \text{en} \quad y \sim_G z \quad &\Longrightarrow \quad \text{er zijn } g, h \in G \text{ zo dat } g \circ x = y \text{ en } h \circ y = z \\ &\Longrightarrow \quad \text{er zijn } g, h \in G \text{ zo dat } (hg) \circ x = z \\ &\Longrightarrow \quad x \sim_G z\,. \end{aligned}$$

Dus $\sim_G$ is inderdaad een equivalentierelatie op X. De equivalentieklassen van $\sim_G$ heten de *banen* van X onder G. Voor $x \in X$ wordt de baan waar x in zit aangegeven met Gx. Er geldt dus

$$Gx = \{g \circ x \mid g \in G\}.$$

Omdat twee verschillende equivalentieklassen steeds disjunct zijn, geldt voor alle $x, y \in X$:

$$\text{óf} \quad Gx = Gy\,, \qquad \text{óf} \quad Gx \cap Gy = \emptyset\,.$$

We zeggen dat G *transitief* op X werkt als er precies één baan van X onder G is.

Definitie 6.11. Laat de groep G werken op de verzameling X, en $x \in X$. De *stabilisator* van x in G, notatie G_x, is

$$G_x = \{g \in G \mid g \circ x = x\}.$$

Opmerking 6.12. Is H een ondergroep van een groep G, en $g \in G$, dan schrijven we

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Het is gemakkelijk na te gaan dat dit weer een ondergroep van G is. We noemen de ondergroepen H en gHg^{-1} *geconjungeerd* in G. Met ziet eenvoudig in dat dit een equivalentierelatie op de verzameling ondergroepen van G is. Kennelijk is H een normaaldeler van G dan en slechts dan als de enige ondergroep van G die met H geconjungeerd is, H zelf is.

Stelling 6.13. *Laat G werken op een verzameling X, en zij $x \in X$. Dan is G_x een ondergroep van G, en voor elke $g \in G$ geldt*

$$G_{g\circ x} = gG_xg^{-1}\,.$$

Bewijs. Er geldt $e \in G_x$, dus $G_x \neq \emptyset$. Voorts, als $g, h \in G_x$, dan geldt $g \circ x = x$ en $h \circ x = x$, dus

$$(gh^{-1}) \circ x = (gh^{-1}) \circ (h \circ x) = (gh^{-1}h) \circ x = g \circ x = x,$$

waaruit volgt dat $gh^{-1} \in G_x$. We concluderen dat G_x een ondergroep van G is.

Laat nu $g \in G$. Dan geldt, voor $a \in G$:

$$\begin{aligned}
a \in G_{g\circ x} &\iff a \circ (g \circ x) = g \circ x \\
&\iff (g^{-1}ag) \circ x = x \\
&\iff g^{-1}ag \in G_x \\
&\iff \text{er is een } h \in G_x \text{ zo dat } g^{-1}ag = h \\
&\iff \text{er is een } h \in G_x \text{ zo dat } a = ghg^{-1} \\
&\iff a \in gG_xg^{-1}
\end{aligned}$$

Hiermee is 6.13 bewezen. □

De "lengte" van een baan Gx kan worden uitgedrukt in de stabilisator G_x:

Stelling 6.14. *Laat G werken op X, en $x \in X$. Dan is de afbeelding $f\colon G/G_x \to Gx$ gegeven door $f(aG_x) = a \circ x$ een welgedefinieerde bijectie. Bijgevolg geldt:*

$$\#Gx = \text{index}[G : G_x]\,.$$

Bewijs. Voor $a, b \in G$ geldt

$$\begin{aligned} aG_x = bG_x &\iff b^{-1}a \in G_x \\ &\iff (b^{-1}a) \circ x = x \\ &\iff a \circ x = b \circ x \end{aligned}$$

Hieruit volgt dat de afbeelding f welgedefinieerd en injectief is. Ook is duidelijk uit de definitie van Gx dat f surjectief is. Dus f is bijectief en $\#Gx = \#G/G_x = \text{index}[G : G_x]$. Dit bewijst 6.14. □

Gevolg 6.15. *Laat G werken op X. Dan geldt*

$$\#X = \sum_{x \in Y} \text{index}[G : G_x],$$

waar $Y \subset X$ een deelverzameling is die uit iedere baan van X onder G precies één element bevat.

Bewijs. Het aantal elementen van X is gelijk aan de som van de aantallen elementen van de diverse banen Gx, met $x \in Y$. Door toepassing van 6.14 volgt hieruit 6.15. □

Voorbeeld 6.16 (Speciaal geval)**.** Stel dat G cyclisch is van orde p, waarbij p een priemgetal is, en laat φ een voortbrenger van G zijn. Voor $x \in X$ zijn er dan twee mogelijkheden: $G_x = \{e\}$ of $G_x = G$, want andere ondergroepen heeft G niet.

Als $G_x = \{e\}$ dan geldt $\text{index}[G : G_x] = p$; dus als we de relatie in 6.15 modulo p beschouwen, vallen de termen met $G_x = \{e\}$ weg. Verder geldt:

$$\begin{aligned} G_x = G &\iff \varphi \in G_x \\ &\iff \varphi(x) = x \\ &\iff \{x\} \text{ is een baan van } X \text{ onder } G. \end{aligned}$$

De relatie in 6.15 levert nu

$$\#X \equiv \#\{x \in X \,:\, \varphi(x) = x\} \mod p.$$

Deze relatie zijn we in Hoofdstuk 3 al in speciale gevallen tegengekomen bij het bewijs van de Stelling van Cauchy 3.32 en bij het tweede bewijs van de Stelling van Fermat 3.33.

Voorbeeld 6.17. Laat G een groep zijn, $X = G$, en laat G op X werken zoals in 6.3(d):

$$^g x = gxg^{-1}.$$

In dit geval heten de banen de *conjungatieklassen* van G, en twee groepselementen heten *geconjungeerd* in G als ze in dezelfde conjungatieklasse zitten. Dus voor $a, b \in G$ geldt:

$$a \text{ en } b \text{ zijn geconjungeerd} \iff \text{er is een } g \in G \text{ zo dat } gag^{-1} = b.$$

De conjungatieklasse waar a in zit bestaat precies uit alle $b \in G$ die met a geconjungeerd zijn. In dit voorbeeld wordt de stabilisator van a de *normalisator* van a genoemd, notatie N_a of N_a^G; dus:

$$N_a = \left\{ g \in G \;\middle|\; {}^g a = a \right\} = \left\{ g \in G \;\middle|\; gag^{-1} = a \right\} = \left\{ g \in G \;\middle|\; ga = ag \right\}.$$

De normalisator van a bestaat dus uit alle groepselementen die met a commuteren. Dit is een ondergroep van G.

Stelling 6.18. *Laat G een eindige groep zijn. Dan wordt voor elke $a \in G$ het aantal elementen van de conjungatieklasse waar a in zit gegeven door* index$[G : N_a]$. *In het bijzonder geldt voor elke conjungatieklasse C van G, dat $\#C$ een* deler *$\#G$ is. Tenslotte geldt de* klasseformule*:*

$$\#G = \sum_{x \in Y} \text{index}[G : N_x],$$

waarbij $Y \subset G$ uit elke conjungatieklasse precies één element bevat.

Bewijs. De eerste bewering van de stelling is, na wat we in Voorbeeld 6.17 gezien hebben, een direct gevolg van 6.14. Dat $\#C = \text{index}[G : N_a]$ een deler van $\#G$ is weten we uit 3.23. De klasseformule is een speciaal geval van 6.15. Dit bewijst 6.18. □

Als toepassing van 6.18 bewijzen we een resultaat dat een belangrijke rol speelt in de theorie van de eindige groepen.

Gevolg 6.19. *Zij G een eindige groep waarvan de orde een macht van een priemgetal p is, $G \neq \{e\}$. Dan geldt $Z(G) \neq \{e\}$.*

Bewijs. Voor elke $x \in G$ is index$[G : N_x]$ een deler van $\#G$, dus een macht van p. Hieruit volgt dat index$[G : N_x]$ òf deelbaar door p, òf gelijk aan 1 is. Verder geldt:

$$\begin{aligned} \text{index}[G : N_x] = 1 \quad &\Longleftrightarrow \quad N_x = G \\ &\Longleftrightarrow \quad gxg^{-1} = x \quad \text{voor alle } g \in G \\ &\Longleftrightarrow \quad x \in Z(G) \end{aligned}$$

Zou $Z(G)$ alleen het eenheidselement bevatten, dan zou index$[G : N_x] = 1$ dus alleen optreden voor $x = e$, en de relatie uit 6.18 zou leveren dat

$$\#G \equiv 1 \mod p,$$

een tegenspraak. Dit bewijst dat $Z(G) \neq \{e\}$, zoals verlangd. □

Uit 6.19 is eenvoudig af te leiden dat elke groep van orde p^2, met p priem, abels is, zie Opgave 6.20. Een preciezer resultaat zullen we langs een andere weg in 7.7(a) bereiken.

We geven een alternatief bewijs van de Stelling van Cauchy 3.32 met behulp van 6.18. Zij p een priemgetal, en G een groep waarvan de orde deelbaar is door p. Met inductie naar $\#G$ bewijzen we dat G een element van orde p heeft. Het geval $\#G = p$ is triviaal (zie 3.30).

Neem eerst aan dat G *abels* is, en kies $a \in G$ met $a \neq e$. Als orde$(a) = k \cdot p$ voor een $k \in Z$, dan heeft a^k orde p. Als $p \nmid$ orde(a), dan is $\#\big(G/\langle a\rangle\big)$ deelbaar door p, dus wegens de inductieveronderstelling heeft $G/\langle a\rangle$ een element $\bar{h} = (h \mod \langle a\rangle)$ van orde p. De orde van h is dan deelbaar door p (zie Gevolg 3.7), dus een geschikte macht van h heeft orde p. Dit besluit het bewijs van 3.32 voor *abelse* G.

Zij G vervolgens *niet-abels*. Dan $Z(G) \subsetneq G$. Als $p \mid \#Z(G)$ dan heeft $Z(G)$, dus ook G, een element van orde p. Stel nu dat $p \nmid \#Z(G)$. We schrijven de klasseformule als volgt:

$$\#G = \#Z(G) + \sum_{x \in Y, x \notin Z(G)} \text{index}[G : N_x]\,.$$

(Vergelijk Opgave 6.7.) Dan zien we dat er een $x \in Y$ met $x \notin Z(G)$ moet zijn waarvoor $p \nmid \text{index}[G : N_x]$. Dan $p \mid \#N_x$, en $\#N_x < \#G$ (want $x \notin Z(G)$), dus uit de inductieveronderstelling volgt dat N_x, en dus ook G, een element van orde p heeft.

Dit besluit het tweede bewijs van 3.32.

Stelling 6.20 (Formule van Burnside)**.** *Laat G een eindige groep zijn die werkt op een eindige verzameling X en duid de verzameling van elementen die door $g \in G$ op zichzelf afgebeeld worden aan met $X^g = \{x \in X | g \circ x = x\}$ (dit zijn de fixpunten van g). Het* aantal *banen van X onder G wordt gegeven door*

$$\#X/G = \frac{1}{\#G} \cdot \sum_{g \in G} \#X^g$$

Bewijs. Beschouw de verzameling van alle mogelijk paren (g, x) waarvoor $gx = x$. Het aantal elementen in deze verzameling kunnen we op 2 manieren tellen. We kunnen voor elke g kijken naar het aantal fixpunten van g of voor elk x naar het aantal $g's$ in de stabilisator van X.

$$\sum_{g \in G} \#X^g = \#\{(g, x) \in G \times X \mid g.x = x\} = \sum_{x \in X} \#G_x.$$

Wegens 6.14 hebben we dat $\#Gx = \text{index}[G : G_x] = \#G/\#G_x$ en dus kunnen we uitdrukking herschrijven als

$$\sum_{g \in G} \#X^g = \#G \sum_{x \in X} \frac{1}{\#Gx}.$$

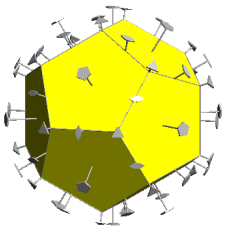
In de laatste som telt elk element mee voor $\frac{1}{\#Gx}$ en dus is de som van de contributies van alle elementen in de baan Gx precies 1. Dit wil zeggen dat deze som het aantal banen telt.

$$\sum_{g \in G} \#X^g = \#G \cdot \#X/G.$$

□

William Burnside, Engels wiskundige, 1852–1927

Voorbeeld 6.21. We bepalen op hoeveel manieren een dodecaeder kan gekleurd worden met twee kleuren op rotatiesymmetrie na.



De symmetrie-assen van een dodecaëder

Aangezien er 12 vlakken zijn die elk op 2 manieren gekleurd kunnen worden zijn er in totaal 2^{12} mogelijkheden: $\#X = 2^{12}$. De rotatiegroep van een dodecaeder is $G = A_5$ en bestaat uit de volgende elementen.

1. De eenheid
   De eenheid houdt alle configuraties vast dus $\#X_g = 2^{12}$

2. 20 rotaties over 120° rond een as die twee hoekpunten verbindt,
   Zo een rotatie permuteert de twaalf vlakken in vier cykels van 3. *Dit wil zeggen dat we in totaal vier kleuren moeten kiezen dus* $\#X_g = 2^4$.

3. 15 rotaties over 180° rond een as die twee middelpunten van ribben verbindt.
   Zo een rotatie permuteert de twaalf vlakken in zes cykels van 2. *Dit wil zeggen dat we in totaal zes kleuren moeten kiezen dus* $\#X_g = 2^6$.

4. 12 rotaties over 72° rond een as die twee middelpunten van vijfhoeken verbindt,
   Zo een rotatie houdt twee vlakken vast en permuteert de andere tien in twee cykels van 5. *Dit wil zeggen dat we in totaal vier kleuren moeten kiezen dus* $\#X_g = 2^4$.

5. 12 rotaties over 144° rond een as die twee middelpunten van vijfhoeken verbindt,
   Zo een rotatie houdt twee vlakken vast en permuteert de andere tien in twee cykels van 5. *Dit wil zeggen dat we in totaal vier kleuren moeten kiezen dus* $\#X_g = 2^4$.

Wanneer we het gewogen gemiddelde nemen van alle $\#X_g$ dan krijgen we

$$\#X/G = \frac{2^{12} + 20 \times 2^4 + 15 \times 2^6 + 12 \times 2^4 + 12 \times 2^4}{60} = 96.$$

Opgaven

6.1 Laat $G \times X \to X, (g, x) \mapsto x * g$, een rechtswerking van een groep G op een verzameling X zijn. Definieer $g \circ x = x * g^{-1}$ voor $g \in G$, $x \in X$. Bewijs dat de afbeelding $G \times X, (g, x) \mapsto g \circ x$, een linkswerking van G op X is.

6.2 Zij G een groep. Zij X en Y verzamelingen. Schrijf $\mathrm{Fun}(X,Y)$ voor de verzameling van functies $f\colon X \to Y$.

(a) Zij $*$ een werking van G op Y. Voor $g \in G$ en $f\colon X \to Y$ definieer $g \bullet f\colon X \to Y$ door $(g \bullet f)(x) := g * f(x)$. Laat zien dat $\bullet$ een groepswerking van G op $\mathrm{Fun}(X,Y)$ definieert.

(b) Zij $*$ een werking van G op X. Voor $g \in G$ en $f\colon X \to Y$ definieer $g \star f\colon X \to Y$ door $(g \star f)(x) := f(g^{-1} * x)$. Laat zien dat $\star$ een groepswerking van G op $\mathrm{Fun}(X,Y)$ definieert.

6.3 Zij G een groep en N een normale ondergroep. Laat zien dat G werkt op N door conjugatie.

6.4 Leid Stelling 4.4 uit Stelling 6.8 af.

6.5 (a) Zij f als in Stelling 6.4. Bewijs: $\mathrm{Ker}(f) = \cap_{x\in X}\, G_x$.
(b) Zij N als in het bewijs van 6.8. Bewijs: $N = \cap_{g\in G}\, gHg^{-1}$.

6.6 Controleer de juistheid van Stelling 6.14 in het geval $X = G/H$ van Voorbeeld 6.3(e), met $x = eH$.

6.7 Zij G een groep, en $a \in G$. Bewijs:

$$a \in Z(G) \Longleftrightarrow N_a = G \Longleftrightarrow \{a\} \text{ is een conjungatieklasse van } G.$$

6.8 Laat $G = \mathrm{SL}_2(\mathbb{R})$ (zie voorbeeld 4.7). Beschouw het zogenaamde 'bovenhalfvlak'

$$\mathcal{H} = \{x + iy \mid x, y \in \mathbb{R}, y > 0\} \subset \mathbb{C}.$$

(a) Laat zien dat G op $\mathcal{H}$ werkt door

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

(b) Bepaal de stabilisator G_z voor $z \in \{i, 2i, e^{\frac{2}{3}\pi i}\}$.

6.9 Zij G een groep, $*_1$ en $*_2$ werkingen van G op verzamelingen X en Y respectievelijk. Voor $g \in G$, $x \in X$ en $y \in Y$ definieer $g * (x,y) := (g *_1 x, g *_2 y)$.

(a) Laat zien dat $*$ een werking van G op $X \times Y$ definieert.

(b) Laat zien dat $G_{(x,y)} = G_x \cap G_y$.

(c) Laat zien dat $(X \times Y)^g = X^g \times Y^g$.

(d) Laat zien dat $G(x,y) \subset Gx \times Gy$. Geef een voorbeeld waarbij de omgekeerde inclusie niet geldt.

6.10 Zij G een *eindige* groep met precies twee conjungatieklassen. Bewijs $\#G = 2$. (Voor een constructie van een *oneindige* groep met precies twee conjungatieklassen zie J.-P. Serre, Arbres Amalgames, SL_2, Astérisque 46 (1977), Ch. I, § 1.4.)

6.11 Laten $\sigma, \tau \in S_n$ twee permutaties zijn, met $n \geq 1$. Bewijs: σ en τ zijn geconjungeerd in S_n dan en slechts dan als σ en τ in hun schrijfwijze als product van disjuncte cykels voor elke $k \in \{1, 2, \ldots, n\}$ evenveel k-cykels hebben (vergelijk Opgave 1.26).

6.12 Laat H een ondergroep van een groep G zijn, en $g \in G$. Bewijs $\mathrm{index}[G : H] = \mathrm{index}[G : gHg^{-1}]$.

6.13 Zij H een ondergroep van een groep G, en

$$N_H = \{g \in G \,:\, gHg^{-1} = H\}$$

(de *normalisator van* H *in* G).

(a) Bewijs dat N_H een ondergroep van G is die H omvat.

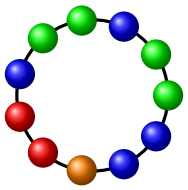
(b) Bewijs dat het aantal met H geconjungeerde ondergroepen van G ten hoogste gelijk is aan $\mathrm{index}[G : H]$.

(c) Stel dat G eindig is, en dat $H \neq G$. Bewijs: $\cup_{g \in G} gHg^{-1} \neq G$.

6.14 Stel dat G een eindige groep is die *transitief* werkt op een verzameling X met $\#X \geq 2$. Bewijs dat er een $g \in G$ bestaat zo dat voor *alle* $x \in X$ geldt $g \circ x \neq x$.

6.15 Laat G transitief werken op X, en zij N een normaaldeler van G. Bewijs dat de banen van X onder N alle even groot zijn; met andere woorden: voor alle x en y in X geldt $\#Nx = \#Ny$.

6.16 Je hebt m kleuren kralen. Van elke kleur heb je een ongelimiteerd aantal. Hoeveel verschillende kralenkettingen kun je maken met 11 kralen? N.B.: Een kralenketting is een ruimtelijk voorwerp.



6.17 Op hoeveel manieren zijn de zijvlakken van een kubus in rood en blauw te kleuren? Hierbij worden twee kleuringen als dezelfde beschouwd waneer er een rotatie van de kubus is die de ene kleuring in de andere voert. Doe dit zowel 'met de hand', als door de stelling van Burnside toe te passen.

6.18 Zij $n \geq 1$. Op hoeveel manieren zijn de zijvlakken van een kubus met n kleuren te kleuren?

6.19 Laat G een groep zijn en $x, y \in G$. Bewijs dat x en y geconjugeerd zijn in G dan en slechts dan als er a, $b \in G$ bestaan zo dat $x = ab$ en $y = ba$.

6.20 Zij G een groep van orde p^2, met p priem. Bewijs dat G *abels* is. (Aanwijzing: 6.19 en Opgave 4.26.)

6.21 Zij G een eindige groep waarvan de orde een macht van een priemgetal p is, en laat X een eindige verzameling zijn waarop G werkt. Definieer $X^G = \{x \in X \mid \text{voor alle } g \in G \text{ geldt } g \circ x = x\}$. Bewijs:

$$\#X \equiv \#X^G \mod p.$$

Hoofdstuk 7

Automorfismen

7.1 Laat G een groep zijn. Zoals we uit 2.7 weten is een *automorfisme* van G een bijectief homomorfisme van G naar zichzelf. De verzameling automorfismen van G wordt aangegeven met $\mathrm{Aut}(G)$; dit is een deelverzameling van $S(G)$ (Voorbeeld 1.16). De identieke afbeelding id_G behoort tot $\mathrm{Aut}(G)$, en uit 2.17 en 2.22 volgt:

$$\begin{aligned} \varphi, \psi \in \mathrm{Aut}(G) &\implies \varphi \circ \psi \in \mathrm{Aut}(G), \\ \varphi \in \mathrm{Aut}(G) &\implies \varphi^{-1} \in \mathrm{Aut}(G). \end{aligned}$$

Dus $\mathrm{Aut}(G)$ is een *ondergroep* van $S(G)$. We noemen $\mathrm{Aut}(G)$ de *automorfismengroep* van G.

Voorbeelden 7.2. (a) Laat $G = V_4 = \{e, a, b, c\}$. Elke permutatie van $\{a, b, c\}$ levert een automorfisme van V_4, dus $\mathrm{Aut}(V_4) \cong S_3$.

(b) De afbeelding $f\colon G \to G$ gegeven door $f(x) = x^{-1}$, is een automorfisme van G dan en slechts dan als G abels is.

In 2.23(e) hebben we gezien dat voor elke groep G en elke $a \in G$ de afbeelding $\varphi_a\colon G \to G, \varphi_a(x) = axa^{-1}$, een automorfisme van G is. Dergelijke automorfismen hadden we *inwendig* genoemd (Engels: inner). De verzameling inwendige automorfismen van G wordt aangegeven met $\mathrm{Inn}(G)$:

$$\mathrm{Inn}(G) = \big\{\varphi_a \;\big|\; a \in G\big\} \subset \mathrm{Aut}(G).$$

Stelling 7.3. *Laat G een groep zijn. Dan is* $\mathrm{Inn}(G)$ *een* normaaldeler *van* $\mathrm{Aut}(G)$*, en*

$$\mathrm{Inn}(G) \cong G/Z(G)$$

waarbij $Z(G)$ het centrum van G aangeeft (zie 4.2(e)*).*

Bewijs. Definieer $f\colon G \to \mathrm{Aut}(G)$ door $f(a) = \varphi_a$. Met een eenvoudige berekening verifieert men dat f een groepshomomorfisme is (dit volgt ook door **??** toe te passen op de in 6.3(d) gedefinieerde werking van G op zichzelf). Het beeld van f is juist $\mathrm{Inn}(G)$, dus wegens 2.15 is $\mathrm{Inn}(G)$ een ondergroep

van $\mathrm{Aut}(G)$. Er geldt

$$\begin{aligned} a \in \mathrm{Ker}(f) &\iff \varphi_a = \mathrm{id}_G \\ &\iff \text{voor alle } x \in G \text{ is } axa^{-1} = x \\ &\iff \text{voor alle } x \in G \text{ is } ax = xa \\ &\iff a \in Z(G) \end{aligned}$$

dus $\mathrm{Ker}(f) = Z(G)$. De isomorfie $\mathrm{Inn}(G) \cong G/Z(G)$ is nu een direct gevolg van de Eerste Isomorfiestelling 5.2.

Om te bewijzen dat $\mathrm{Inn}(G)$ een normaaldeler van $\mathrm{Aut}(G)$ is, is het voldoende aan te tonen dat

$$\psi \circ \varphi_a \circ \psi^{-1} = \varphi_{\psi(a)} \qquad (*)$$

voor alle $\psi \in \mathrm{Aut}(G)$ en $a \in G$. En inderdaad, voor alle $x \in G$ geldt

$$\begin{aligned} \big(\psi \circ \varphi_a \circ \psi^{-1}\big)(x) &= \psi\big(\varphi_a(\psi^{-1}(x))\big) \\ &= \psi\big(a \cdot \psi^{-1}(x) \cdot a^{-1}\big) \\ &= \psi(a) \cdot \psi(\psi^{-1}(x)) \cdot \psi(a^{-1}) \\ &= \psi(a) \cdot x \cdot \psi(a)^{-1} \\ &= \varphi_{\psi(a)}(x) \end{aligned}$$

Hiermee is 7.3 bewezen. □

Voorbeeld 7.4. Laat $G = S_3$. Elk automorfisme van G moet de elementen van orde 2 van G permuteren. Omdat G drie elementen van orde 2 heeft, namelijk (1 2), (1 3) en (2 3), kan dit op niet meer dan $3! = 6$ manieren geschieden. Bovendien is een automorfisme van G volledig bepaald door de manier waarop het deze drie verwisselingen permuteert, want deze drie elementen brengen de hele groep G voort. We concluderen hieruit: G heeft ten hoogste 6 automorfismen. Uit een eenvoudige berekening ziet men dat $Z(G) = \{(1)\}$. Dus de groep $G/Z(G) \cong G = S_3$ heeft 6 elementen, en wegens 7.3 heeft $\mathrm{Inn}(G)$ dus ook 6 elementen. Maar $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$, dus al met al vinden we:

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

Voorbeeld 7.5. Laat $G = \mathbb{Z}/n\mathbb{Z}$, waarbij n een positief geheeld getal is. Omdat G wordt voortgebracht door $\bar{1} = (1 \bmod n)$, wordt elk automorfisme ψ van G volkomen bepaald door $\psi(\bar{1})$:

$$\psi(\bar{k}) = \psi(\underbrace{\bar{1} + \cdots + \bar{1}}_{k \text{ termen}}) = \underbrace{\psi(\bar{1}) + \cdots + \psi(\bar{1})}_{k \text{ termen}} = \bar{k} \cdot \psi(\bar{1})\,.$$

(Let op: de vermenigvuldiging is hier zoals gedefinieerd in 1.15; het is *niet* de groepsbewerking op G, die in dit voorbeeld immers additief geschreven wordt.) Omdat ψ bijectief is, bestaat er een $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ met $\psi(\bar{k}) = \bar{1}$, d.w.z. $\bar{k} \cdot \psi(\bar{1}) = \bar{1}$. Volgens de definitie van $(\mathbb{Z}/n\mathbb{Z})^*$ (zie 1.15) betekent dit precies, dat $\psi(\bar{1}) \in (\mathbb{Z}/n\mathbb{Z})^*$.

We hebben nu bewezen: elk automorfisme ψ van $\mathbb{Z}/n\mathbb{Z}$ is van de vorm

$$\psi(\bar{k}) = \bar{k} \cdot \bar{a} \qquad (*)$$

waarbij $\bar{a}$ $(= \psi(\bar{1}))$ een element van $(\mathbb{Z}/n\mathbb{Z})^*$ is dat alleen van ψ afhangt. We laten het aan de lezer over om te controleren dat omgekeerd voor elke $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ de door $(*)$ gedefinieerde afbeelding een automorfisme van de additieve groep $\mathbb{Z}/n\mathbb{Z}$ is, en tevens dat de afbeelding $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^*$ gegeven door $\psi \mapsto \psi(\bar{1})$ een isomorfisme is. We concluderen:

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^* .$$

De volgende stelling beschrijft een situatie waarin men automorfismen op een natuurlijke manier tegenkomt.

Stelling 7.6. *Laat G een groep zijn en N een normaaldeler van G. Dan is er een groepshomomorfisme $f\colon G \to \mathrm{Aut}(N)$ met $f(a) = \varphi_a|_N$ (de beperking van φ_a tot N) voor alle $a \in G$. Als bovendien N abels is, is er een groepshomomorfisme $g\colon G/N \to \mathrm{Aut}(N)$ met $g(aN) = f(a)$, voor alle $aN \in G/N$.*

Bewijs. Omdat N een normaaldeler is, geldt $\varphi_a[N] \subset N$ voor alle $a \in G$, en het is eenvoudig na te gaan dat $\varphi_a|_N$ een automorfisme van N is (het hoeft *geen* inwendig automorfisme van N te zijn, want a hoeft niet tot N te behoren). Uit $\varphi_{ab} = \varphi_a \circ \varphi_b$ volgt $\varphi_{ab}|_N = (\varphi_a|_N) \circ (\varphi_b|_N)$, voor alle $a, b \in G$, dus de afbeelding $f\colon G \to \mathrm{Aut}(N)$, $f(a) = \varphi_a|_N$, is inderdaad een groepshomomorfisme. Laat nu N abels zijn. Dan geldt $\varphi_a|_N = \mathrm{id}_N$ voor alle $a \in N$, dus $N \subset \mathrm{Ker}(f)$. Wegens 5.1 (de Homomorfiestelling) bestaat er nu een homomorfisme $g\colon G/N \to \mathrm{Aut}(N)$ met $g(aN) = f(a)$, voor alle $a \in N$. Hiermee is 7.6 bewezen. □

Als toepassing van 7.6 bewijzen we een stelling, die impliceert dat groepen waarvan de orde een product van twee priemgetallen is onder bepaalde voorwaarden *abels* zijn.

Stelling 7.7. (a) *Laat p een priemgetal zijn, en G een groep van orde p^2. Dan geldt $G \cong (\mathbb{Z}/p^2\mathbb{Z})$ of $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.*

(b) *Laten p en q priemgetallen zijn met $p > q$, en veronderstel dat q* geen *deler is van $p - 1$. Dan is elke groep G van orde pq* cyclisch*: $G \cong \mathbb{Z}/pq\mathbb{Z}$.*

(Voor het geval dat q een deler is van $p - 1$, zie 7.11 en Opgave 7.12.)

Bewijs. We geven het bewijs van (a) en (b) gelijktijdig. Laat G een groep van orde pq zijn, waarbij we in het geval (a) $q = p$ nemen. Wegens de Stelling van Cauchy 3.32 heeft G een ondergroep H van orde p, en voor deze H geldt $\mathrm{index}[G : H] = q$. Omdat q het kleinste priemgetal is dat $\#G$ deelt volgt uit 6.10 dat H een normaaldeler van G is. Wegens 7.6 is er dus een groepshomomorfisme $g\colon G/H \to \mathrm{Aut}(H)$ waarvoor geldt dat

$$g(aH) = \varphi_a|_H \quad \text{voor alle } a \in G.$$

Omdat H cyclisch van orde p is, zien we uit 7.5, toegepast op $n = p$, dat $\mathrm{Aut}(H) \cong (\mathbb{Z}/p\mathbb{Z})^*$, dus de orde van $\mathrm{Aut}(H)$ is gelijk aan $p - 1$. Nu is enerzijds de orde van het beeld $g[G/H]$ van g een

deler van $\#\mathrm{Aut}(H) = p-1$ (want $g[G/H]$ is een ondergroep van $\mathrm{Aut}(H)$), en anderzijds is het een deler van $\#(G/H) = q$ (want $g[G/H]$ is isomorf met een factorgroep van G/H). Dus $\#g[G/H]$ deelt $\mathrm{ggd}(p-1, q)$. Maar q is een priemgetal dat $p-1$ niet deelt (óók als $q = p$), dus $\mathrm{ggd}(p-1, q) = 1$, en we concluderen dat $g[G/H]$ slechts één element heeft en dus alleen uit het eenheidselement id_H van $\mathrm{Aut}(H)$ bestaat. Krachtens de definitie van g betekent dit:

$$\text{voor alle } a \in G \text{ en } x \in H \text{ geldt: } ax = xa. \tag{§}$$

Kies nu $a \in G$ met $a \notin H$. Dan is aH een voortbrenger van de groep G/H, die orde q heeft, dus orde(a) is deelbaar door q. Hieruit volgt dat de orde van a gelijk is aan q of pq. Als orde$(a) = pq$ dan moet $\langle a\rangle$ gelijk aan G zijn, dus $G = \langle a\rangle \cong \mathbb{Z}/pq\mathbb{Z}$, en we zijn klaar.

Neem dus aan dat a orde q heeft. We bewijzen dat $G \cong \langle a\rangle \times H$ door 2.27 toe te passen op $H_1 = \langle a\rangle$ en $H_2 = H$. Hiertoe moeten we voorwaarden (a), (b) en (c) van 2.27 controleren. Voorwaarde (a) volgt uit (§). Voor (b): als $a^n \in H_1 \cap H_2 = \langle a\rangle \cap H$, dan $(aH)^n = eH$, dus n is deelbaar door orde$(aH) = q$, maar ook orde$(a) = q$, dus $a^n = e$. Voorwaarde (c): deze voorwaarde was in het bewijs van 2.27 alleen nodig om te bewijzen dat het aldaar gedefinieerde groepshomomorfisme $f\colon H_1 \times H_2 \to G$ surjectief is. Dat f injectief is volgt in onze situatie al uit (b), en omdat $H_1 \times H_2$ en G allebei pq elementen hebben moet f ook surjectief zijn.

Hiermee zijn de voorwaarden van 2.27 gecontroleerd, en we concluderen dat $G \cong \langle a\rangle \times H \cong (\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. Als $q \neq p$ geldt verder dat $(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}$ wegens 2.29. Hiermee is 7.7 bewezen. □

De conditie dat q geen deler is van $p-1$ is in 7.7(b) werkelijk nodig; d.w.z., als p en q priemgetallen zijn met $q \mid p-1$, dan bestaat er een niet-commutatieve groep van orde pq. In het geval $p = 3$, $q = 2$ is de groep S_3 zo'n voorbeeld, en algemener is voor $q = 2$ de groep D_p (zie 1.16) een niet-abelse groep van orde pq.

Voor grotere q zullen we zo'n groep in 7.11(a) construeren, als speciaal geval van de constructie van het *semidirecte product*.

Definitie 7.8. Laten H en N twee groepen zijn, en $\tau\colon H \to \mathrm{Aut}(N)$ een groepshomomorfisme. Het *semidirecte product van H met N met betrekking tot τ*, notatie $N \rtimes_\tau H$, is de verzameling $N \times H$ met de volgende groepsbewerking:

$$(n_1, h_1) \cdot (n_2, h_2) = \big(n_1 \cdot \tau(h_1)(n_2), h_1h_2\big) \qquad (n_i \in N, h_i \in H).$$

Als er geen verwarring mogelijk is over welk homomorfisme τ wordt bedoeld, dan wordt het semidirecte product vaak gewoon met $N \rtimes H$ aangegeven. Soms wordt de volgorde van de twee factoren verwisseld; in dit geval schrijft men $H \ltimes_\tau N$ of $H \ltimes N$. (Het is gemakkelijk te onthouden of men $\rtimes$ dient te gebruiken of $\ltimes$, als men bedenkt dat $N \lhd G$ betekent dat N een normaaldeler is.) Merk op dat als τ de triviale afbeelding is die alles op het identiteitsmorfime id_N afbeeldt, dan is semidirecte product gelijk aan het directe product.

Stelling 7.9. *Als H, N twee groepen zijn en $\tau\colon H \to \mathrm{Aut}(N)$ een groepshomomorfisme dan is $N \rtimes_\tau H$ een groep met $\{e_N\} \times H \cong H$ als ondergroep en $\pi : N \rtimes_\tau H \to H : (n, h) \mapsto h$ is een surjectief groepsmorfisme met $N \times \{e_H\} \cong N$ als kern.*

Bewijs. Zie Opgave 7.8. □

Stelling 7.10. *Stel G een groep met twee ondergroepen N, H zodanig dat*

1. *$N \cap H = \{e_G\}$,*
2. *$G = NH$,*
3. *N is een normaaldeler.*

dan is $G \cong N \rtimes_\tau H$ met $\tau(h) : N \to N : n \mapsto hnh^{-1}$.

Bewijs. Zie Opgave 7.9. □

Voorbeelden 7.11. (a) Laten p en q priemgetallen zijn met $q|p-1$. Zij $N = \mathbb{Z}/p\mathbb{Z}$, dan heeft $\mathrm{Aut}(N)$ orde $p-1$ (zie 7.5 en het bewijs van 7.7) dus wegens de Stelling van Cauchy 3.32 is er een ondergroep $H \subset \mathrm{Aut}(N)$ van orde q. Laat $\tau\colon H \to \mathrm{Aut}(N)$ de identieke afbeelding zijn. Dan is het semidirecte product van H met N met betrekking tot τ een groep van orde pq, en deze groep is niet commutatief (zie 7.9(e) en Opgave 7.10).

(b) De groep $D_n = \{1, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \rho\sigma, \ldots, \rho^{n-1}\sigma\}$ (zie 1.21) is isomorf met het semidirecte product van $H = \{1, \sigma\} (\cong \mathbb{Z}/2\mathbb{Z})$ met $N = \{1, \rho, \ldots, \rho^{n-1}\} (\cong \mathbb{Z}/n\mathbb{Z})$ met betrekking tot de afbeelding $\tau\colon H \to \mathrm{Aut}(N)$ gegeven door

$$\tau(1) = \mathrm{id}_N, \quad \tau(\sigma)\colon \rho^i \mapsto \rho^{-i} \quad (\rho^i \in N).$$

(c) Voor elke $n \in \mathbb{Z}_{>1}$ is S_n semidirecte product van een groep van twee elementen (bijvoorbeeld $\{(1), (1\ 2)\}$) met A_n met betrekking tot een geschikte τ. Dit volgt ook uit Opgave 7.9.

We besluiten deze paragraaf met een bespreking van *karakteristieke ondergroepen*. De definitie 4.1 van de normaaldeler kan men ook zo formuleren:

> Een ondergroep N van G is normaaldeler van G als $\varphi[N] = N$ voor alle $\varphi \in \mathrm{Inn}(G)$.

Vervangen we hierin $\mathrm{Inn}(G)$ door $\mathrm{Aut}(G)$ dan krijgen we de definitie van een karakteristieke ondergroep.

Definitie 7.12. Een ondergroep N van een groep G heet *karakteristiek* als voor alle $\psi \in \mathrm{Aut}(G)$ geldt $\psi[N] = N$.

Het volgt direct uit de definitie dat elke karakteristieke ondergroep van G een normaaldeler van G is. De omkering geldt niet: $\{e, a\} \subset V_4$ is normaal (want V_4 is abels), maar niet karakteristiek.

Voorbeelden 7.13. (a) Voor elke groep G zijn $Z(G)$ en $[G, G]$ (zie 4.2(e) en (f)) karakteristieke ondergroepen van G. Dit volgt rechtstreeks uit de definities.

(b) De ondergroep A_3 van S_3 bestaat precies uit de elementen van S_3 die orde 1 of 3 hebben. Hieruit volgt dat A_3 een karakteristieke ondergroep van S_3 is. Dit kan men ook direct afleiden uit $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3)$ (zie 7.4) of uit 7.13(a) en 4.15(a).

Opgaven

7.1 Bewijs: $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

7.2 Bewijs: voor elke $a \in \mathbb{Q}^*$ is de afbeelding $\mathbb{Q} \to \mathbb{Q}$, die x op ax afbeeldt, een automorfisme van de additieve groep $\mathbb{Q}^+$. Bewijs dat omgekeerd elk automorfisme van $\mathbb{Q}^+$ van deze vorm is, voor een eenduidig bepaalde a. Concludeer $\mathrm{Aut}(\mathbb{Q}^+) \cong \mathbb{Q}^*$.

7.3 Laat G een niet-abelse groep zijn. Bewijs: $\#\mathrm{Inn}(G) \geq 4$. (Aanwijzing: Opgave 4.26).

7.4 Laat G een groep zijn met $Z(G) = \{e\}$. Bewijs: $Z(\mathrm{Aut}(G)) = \{\mathrm{id}_G\}$. (Aanwijzing: gebruik $(*)$ uit het bewijs van 7.3.)

7.5 Is $\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z})$ cyclisch? en $\mathrm{Aut}(\mathbb{Z}/16\mathbb{Z})$? Motiveer je antwoorden.

7.6 Laat G een groep zijn. Een *anti-automorfisme* van G is een bijectieve afbeelding $\varphi\colon G \to G$ zo dat voor alle $a, b \in G$ geldt: $\varphi(ab) = \varphi(b)\varphi(a)$. Laat A de verzameling anti-automorfismen van G zijn, en $B = A \cup \mathrm{Aut}(G)$.

(a) Bewijs: $x \mapsto x^{-1}$ is een anti-automorfisme van G.

(b) Bewijs: $A = \mathrm{Aut}(G)$ dan en slechts dan als G abels is.

(c) Stel dat G niet abels is. Bewijs: B is een groep, en $B \cong \mathrm{Aut}(G) \times (\mathbb{Z}/2\mathbb{Z})$.

7.7 Zij G een eindige groep van oneven orde, en N een normaaldeler van G van orde 17. Bewijs: $N \subset Z(G)$. (Aanwijzing: bereken $\mathrm{Aut}(N)$ m.b.v. 7.5, en pas 7.6 toe.)

7.8 Bewijs dat $N \times H$ met de in 7.8 gedefinieerde bewerking inderdaad een groep vormt, met eenheidselement (e, e) en $(n, h)^{-1} = (\tau(h^{-1})(n^{-1}), h^{-1})$ voor $n \in N$, $h \in H$.

7.9 Laat G een groep zijn, $H \subset G$ een ondergroep en $N \subset G$ een normaaldeler. Zij $\tau\colon H \to \mathrm{Aut}(N)$ de beperking tot H van de afbeelding f uit 7.6. Veronderstel dat elke $g \in G$ op precies één manier geschreven kan worden als $g = n \cdot h$, met $n \in N$ en $h \in H$. Bewijs: G is isomorf met het semidirecte product van H met N met betrekking tot τ.

7.10 Zij $G = N \rtimes_\tau H$ een semidirect product als in Definitie 7.8. Bewijs: G is abels dan en slechts dan als H en N allebei abels zijn en $\tau(h) = \mathrm{id}_N$ voor alle $h \in H$.

7.11 Zij $\mathrm{E}(\mathbb{R}^2)$ de in 1.20 besproken groep van isometriën van $\mathbb{R}^2$. Bewijs dat $\mathrm{E}(\mathbb{R}^2) \cong \mathbb{R}^2 \rtimes_\tau \mathrm{O}_2(\mathbb{R})$, waarbij $\tau\colon \mathrm{O}_2(\mathbb{R}) \to \mathrm{Aut}(\mathbb{R}^2)$ de inclusie-afbeelding is. (Vgl. Opgave 4.15.)

7.12 Bij het vak Ringen en Lichamen zullen we bewijzen dat $(\mathbb{Z}/p\mathbb{Z})^*$ *cyclisch* is als p een priemgetal is. Leid hieruit af: als p en q priemgetallen zijn met $q \mid p - 1$, dan is er op isomorfie na slechts één niet-commutatieve groep van orde pq. (Vergelijk 7.11(a).)

7.13 Laat $n \in \mathbb{Z}_{>1}$, en definieer

$$L_n = \{\sigma \in S_n : \exists a, b \in \mathbb{Z} \text{ met } \gcd(a,n) = 1 \text{ en } \sigma(i) = ai + b \mod n \text{ voor } i = 1, 2, \ldots, n\}.$$

Bewijs: L_n is een ondergroep van S_n van orde $n \cdot \varphi(n)$, en L_n is isomorf met het semidirecte product van $(\mathbb{Z}/n\mathbb{Z})^*$ met $\mathbb{Z}/n\mathbb{Z}$ met betrekking tot het isomorfisme $\tau\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ uit 7.5.

7.14 Bepaal alle karakteristieke ondergroepen van de quaternionengroep Q uit 1.13.

7.15 Bewijs dat alle ondergroepen van een cyclische groep karakteristiek zijn.

7.16 Laat G een eindige groep zijn en $N \subset G$ een normaaldeler met de eigenschap $\gcd(\#N, \#(G/N)) = 1$. Bewijs dat $N = \{x \in G : \mathrm{orde}(x) | \#N\}$ en dat N een karakteristieke ondergroep van G is.

7.17 Zij G een groep, en N de ondergroep van G voortgebracht door $\{x^2 : x \in G\}$. Bewijs dat N een karakteristieke ondergroep van G is. (Vergelijk Opgave 4.25)

7.18 (a) Bewijs: als H een karakteristieke ondergroep van N is, en N een karakteristieke ondergroep van G, dan is H ook een karakteristieke ondergroep van G.
(b) Bewijs: als H een karakteristieke ondergroep van N is, en N een normale ondergroep van G, dan is H ook een normale ondergroep van G.
(c) Vind een tegenvoorbeeld tegen (a), met overal 'karakteristiek' vervangen door 'normaal'.

7.19 Laat G een groep zijn met de eigenschap dat $x^2 = e$ voor alle $x \in G$, en veronderstel dat $\#G \geq 4$. Merk op dat G wegens Opgave 1.14 abels is.

(a) Bewijs dat G een ondergroep J bevat met $J \cong V_4$.

(b) Bewijs dat er een ondergroep H van G bestaat met $G \cong V_4 \times H$ (aanwijzing: pas het lemma van Zorn toe op de verzameling ondergroepen H van G met $H \cap J = \{e\}$).

(c) Bewijs: $\#\mathrm{Aut}(G) \geq 6$.

7.20 Laat G een groep zijn met $\mathrm{Aut}(G) = \{\mathrm{id}_G\}$. Bewijs: $\#G \leq 2$. (Aanwijzing: combineer 7.2(b), Opgave (7.3) en Opgave (7.19).)

7.21 Laat G een groep zijn en $N \subset G$ een normaaldeler. Bewijs: als $f\colon G \to \mathrm{Aut}(N)$ de afbeelding uit Stelling 7.6 is, dan is er een homomorfisme $g\colon G/N \to \mathrm{Aut}(N)/\mathrm{Inn}(N)$ met $g(aN) = f(a)\mathrm{Inn}(N)$, voor alle $a \in G$.

7.22 Zij G een groep. Bewijs:

(a) als G cyclisch is, is $\mathrm{Aut}(G)$ abels.

(b) als $\mathrm{Aut}(G)$ cyclisch is, is G abels.

7.23 Laat G een groep zijn, $G' = [G, G]$ en $G'' = [G', G']$ (zie 4.2(f)). Veronderstel dat G'' cyclisch is.

(a) Bewijs: $G'' \subset Z(G')$ (aanwijzing: pas 7.6 toe met $N = G''$).

(b) Stel dat ook G'/G'' cyclisch is. Bewijs: $G'' = \{e\}$.

7.24 Bewijs: $\mathrm{Aut}(Q) \cong S_4$.

7.25 Bewijs dat S_4 isomorf is met het semidirecte product van $\mathrm{Aut}(V_4)$ met V_4 met betrekking tot $\mathrm{id}_{\mathrm{Aut}(V_4)}$.

7.26 Zij G een niet-commutatieve groep die behalve $\{e\}$ en G geen normaaldeler bezit.

(a) Bewijs: $G \cong \mathrm{Inn}(G)$

(b) Bewijs: als $\psi \in \mathrm{Aut}(G)$ en $\psi \circ \varphi = \varphi \circ \psi$ voor alle $\varphi \in \mathrm{Inn}(G)$, dan $\psi = \mathrm{id}_G$.

(c) Bewijs: als N een normaaldeler van $\mathrm{Aut}(G)$ is met $N \cap \mathrm{Inn}(G) = \{\mathrm{id}_G\}$, dan $N = \{\mathrm{id}_G\}$. (Aanwijzing: Opgave 4.6(a).)

(d) Bewijs dat $\mathrm{Inn}(G)$ een karakteristieke ondergroep van $\mathrm{Aut}(G)$ is.

(e) Bewijs: $\mathrm{Aut}(\mathrm{Aut}(G)) = \mathrm{Aut}(\mathrm{Inn}(G)) \cong \mathrm{Aut}(G)$ (vergelijk Opgave 7.4).

Hoofdstuk 8

Eindige abelse groepen

Elke cyclische groep is abels, en hetzelfde geldt voor een directe som van cyclische groepen. De volgende stelling zegt dat omgekeerd elke eindige abelse groep op deze wijze verkregen wordt.

Stelling 8.1. *Laat G een eindige abelse groep zijn. Dan zijn er positieve gehele getallen $d_1, d_2, \ldots, d_t$, met $t \in \mathbb{Z}_{>0}$, zodanig dat*

$$G \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z}).$$

De getallen $d_1, d_2, \ldots, d_t$ kunnen zo gekozen worden, dat bovendien geldt:

$$d_{i+1} \mid d_i \qquad \textit{voor } 1 \leq i < t$$

(dus $d_1 \mid d_2 \mid \cdots \mid d_{t-1} \mid d_t$).

Als we de getallen d_i positief kiezen en zo dat $d_i \mid d_{i+1}$, dan zijn ze eenduidig door G bepaald; zie Opgave 8.6. Voordat we met het bewijs beginnen leiden we enkele hulpresultaten af.

Lemma 8.2. *Laat G een* abelse *groep zijn, en x, $y \in G$ elementen van eindige orde. Veronderstel dat* $\mathrm{orde}(x)$ *en* $\mathrm{orde}(y)$ *onderling ondeelbaar zijn. Dan geldt* $\mathrm{orde}(xy) = \mathrm{orde}(x) \cdot \mathrm{orde}(y)$.

(Vergelijk Opgave 3.22.)

Bewijs. Laat $n = \mathrm{orde}(x)$, $m = \mathrm{orde}(y)$ en $k = \mathrm{orde}(xy)$. We moeten bewijzen dat $k = n \cdot m$. Uit $(xy)^{nm} = x^{nm}y^{nm} = e \cdot e = e$ (want G is abels!) volgt in elk geval dat *nm deelbaar* is door $\mathrm{orde}(xy) = k$.

Wegens $(xy)^k = e$ geldt $e = (xy)^{kn} = x^{kn}y^{kn} = y^{kn}$, dus kn is deelbaar door $\mathrm{orde}(y) = m$. Maar $\mathrm{ggd}(n, m) = 1$, dus k is deelbaar door m. Evenzo ziet men dat k deelbaar is door n. Dus k is deelbaar door $\mathrm{kgv}(n, m) = nm$. We zagen net al dat nm deelbaar is door k, dus $nm = k$, zoals verlangd. Hiermee is 8.2 bewezen. □

Opmerking 8.3. De voorwaarde dat G abels is kan in 8.2 niet worden weggelaten (zie Opgave 8.1).

Lemma 8.4. *Laat G een eindige abelse groep zijn, en $a \in G$ een element waarvan de orde zo groot mogelijk is, d.w.z.*

$$\mathrm{orde}(a) = \max\left\{\mathrm{orde}(x) \;\middle|\; x \in G\right\}.$$

Dan is, voor elke $b \in G$, de orde van b een deler *van de orde van a.*

Bewijs. Laat $b \in G$. Om te bewijzen dat orde(b) een deler is van orde(a), is het voldoende te bewijzen dat voor elke priemgetal p het aantal factoren p in orde(a) groter dan of gelijk aan het aantal factoren p in orde(b) is. Laat p dus een priemgetal zijn, en schrijf orde$(a) = p^i \cdot n$ en orde$(b) = p^j \cdot m$, met $p \nmid n$ en $p \nmid m$. Te bewijzen: $i \geq j$.

Uit orde$(a) = p^i \cdot n$ volgt dat orde$(a^{p^i}) = n$; en uit orde$(b) = p^j \cdot m$ volgt orde$(b^m) = p^j$. Voorts ggd$(n, p^j) = 1$ dus 8.2, toegepast op $x = a^{p^i}$, $y = b^m$, impliceert dat orde$(a^{p^i} \cdot b^m) = n \cdot p^j$. Maar a heeft maximale orde, dus $n \cdot p^j \leq$ orde$(a) = n \cdot p^i$, en hieruit volgt $i \leq j$, zoals verlangd. Dit bewijst 8.4. □

Lemma 8.5. *Laat G een eindige abelse groep zijn en $a \in G$ een element waarvan de orde zo groot mogelijk is. Schrijf $H = \langle a \rangle$, en zij $\varphi\colon G \to G/H$ de canonieke afbeelding. Dan bestaat er voor elke $y \in G/H$ een $x \in G$ waarvoor geldt*

$$\varphi(x) = y \quad \textit{en} \quad \text{orde}(x) = \text{orde}(y).$$

Bewijs. Merk op dat het zinvol is om over de groep G/H te praten, want wegens de commutativiteit van G is elke ondergroep een normaaldeler van G.

Laat $k =$ orde(y), en kies eerst $z \in G$ willekeurig met $\varphi(z) = y$. Wegens 3.7 is orde(z) dan deelbaar door orde$(y) = k$, dus orde$(z) = k\ell$ voor een $\ell \in \mathbb{Z}_{>0}$. Verder is orde(a) wegens 8.4 deelbaar door orde$(z) = k\ell$, dus orde$(a) = k \cdot \ell \cdot m$ voor een $m \in \mathbb{Z}_{>0}$.

Uit $\varphi(z^k) = y^k = \overline{e}$ (het eenheidselement van G/H) blijkt dat $z^k \in \text{Ker}(\varphi) = H = \langle a \rangle$, dus $z^k = a^i$ voor een $i \in \mathbb{Z}$. Nu geldt $a^{i\ell} = z^{k\ell} = e$, dus $i\ell$ is deelbaar door orde$(a) = k\ell m$, en daarom is i deelbaar door km, laten we zeggen $i = jkm$.

Neem nu $x = z \cdot a^{-jm}$. Dan geldt $\varphi(x) = \varphi(z) = y$, en

$$x^k = z^k \cdot a^{-jkm} = a^i \cdot a^{-i} = e,$$

dus orde(x) is een deler van k. Omgekeerd is orde(x) ook deelbaar door $k =$ orde(y), wegens 3.7, dus orde$(x) = k$, zoals verlangd. Dit bewijst 8.5. □

Bewijs van 8.1. Het bewijs wordt gevoerd met volledige inductie naar de orde van G. Als orde$(G) = 1$ is de stelling duidelijk (neem $t = d_1 = 1$; of zelfs $t = 0$). Neem dus aan dat orde$(G) > 1$, en dat de uitspraak van de stelling juist is voor alle abelse groepen van kleinere orde dan G.

Laat $a \in G$ een element van zo groot mogelijke orde zijn. Schrijf $H = \langle a \rangle$, en zij $\varphi\colon G \to G/H$ de canonieke afbeelding. De groep G/H heeft een kleinere orde dan G, dus de inductiehypothese impliceert dat G/H isomorf is met een directe som van cyclische groepen:

$$G/H \cong (\mathbb{Z}/d_2\mathbb{Z}) \times (\mathbb{Z}/d_3\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z}), \qquad (*)$$

waarbij $t, d_2, d_3, \ldots, d_t$ positieve gehele getallen zijn, en $d_{i+1} \mid d_i$ voor $1 < i < t$.

Het isomorfisme $(*)$ betekent, dat er elementen $y_2, y_3, \ldots, y_t \in G/H$ bestaan, met orde$(y_i) = d_i$, zodanig dat elk element van G/H eenduidig kan worden geschreven als $y_e^{e_2} \cdot y_3^{e_3} \cdots y_t^{e_t}$, met $e_i \in \mathbb{Z}$ en $0 \leq e_i < d_i$ (voor $2 \leq i \leq t$).

Wegens 8.5 kunnen we voor elke i een $x_i \in G$ kiezen met $\varphi(x_i) = y_i$ en orde$(x_i) = d_i$. Zij $K \subset G$ de ondergroep voortgebracht door $x_2, x_3, \ldots, x_t$. Omdat G commutatief is, en omdat $x_i^{d_i} = e$, kan elk element van K geschreven worden als $x_2^{e_2} \cdot x_3^{e_3} \cdots x_t^{e_t}$, met $e_i \in \mathbb{Z}$ en $0 \leq e_i < d_i$. Hieruit zien we dat $\#K \leq d_2 \cdot d_3 \cdots d_t = \#(G/H)$. Wegens

$$\varphi\left(x_2^{e_2} \cdot x_3^{e_3} \cdots x_t^{e_t}\right) = y_2^{e_2} \cdot y_3^{e_3} \cdots y_t^{e_t}$$

is de beperking van de afbeelding $\varphi\colon G \to G/H$ tot K surjectief, dus we moeten hebben

$$\begin{aligned} &\#K = \#(G/H), \\ &\text{de afbeelding } \varphi \text{ levert een isomorfisme } K \cong G/H. \end{aligned}$$

In het bijzonder is de beperking van φ tot K *injectief*, dus $K \cap H = \{e\}$. We passen nu de Stelling 2.27 toe op K en H. Voorwaarde (b) van 2.27 hebben we net gecontroleerd, voorwaarde (a) is vervuld omdat G abels is, en voorwaarde (c) bewijst men aldus: omdat de beperking van φ tot K surjectief is, bestaat er voor elke $g \in G$ een $h_1 \in K$ met $\varphi(g) = \varphi(h_1)$, en dan geldt $g = h_1 h_2$ met $h_2 \in \mathrm{Ker}(\varphi) = H$. Uit 2.27 concluderen we nu:

$$G \cong H \times K \cong H \times (G/H).$$

Schrijven we $d_1 = \text{orde}(a)$, dan $H = \langle a \rangle \cong \mathbb{Z}/d_1\mathbb{Z}$ en

$$G \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z}).$$

Wegens 8.4 is orde(a) $(= d_1)$ deelbaar door orde(x_2) $(= d_2)$, d.w.z. $d_2 \mid d_1$. Aangezien we boven al hebben gezien dat $d_{i+1} \mid d_i$ voor $i = 2, 3, \ldots, t-1$ is hiermee Stelling 8.1 volledig bewezen. □

In de rest van deze paragraaf zullen we een veralgemenisering van 8.1 bewijzen voor abelse groepen die door een eindige aantal elementen voortgebracht kunnen worden, zie 8.8. Het volgende hulpresultaat is ook op zichzelf belangrijk.

Stelling 8.6. *Zij n een niet-negatief geheel getal, en laat H een ondergroep van $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$ zijn. Dan geldt $H \cong \mathbb{Z}^k$ voor een $k \in \mathbb{Z}$ met $0 \leq k \leq n$.*

Bewijs. Voor de groepen $\mathbb{Z}$ en $\mathbb{Z}^n$ zullen we in dit bewijs de gebruikelijke *additieve* notatie hanteren. Het bewijs wordt gevoerd met volledige inductie naar n.

Als $n = 0$ dan geldt bij afspraak $\mathbb{Z}^n = \{0\}$, dus ook $H = \{0\} = \mathbb{Z}^0$. Voor $n = 1$ is 8.6 een direct gevolg van 2.6(a).

Laat nu $n > 1$, en zij $H \subset \mathbb{Z}^n$ een ondergroep. Definieer $\pi\colon \mathbb{Z}^n \to \mathbb{Z}$ door $\pi((a_1, a_2, \ldots, a_n)) = a_n$ (projectie op de laatste coördinaat). Dan is π een groepshomomorfisme, en $\pi[H]$ is een ondergroep van $\mathbb{Z}$.

Als $\pi[H] = \{0\}$ dan hebben alle elementen van H de laatste coördinaat gelijk aan nul, dus H kan opgevat worden als ondergroep van $\mathbb{Z}^{n-1}$. De inductiehypothese garandeert in dit geval dat $H \cong \mathbb{Z}^k$ voor een $k \leq n-1$.

Stel vervolgens $\pi[H] \neq \{0\}$. Wegens 2.6(a) is er dan een $m \in \mathbb{Z}_{>0}$ met $\pi[H] = m\mathbb{Z}$. Kies $a \in H$ met $\pi(a) = m$, en definieer

$$H_1 = \left\{h \in H \;\middle|\; \pi(h) = 0\right\}, \qquad H_2 = \langle a \rangle .$$

Omdat a oneindige orde heeft, geldt $H_2 \cong \mathbb{Z}$. Omdat H_1 als ondergroep van $\mathbb{Z}^{n-1}$ opgevat kan worden, impliceert de inductiehypothese dat $H_1 \cong \mathbb{Z}^\ell$ voor een $\ell \in \mathbb{Z}$ met $0 \leq \ell \leq n-1$.

Voor elke $h \in H$ geldt $\pi(h) \in \pi[H] = m\mathbb{Z}$, dus $\pi(h) = j \cdot m$ voor een eenduidig bepaalde $j \in \mathbb{Z}$. Dan geldt $\pi(h) = \pi(h_2)$ voor een eenduidige bepaalde $h_2 \in H_2$, namelijk $h_2 = j \cdot a$. Uit $\pi(h - h_2) = 0$ blijkt dat $h_1 = h - h_2$ tot H_1 behoort. We concluderen dat elke $h \in H$ een eenduidige schrijfwijze $h = h_1 + h_2$ heeft, met $h_1 \in H_1$, $h_2 \in H_2$. Dit impliceert $H \cong H_1 \times H_2$, dus $H \cong \mathbb{Z} \times \mathbb{Z}^\ell \cong \mathbb{Z}^{\ell+1}$ met $1 \leq \ell + 1 \leq n$, zoals verlangd.

Hiermee is de inductiestap voltooid. Dit bewijst 8.6. □

Definitie 8.7. Een groep G heet *eindig voortgebracht* als er een eindige deelverzameling van G is die G voortbrengt.

Stelling 8.8. *Elke eindig voortgebrachte* abelse *groep G is isomorf met het directe product van een aantal* cyclische *groepen.*

Bewijs. Zij $V \subset G$ een eindige deelverzameling die G voortbrengt. In dit bewijs noemen we een eindige deelverzameling $X \subset G$ *lineair onafhankelijk* (over $\mathbb{Z}$) als voor gehele getallen m_x ($x \in X$) geldt:

$$\prod_{x \in X} x^{m_x} = e \quad \Longrightarrow \quad m_x = 0 \text{ voor alle } x \in X.$$

Zij W een lineair onafhankelijke deelverzameling van V waarvan het aantal elementen zo groot mogelijk is. (Het is niet uitgesloten dat dit aantal *nul* is.) Schrijf $W = \{w_1, w_2, \ldots, w_n\}$ en zij $H = \langle W \rangle$ de door W voortgebrachte ondergroep van G. Het groepshomomorfisme

$$\mathbb{Z}^n \to H, \qquad \text{gegeven door} \quad (a_1, a_2, \ldots, a_n) \mapsto \prod_{i=1}^{n} w_i^{a_i}$$

is surjectief, en wegens de lineaire onafhankelijkheid van W ook injectief. Dus $\mathbb{Z}^n \cong H$.

Laat $x \in V - W$. Dan is $W \cup \{x\}$ niet lineair onafhankelijk, dus er is een relatie $x^{m_0} \cdot w_1^{m_1} \cdots w_n^{m_n} = e$ met $m_i \in \mathbb{Z}$, niet alle nul. Omdat W zelf wel lineair onafhankelijk is moet in feite $m_0 \neq 0$. Dan $x^{m_0} = (w_1^{m_1} \cdots w_n^{m_n})^{-1} \in H$, waarmee is bewezen dat er voor elke $x \in V - W$ een $m_0 \in \mathbb{Z} - \{0\}$ bestaat zo dat $x^{m_0} \in H$. (Natuurlijk hangt m_0 hier van x af.) Laat m het product van al de getallen m_0 zijn, waarvij x de verzameling $V - W$ doorloopt (met $m = 1$ als $V = W$). Dan geldt $m \neq 0$, en $x^m \in H$ voor alle $x \in V - W$. Natuurlijk geldt ook $x^m \in H$ voor alle $x \in W$; dus het geldt voor alle $x \in V$. Omdat V de hele groep voortbrengt concluderen we dat $x^m \in H$ geldt voor *alle* $x \in G$.

Definieer het groepshomomorfisme $\varphi\colon G \to H$ door $\varphi(c) = x^m$. Dan is $\varphi[G]$ een ondergroep van H, en $H \cong \mathbb{Z}^n$, dus wegens 8.6 geldt $\varphi[G] \cong \mathbb{Z}^k$ voor zeker $k \leq n$. Dit wil zeggen dat er $x_1, x_2, \ldots, x_k \in G$ zijn zodanig dat $\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_k)$ een lineair onafhankelijk stelsel voortbrengers voor $\varphi[G]$ is. Definieer nu

$$H_1 = \mathrm{Ker}(\varphi) \quad \text{en} \quad H_2 = \langle x_1, x_2, \ldots, x_k \rangle .$$

Omdat $\{\varphi(x_1), \ldots, \varphi(x_k)\}$ onafhankelijk is, is $\{x_1, x_2, \ldots, x_k\}$ het ook, dus $H_2 \cong \mathbb{Z}^k$, en φ induceert een isomorfisme $H_2 \cong \varphi[G]$. Voor elke $g \in G$ is er precies één $h_2 \in H_2$ met $\varphi(g) = \varphi(h_2)$, en dan geldt $g = h_1 h_2$ met $h_1 \in \mathrm{Ker}(\varphi) = H_1$. Dus elke $g \in G$ is eenduidig te schrijven als $g = h_1 h_2$, met $h_1 \in H_1$ en $h_2 \in H_2$, en dit impliceert

$$G \cong H_1 \times H_2.$$

We weten al dat H_2 een direct product van cyclische groepen is: $H_2 \cong \mathbb{Z}^k$. We moeten nu nog H_1 behandelen.

Er geldt dat $H_1 \cong G/H_2$, dus H_1 is evenals G eindige voortgebracht, zeg $H_1 = \langle z_1, z_2, \ldots, z_t \rangle$. Elk element van H_1 kan dus geschreven worden als $\prod_{i=1}^{t} z_i^{k_i}$ met $k_i \in \mathbb{Z}$. Maar uit $z_i \in H = \mathrm{Ker}(\varphi)$ blijkt dat $z_i^m = \varphi(z_i) = e$, dus we mogen annemen dat geldt $0 \leq k_i < |m|$, voor $i = 1, 2, \ldots, t$. Dan zijn er nog maar eindig veel mogelijkheden voor $k_1, k_2, \ldots, k_t$ overgebleven, dus de abelse groep H_1 is *eindig*. Uit 8.1 volgt nu dat H_1 isomorf is met het product van een eindig aantal cyclische groepen.

Hiermee is 8.8 bewezen. □

Opmerking 8.9. De classificatie van eindige abelse groepen heeft dus een eenvoudige oplossing: elke eindige abelse groep is het direct product van cyclische groepen. Door de Chinese reststelling 2.24 kunnen we ons beperken tot cyclische groepen waarvan de orde een priemmacht is, want elke cyclische groep waarvan de orde het product is van twee onderling ondeelbare getallen kunnen we als een product van kleinere cyclische groepen. We hebben dus een aantal bouwstenen (cyclische groepen van de vorm $\mathbb{Z}/p^n\mathbb{Z}$) en een methode om van kleinere groepen grotere te maken (het direct product) en die volstaan om alle eindige abelse groepen te maken.

Stelling 8.10. *Stel G een eindige abelse groep met orde $n = p_1^{n_1} \cdots p_k^{n_k}$ dan bestaan er partities $n_1 = m_{1,1} + \cdots + m_{1,r_1}$, …, $n_k = m_{k^1} + \cdots + m_{k,r_k}$ zodanig dat*

$$G \cong \mathbb{Z}/p_1^{m_{1,1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{m_{1,r_1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{m_{k,1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{m_{k,r_k}}\mathbb{Z}$$

Deze ontbinding is uniek op herordening van de factoren na.

Bewijs. Gebruik stelling 8.1 om G te schrijven als een product van cyclische groepen. Gebruik dan de Chinese reststelling 2.24 om elke cyclische groep te schrijven als een product van cyclische groepen met ordes die priemmachten zijn. Aangezien de orde van een direct product het product van de ordes is moet het product van al deze priemmachten gelijk zijn aan de orde van G. De uniciteit volgt uit opgave 8.6. □

Gevolg 8.11. *Het aantal eindige abelse groepen met orde $p_1^{n_1} \cdots p_k^{n_k}$ op isomorfie na is*

$$P_{n_1} \times \cdots \times P_{n_k}$$

waarbij P_n het aantal partities van n is.

Opmerking 8.12. Kunnen we iets gelijkaardigs doen voor niet abelse groepen? Hier duiken twee problemen op, welke bouwstenen moeten we gebruiken en op welke manieren kunnen we die aan 'elkaar plakken'. Om het aantal bouwstenen te beperken maken we best gebruik van meer geavanceerde

plakmethoden dan enkel het direct product. Een mogelijkheid om is om ook semidirecte producten toe te laten, maar zelfs als we dat doen is het een hopeloze taak om alle groepen te bepalen die niet het semidirect product zijn van kleinere groepen.

Om de classificatie zo eenvoudig mogelijk te maken moeten we 'plakken' dus zo ruim mogelijk interpreteren: we zeggen dat G een extensie is van een groep Q met een groep N als $N \lhd G$ en $G/N \cong Q$. In deze interpretatie zijn de bouwstenen groepen die geen niet-triviale normaaldelers hebben: de simpele groepen. In de jaren 60-80 van de vorige eeuw werd hier heel veel onderzoek naar gedaan en uiteindelijk is men er in geslaagd om een complete classificatie te geven van alle eindige simpele groepen. Een overzicht hiervan kan je vinden op het einde van de syllabus.

Opgaven

8.1 Bewijs dat de groep S_3 elementen x en y bevat waarvoor geldt:

$$\mathrm{ggd}\big(\mathrm{orde}(x), \mathrm{orde}(y)\big) = 1, \quad \mathrm{orde}(xy) \neq \mathrm{orde}(x) \cdot \mathrm{orde}(y).$$

8.2 Bewijs dat elke eindige abelse groep G geschreven kan worden als

$$G \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z}),$$

waarbij $p_1, p_2, \ldots, p_r$ priemgetallen zijn en $k_1, k_2, \ldots, k_r \in \mathbb{Z}^{\geq 0}$.

8.3 Schrijf elk van de volgende groepen als product van een eindig aantal cyclische groepen:

$$V_4, \quad (\mathbb{Z}/21\mathbb{Z})^*, \quad (\mathbb{Z}/35\mathbb{Z})^*, \quad (\mathbb{Z}/40\mathbb{Z})^*.$$

Opmerking: Bij het vak Ringen en Lichamen zullen we zien hoe in het algemeen de groep $(\mathbb{Z}/n\mathbb{Z})^*$ als product van cyclische groepen geschreven kan worden.

8.4 Zij G een eindige abelse groep waarvan de orde *kwadraatvrij* is, d.w.z. niet deelbaar door het kwadraat van een geheel getal groter dan 1. Bewijs dat G cyclisch is.

8.5 Bepaal voor $n = 43, 143, 243, 343$ het aantal abelse groepen van orde n, op isomorfie na.

8.6

(a) Zij $G \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z})$, laat p een priemgetal zijn, $k \in \mathbb{Z}_{>0}$, en definieer:

$$H_1 = \left\{ x^{p^{k-1}} \;\middle|\; x \in G \right\}, \qquad H_2 = \left\{ x^{p^k} \;\middle|\; x \in G \right\}.$$

Bewijs: H_1 en H_2 zijn ondergroepen van G met $H_2 \subset H_1$, en $\#(H_1/H_2) = p^u$, waarbij u het aantal indices i is waarvoor d_i deelbaar is door p^k.

(b) Bewijs dat $d_1, d_2, \ldots, d_t$ in Stelling 8.1 eenduidig door G bepaald zijn, als we bovendien eisen dat $d_i > 1$ voor $1 \leq i \leq t$.

8.7 Stel dat $\mathbb{Z}^k \cong \mathbb{Z}^\ell$, met $k, \ell \in \mathbb{Z}_{\geq 0}$. Bewijs: $k = \ell$.

8.8* Laat $H \subset \mathbb{Z}^n$ een ondergroep zijn, en $H \cong \mathbb{Z}^k$, met $k, n \in \mathbb{Z}_{\geq 0}$, $k \leq n$.

(a) Bewijs: $k = n \iff \text{index}[\mathbb{Z}^n : H] < \infty$.

(b) Stel dat $k = n$, en dat H wordt voortgebracht door de rijen van de matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ met coëfficiënten $a_{ij} \in \mathbb{Z}$. Bewijs dat $|\det(A)|$ niet van de keuze van A maar alleen van H afhangt, en dat $|\det(A)| = \text{index}[\mathbb{Z}^n : H]$.

8.9 Definieer $H \subset \mathbb{Z}^2$ door $H = \big\{(x, y) \in \mathbb{Z}^2 \;\big|\; 3x + 4y \equiv 0 \bmod 5\big\}$. Geef een isomorfisme $\mathbb{Z}^2 \xrightarrow{\sim} H$ aan, en bewijs dat $\text{index}[\mathbb{Z}^2 : H] = 5$.

8.10 Bewijs dat in het bewijs van 8.8 geldt $k = n$, d.w.z. $\varphi[G] \cong \mathbb{Z}^n$.

8.11* Zij G een eindig voortgebracht abelse groep en

$$G \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z})$$

met $d_i \in \mathbb{Z}$ (eventueel nul), $d_{i+1} \mid d_i$ $(1 \leq i < t)$ en $|d_t| \neq 1$.

Bewijs dat G met behulp van t elementen voortgebracht kan worden maar niet met minder.

8.12 Zij G een eindig voortgebrachte abelse groep, en $H \subset G$ een ondergroep.

(a) Bewijs: H is eindig voortgebracht.

(b) Kan het minimum aantal voortbrengers van H groter dan dat van G zijn?

Bijlage A

Meetkunde en groepentheorie

In deze appendix gaan we meetkunde bekijken vanuit het gezichtspunt van de groepentheorie. Dit idee werd eind 19de eeuw geïntroduceerd door de Duitse wiskundige Felix Klein en staat bekend als het Erlangenprogramma, naar de Duitse stad waar hij professor was.

In die tijd was er een enorme toevloed aan nieuwe meetkundes ontstaan: hyperbolische meetkunde, projectieve meetkunde, hogerdimensionale meetkunde. Elk van die nieuwe meetkundes had zijn eigen terminologiën, concepten en stellingen. Om orde te scheppen in deze chaos bedacht Klein dat we met elke soort meetkunde een groep van symmetriën kunnen associëren.

Deze groep heeft dan verschillende groepswerkingen op verzamelingen van objecten in die meetkunde, bijvoorbeeld op de verzameling van alle punten, of de verzameling van alle lijnen enz. Interessante concepten zijn eigenschappen van die objecten die bewaard blijven onder de symmetriën, zoals lengtes en hoeken in de Euclidische meetkunde. Door de symmetriegroep van een meetkunde en zijn groepswerkingen in detail te bestuderen kunnen we veel informatie over de meetkunde bekomen.

We gaan het Erlangenprogramma in detail toepassen op de Euclidische meetkunde, zowel in het vlak als in de ruimte. Daarna zullen we ook nog enkele andere voorbeelden kort bespreken.

A.1 Het Euclidische Vlak

We definiëren het Euclidische vlak als de verzameling $\mathbb{E}_2 = \mathbb{R}^2$. De punten in het vlak kunnen we dus voorstellen als kolomvectoren $p = \binom{p_1}{p_2}$. Op de verzameling $\mathbb{E}_2$ definiëren we een afstand $d(p,q) = |p-q| = \sqrt{(p_1-q_1)^2 + (p_2-q_2)^2}$.

Definitie A.1. Een isometrie van het Euclidisch vlak is een bijectieve afbeelding die afstanden bewaart:

$$\varphi : \mathbb{R}^2 \to \mathbb{R}^2 : \forall p, q \in \mathbb{R}^2 : d(p,q) = d(\varphi(p), \varphi(q))$$

De verzameling van alle isometriën duiden we aan met $\mathrm{Isom}(\mathbb{E}_2)$.

De samenstelling van afbeeldingen geeft een groepsstructuur op $\mathrm{Isom}(\mathbb{E}_2)$ want

- de samenstelling van twee isommetriën is een isometrie want

$$d(\varphi\psi(p), \varphi\psi(q)) = d(\psi(p), \psi(q)) = d(p,q),$$

- de inverse van een isometrie is een isometrie want

$$d(\varphi^{-1}(p), \varphi^{-1}(q)) = d(\varphi\varphi^{-1}(p), \varphi\varphi^{-1}(q)) = d(p, q).$$

Stelling A.2. *Een isometrie beeldt cirkels op cirkels af en rechten op rechten. Lijnstukken worden afgebeeld op lijnstukken van dezelfde lengte, en driehoeken worden afgebeeld op een congruente driehoeken Een hoek wordt afgebeeld op een hoek met dezelfde grootte (maar niet noodzakelijk dezelfde orientatie).*

Bewijs. Een cirkel $C(p, \rho)$ met middelpunt p en straal ρ is de verzameling van alle punten op afstand ρ van p dus

$$\begin{aligned}\varphi(C(p,r)) &= \varphi\{q|d(p,q) = r\} = \{\varphi(q)|d(p,q) = r\}\\ &= \{\varphi(q)|d(\varphi(p),\varphi(q)) = r\}\\ &= \{q'|d(\varphi(p),q') = r\} = C(\varphi(p), r).\end{aligned}$$

Elke rechte kunnen we definiëren als een middelloodlijn van twee punten p, q:

$$\ell = \{x|d(x,p) = d(x,q)\}$$

bijgevolg is $\varphi(\ell)$ de middelloodlijn van $\varphi(p), \varphi(q)$.

Het lijnstuk $[pq]$ is de verzameling

$$[pq] = \{x|d(p,q) = d(p,x) + d(x,q)\}$$

en bijgevolg is $\varphi([pq]) = [\varphi(p)\varphi(q)]$.

Als p, q, r niet op een gezamelijke rechte liggen dan is $\triangle pqr = [pq] \cup [qr] \cup [rp]$ en dus is $\varphi(\triangle pqr) = \triangle\varphi(p)\varphi(q)\varphi(r)$. De zijden van $\varphi(\triangle pqr)$ hebbben dezelfde lengte en dus zijn $\triangle pqr$ en $\varphi(\triangle pqr)$ congruent. Dit wil dus ook zeggen dat ze dezelfde hoeken hebben. □

De concepten cirkel, rechte, driehoek, hoekgrootte zijn dus allemaal zinnige concepten in de Euclidische meetkunde. Er zijn ook concepten die niet zinnig zijn in de Euclidische meetkunde zoals wijzerzin en tegenwijzerzin, links en rechts, horizontaal en vertikaal want er zijn isometriën die deze begrippen omwisselen (b.v. spiegelingen).

We gaan nu proberen de groep van isometriën van het Euclidisch vlak te beschrijven. Dit doen we op twee manieren: meetkundig en algebraisch.

A.3 De algebraische beschrijving van $\mathrm{Isom}(\mathbb{E}_2)$.

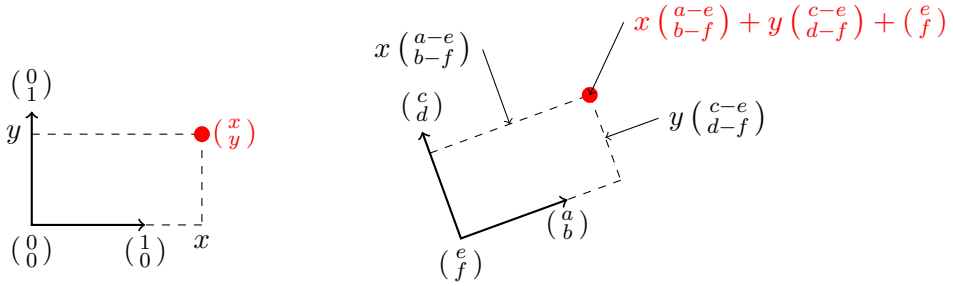
Stelling A.4. *Een isometrie is volledig bepaald door de drie beelden $\varphi\binom{0}{0}$, $\varphi\binom{1}{0}$ en $\varphi\binom{0}{1}$. Meer bepaald als*

$$\varphi\binom{0}{0} = \binom{e}{f}, \varphi\binom{1}{0} = \binom{a}{b} \text{ en } \varphi\binom{0}{1} = \binom{c}{d}$$

dan is

$$\varphi\binom{x}{y} = \begin{pmatrix} a-e & c-e \\ b-f & d-f \end{pmatrix}\binom{x}{y} + \binom{e}{f}$$

Bewijs. Dit volgt eenvoudig uit de onderstaande tekening.



□

Niet elke afbeelding van die vorm is een isometrie, om de afstanden te bewaren hebben we nog een extra voorwaarde nodig.

Stelling A.5. *De afbeelding*

$$\varphi : \binom{x}{y} \mapsto A\binom{x}{y} + \vec{b}$$

is een isometrie als en slechts als $A^\top A = 1$

Er zijn twee mogelijke vormen voor A:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ en } \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \text{ met } \theta \in [0, 2\pi)$$

Bewijs. We gebruiken het feit dat als we een punt x voorstellen door een kolomvector dan $|x| = \sqrt{x^\top x}$. Dus

$$\begin{aligned} |\varphi(p) - \varphi(q)| &= \sqrt{(\varphi(p) - \varphi(q))^\top (\varphi(p) - \varphi(q))} \\ &= \sqrt{(Ap + b - Aq - b)^\top (Ap + b - Aq - b)} \\ &= \sqrt{(A(p-q))^\top A(p-q)} \\ &= \sqrt{(p-q)^\top A^\top A(p-q)} \end{aligned}$$

Deze uitdrukking is gelijk aan $\sqrt{(p-q)^\top (p-q)}$ voor alle mogelijke p en q. Dit is waar als en slechts als $A^\top A = 1$. (hint: gebruik voor $p - q$ $\binom{1}{0}$ en $\binom{0}{1}$ om te zien dat de diagonaalelementen van $A^\top A$ 1 zijn en $\binom{1}{\pm 1}$ om te zien dat de niet-diagonaal elementen nul zijn).

De twee mogelijkheden voor A volgen uit het feit dat $A^\top A = 1$ impliceert dat het inproduct van een kolom van A met zichzelf 1 is. en met de andere kolom 0. Het zijn dus twee vectoren van lengte 1 die loodrecht op elkaar staan. Als we de eerste vector voorstellen door $\binom{\cos\theta}{\sin\theta}$ dan volgt het gestelde omdat er slechts 2 eenheidsvectoren zijn die daar loodrecht op staan namelijk $\binom{-\sin\theta}{\cos\theta}$ en $\binom{\sin\theta}{-\cos\theta}$. In het eerste geval is de determinant van A gelijk aan 1 in thet tweede is $\det A = -1$ □

Stelling A.6 (Algebraische classificatie van isometriën).

$$\mathrm{Isom}(\mathbb{E}_2) = \{\varphi : \mathbb{R}^2 \to \mathbb{R}^2 : \vec{x} \to A\vec{x} + \vec{b} | A \in \mathrm{Mat}_2(\mathbb{R}), \vec{b} \in \mathbb{R}^2 \text{ en } A^\top A = 1\}$$

Elke isometrie van het vlak is op unieke wijze te schrijven als een van deze twee vormen.

- $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \vec{b}$
  Dit noemen we een directe isometrie.

- $\begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \vec{b}$
  Dit noemen we een indirecte isometrie.

A.7 De meetkundige beschrijving van $\mathrm{Isom}(\mathbb{E}_2)$.

Definitie A.8. Een spiegeling is een niet-triviale isometrie die alle punten van een bepaalde rechte op zichzelf afbeeldt. Die rechte wordt de as van de spiegeling genoemd.

Voor een gegeven as ℓ is er precies 1 spiegeling want het beeld van $x \notin \ell$ moet de unieke y zijn zodat ℓ de middelloodlijn is van x, y. Deze spiegeling duiden we aan met σ_ℓ. Een spiegeling is zijn eigen inverse en heeft dus orde 2.

Stelling A.9. *Elke isometrie is de samenstelling van ten hoogste* 3 *spiegelingen.*

Bewijs. Stel

$$\varphi\begin{pmatrix} 0 \\ 0 \end{pmatrix} = p_0, \varphi\begin{pmatrix} 1 \\ 0 \end{pmatrix} = p_1 \text{ en } \varphi\begin{pmatrix} 0 \\ 1 \end{pmatrix} = p_2$$

We gaan via 3 afbeeldingen de drie basisvectoren naar p_0, p_1 en p_2 brengen en elk van die afbeeldingen is ofwel een spiegeling ofwel de triviale afbeelding. Als $p_0 \neq 0$ dan passen we een spiegeling σ_1 toe om de middelloodlijn tussen p_0 en 0 anders laten we σ_1 de triviale isometrie zijn. Vervolgens kijken we of $\sigma_1\begin{pmatrix} 1 \\ 0 \end{pmatrix} \neq p_1$, is dat het geval dan passen we een spiegeling σ_2 toe om de middelloodlijn tussen p_1 en $\sigma_1\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (Anders nemen we voor σ_2 de triviale isometrie). Merk op dat $\sigma_1(p_0)$ op die middelloodlijn ligt want

$$|p_0\sigma_1\begin{pmatrix} 1 \\ 0 \end{pmatrix}| = 1 = |p_0p_1|.$$

Bijgevolg is $\sigma_2\sigma_1\begin{pmatrix} 0 \\ 0 \end{pmatrix} = p_0$ en $\sigma_2\sigma_1\begin{pmatrix} 1 \\ 0 \end{pmatrix} = p_1$. Er zijn nu twee mogelijkheden ofwel is $\sigma_2\sigma_1\begin{pmatrix} 0 \\ 1 \end{pmatrix} = p_2$ en dan is $\varphi = \sigma_2\sigma_1$. Ofwel is p_2 het spiegelbeeld van $\sigma_2\sigma_1\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ om de as p_0p_1. In dat geval is $\varphi = \sigma_3\sigma_2\sigma_1$ waarbij σ_3 de spiegeling om p_0p_1 is. □

Stelling A.10 (Meetkundige classificatie van isometriën). *De groep* $\mathrm{Isom}(\mathbb{E}_2)$ *wordt voortgebracht door alle spiegelingen.*

$$\mathrm{Isom}(\mathbb{E}_2) = \langle \sigma_\ell | \ell \textit{ is een rechte in } \mathbb{E}_2 \rangle$$

Elke isometrie van het vlak behoort tot 1 van deze 4 types.

- *Spiegelingen.*
- *Draaiingen. Dit zijn samenstellingen van twee spiegelingen met snijdende assen. Het snijpunt is het centrum van de draaiing en de draaihoek is 2 keer de hoek van tussen de spiegelassen.*
- *Verschuivingen. Dit zijn samenstellingen van twee spiegelingen met evenwijdige assen. De richting van de verschuiving is loodrecht op de assen en de afstand is 2 keer de afstand tussen de twee assen.*

- *Glijspiegelingen. Dit zijn samenstellingen van 3 spiegelingen die niet te schrijven zijn als samenstellingen van minder spiegelingen.*

Merk op dat we draaiingen en verschuivingen op verschillende manieren kunnen schrijven als het product van twee spiegelingen. Het enige wat van belang is voor een draaiing is de hoek tussen de twee spiegelingassen en hun snijpunt. Voor een verschuiving is enkel de parallelklasse van de assen en hun onderlinge afstand van belang.

Stelling A.11. *Een glijspiegeling is steeds te schrijven als de samenstelling van een spiegeling en een verschuiving in de richting evenwijdig aan de spiegelas.*

Bewijs. Een glijspiegeling is een samenstelling van 3 spiegelingen.

Stel dat de drie assen van de spiegelingen ℓ_1, ℓ_2, ℓ_3 evenwijdig zijn dan kunnen we de eerste twee spiegelingen zien als een verschuiving. Die verschuiving kunnen we ook voorstellen door $\sigma_{\ell_4}\sigma_{\ell_3}$ (waarbij ℓ_4 een rechte is evenwijdig met ℓ_3 en de afstand tussen ℓ_4 en ℓ_3 is dezelfde als tussen ℓ_1 en ℓ_2). Bijgevolg is

$$\sigma_{\ell_1}\sigma_{\ell_2}\sigma_{\ell_3} = \sigma_{\ell_4}\sigma_{\ell_3}\sigma_{\ell_3} = \sigma_{\ell_4}$$

en is onze afbeelding geen glijspiegeling.

We kunnen dus veronderstellen dat ℓ_2 niet tegelijk evenwijdig is met ℓ_1 en ℓ_3. Als ℓ_2 en ℓ_3 snijden dan is hun product een draaiing. Die twee spiegelingen kunnen we dus vervangen door twee andere spiegelingen $\sigma_{\ell'_3}$ en $\sigma_{\ell'_2}$ met assen die in hetzelfde punt snijden en met een even grote hoek ertussen. Kies de 2 nieuwe spiegelingen zo dat ℓ'_2 evenwijdig is met ℓ_1. Onze glijspiegeling $\sigma_{\ell_1}\sigma_{\ell_2}\sigma_{\ell_3} = \sigma_{\ell_1}\sigma_{\ell'_2}\sigma_{\ell'_3}$ is dus de samenstelling van een spiegeling $\sigma_{\ell'_3}$ en een verschuiving $\sigma_{\ell_1}\sigma_{\ell'_2}$.

Splits de verschuiving in een component evenwijdig met de as ℓ'_3 en een component loodrecht op ℓ'_3. De component loodrecht op ℓ'_3 kan je schrijven als $\sigma_{\ell''_3}\sigma_{\ell'_3}$ waarbij $\ell''_3 // \ell_3$. De component evenwijdig met ℓ'_3 kan je schriijven als $\sigma_{\ell_5}\sigma_{\ell_4}$ met $\ell_4, \ell_5 \perp \ell'_3$. Dit geeft

$$\sigma_{\ell_1}\sigma_{\ell_2}\sigma_{\ell_3} = \sigma_{\ell_1}\sigma_{\ell'_2}\sigma_{\ell'_3} = \sigma_{\ell_5}\sigma_{\ell_4}\sigma_{\ell''_3}\sigma_{\ell'_3}\sigma_{\ell'_3} = \sigma_{\ell_5}\sigma_{\ell_4}\sigma_{\ell''_3}$$

en hebben we onze glijspiegeling geschreven als spiegeling om ℓ''_3 en translatie evenwijdig met ℓ''_3. Merk op dat deze spiegeling en verschuiving met elkaar commuteren.

Als ℓ_1 en ℓ_2 snijden kunnen we hetzelfde principe toepassen. □

A.12 Van algebra naar meetkunde. Het verband tussen de algebraische en meetkundige zienswijze is als volgt Stel $\varphi : \vec{x} \mapsto A\vec{x} + \vec{b}$. We kijken eerst naar de fixpunten van de afbeelding. Dit zijn de punten die op zichzelf worden afgebeeld: $\text{Fix}(\varphi) = \{p \in \mathbb{E}_2 | \varphi(p) = p\}$.

Dit zijn met andere woorden de oplossingen van het stelsel

$$(A - 1)\vec{x} + b = 0$$

Aangezien dit stelsel 2 vergelijkingen heeft en twee onbekenden zijn er 4 mogelijkheden.

- $\text{Fix}(\varphi) = \mathbb{E}_2$. In dat geval is $A = 1$ en $\vec{b} = 0$ en is de isometrie de identiteit.

- Fix(φ) is een lijn. De isometrie fixeert een rechte en dus is het een spiegeling.
- Fix(φ) is een punt. De isometrie fixeert een punt en dus is het een draaiing.
- Fix(φ) $= \emptyset$. In dat geval moeten we een onderscheid maken tussen $A = 1$ en $A \neq 1$. In het eerste geval is de afbeelding $\vec{x} \mapsto \vec{x} + \vec{b}$ een verschuiving. In het tweede geval is het geen spiegeling, verschuiving of draaiing en moet het dus een glijspiegeling zijn.

  Om de as van de glijspiegeling te vinden kan je het volgende trukje toepassen. Als je kijkt naar φ^2 dan is dit een verschuiving in de richting van de as van de glijspiegeling over 2 keer de afstand waarmee je verschuift voor de glijspiegeling. De uitdrukking voor φ^2 is $\vec{x} \mapsto A^2\vec{x} + A\vec{b} + \vec{b}$ de verschuiving is dus over $A\vec{b}+\vec{b}$. Als je φ samenstelt met een verschuiving over $-\frac{A\vec{b}+\vec{b}}{2}$ doe je deze verschuiving ongedaan en kijg je dus een spiegeling over de as van de glijspiegeling. De as van de glijspiegeling is dus de as van de spiegeling $\vec{x} \mapsto A\vec{x} + \vec{b} - \frac{A\vec{b}+\vec{b}}{2} = A\vec{x} + \frac{\vec{b}-A\vec{b}}{2}$.

A.13 Enkele groepswerkingen van Isom($\mathbb{E}_2$).

- De groep Isom($\mathbb{E}_2$) werkt van nature op de verzameling $\mathbb{E}_2$, de verzameling van alle punten in het vlak. Deze werking is transitief want je kan de oorsprong naar elk ander punt verschuiven. De stabilisator van de oorsprong is

$$\text{Stab}(0) = O_2 := \{\vec{x} \to A\vec{x} | A^\top A = 1\}.$$

  Dit is de groep van alle rotaties rond de oorsprong en spiegelingen met as door de oorsprong. Deze groep wordt de *orthogonale groep* in 2 dimensies genoemd.

- De groep Isom($\mathbb{E}_2$) werkt ook op de verzameling van alle rechtes, $\mathcal{L}$. Deze werking is ook transitief want je kan de X-as op elke andere rechte afbeelden door ze eerst in de juiste richting te draaien en dan te verschuiven. De stabilisator van de X-as is de groep

$$\text{Stab}(X) = \{\vec{x} \to A\vec{x} + \vec{b} | A = \left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} s \\ 0 \end{smallmatrix}\right)\}$$

  Deze bestaat uit verschuivingen in de X-richting, rotaties over 180° rond een punt op de X-as, spiegelingen rond rechts loodrecht op de X-as, en (glij)spiegelingen, evenwijdig aan de X as.

- De groep Isom($\mathbb{E}_2$) werkt op de verzameling van de cirkels, $\mathcal{C}$. Deze werking is niet transitief, voor elke mogelijke straal is er 1 baan. De stabilisator van een cirkel met straal r en middelpunt de oorsprong is O_2.

- De groep Isom($\mathbb{E}_2$) werkt op de verzameling van de driehoeken, $\mathcal{D}$. Deze werking is niet transitief, voor elke mogelijke combinatie van 3 lengtes voor de zijden is er één baan (=congruentieklasse). De banenruimte kunnen we identificeren met de verzameling

$$\{(a, b, c) | a \geq b \geq c > 0 \text{ en } a < b + c \text{ (driehoeksongelijkheid)}\}.$$

  De stabilisator van een congruentieklasse hangt af van het soort driehoek, bij een gelijkzijdige driehoek is de stabilisator isomorf met D_3. bij een gelijkbenige $\mathbb{Z}/2\mathbb{Z}$ (nl de identiteit en een spiegeling) en bij een gewone driehoek is de stabilisator triviaal.

- De laatste objecten waar we naar kijken zijn kegelsneden. Dit zijn deelverzamelingen van het vlak die voldoen aan een vergelijking van de vorm $aX^2 + bXY + cY^2 + dX + eY + f = 0$. We beperken ons tot echte kegelsneden, dit wil zeggen dat de kegelsnede niet leeg of één enkel punt is, en geen rechte bevat. Er zijn 3 soorten kegelsneden: ellipsen, parabolen en hyperbolen (dit is wanneer $b^2 - 4ac < 0$, $b^2 - 4ac = 0$ en $b^2 - 4ac > 0$).

  Een ellips $E(p, q, \rho)$ is de verzameling van alle punten waarvoor de som van de afstanden tot de brandpunten p en q gelijk is aan ρ.

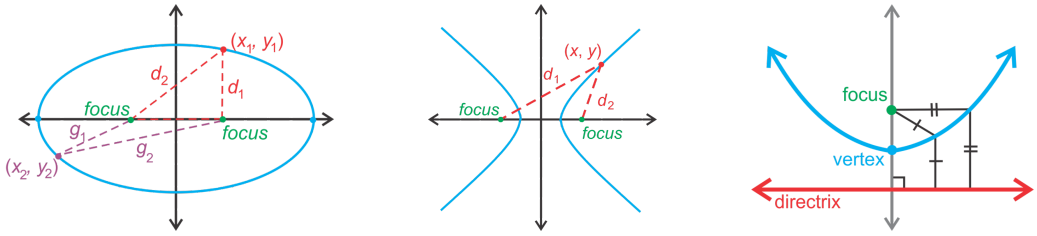
  $$E(p, q, \rho) = \{x \in \mathbb{E}_2 | d(x, p) + d(x, q) = \rho\}$$

  Een hyperbool $H(p, q, \rho)$ is de verzameling van alle punten waarvoor het verschil van de afstanden tot de brandpunten p en q gelijk is aan ρ.

  $$H(p, q, \rho) = \{x \in \mathbb{E}_2 | |d(x, p) - d(x, q)| = \rho\}$$

  Een parabool $P(p, \ell)$ is de verzameling van alle punten waarvoor de afstand tot een rechte ℓ gelijk is aan de afstand tot het brandpunt p.

  $$P(p, \ell) = \{x \in \mathbb{E}_2 | d(x, p) = \min_{q \in \ell} d(x, q)\}.$$



  Voor een isometrie φ hebben we $\varphi(E(p, q, \rho)) = E(\varphi(p), \varphi(q), \rho)$, $\varphi(H(p, q, \rho)) = H(\varphi(p), \varphi(q), \rho)$ en $\varphi(P(p, \ell)) = P(\varphi(p), \varphi(\ell))$. Twee ellipsen/hyperbolen zitten dus in dezelfde baan als $d(p_1, q_1) = d(p_2, q_2)$ en $\rho_1 = \rho_2$. Twee parabolen zitten in dezelfde baan als $\min_{q \in \ell_1} d(p_1, q) = \min_{q \in \ell_2} d(p_2, q)$.

  Meestal is de stabilisator van een ellips of hyperbool is de viergroep van Klein. Hij wordt gegenereerd door de door de spiegeling om de as pq en de spiegeling om de middelloodlijn van p, q. Er is echter een speciaal geval: wanneer $p = q$ is de ellips een cirkel en is de symmetriegroep O_2. De stabilisator van een parabool is $\mathbb{Z}/2\mathbb{Z}$ en is voortgebracht door de spiegeling met as door het brandpunt en loodrecht op ℓ.

- Tot slot kunnen we ook de conjugatieactie van $\mathrm{Isom}(\mathbb{E}_2)$ op zichzelf beschouwen. Als p een fixpunt is van φ dan is $\psi(p)$ een fixpunt van $\psi\varphi\psi^{-1}$. Dit wil zeggen dat ψ een draaiing rond p conjugeert tot een draaiing rond $\psi(p)$ over dezelfde hoek, maar eventueel in tegengestelde richting als ψ een (glij)spiegeling is. Een spiegeling om ℓ wordt geconjugeerd tot een spiegeling om $\psi(\ell)$. Wanneer we deze gedachtengang verder uitwerken krijgen we de volgende classificatie.

  – Alle spiegelingen vormen een conjugatieklasse, de stabilisator van een spiegeling is dezelfde als de stabilisator van de as.

- Alle draaiingen met dezelfde draaiingshoek (ongeorienteerd) vormen een conjugatieklasse. De stabilisator van een draaiing om de oorsprong is de groep van alle draaiingen rond de oorsprong. Deze groep noemen we de *speciale orthogonale groep* $SO_2 = \{A \in \mathrm{Mat}_2(\mathbb{R}) | A^\top A = 1 \text{ en } \det A = 1\}$. Als de draaiingshoek 180° is dan zitten ook de spiegelingen met assen door dat punt in de stabilisator en is de stabilisator O_2.
- Alle verschuivingen over dezelfde afstand vormen een conjugatieklasse. De stabilisator van een verschuiving is voortgebracht door alle verschuivingen en alle (glij)spiegelingen met een as evenwijdig met de verschuivingsrichting.
- Alle glijspiegelingen die over dezelfde afstand verschuiven vormen een conjugatieklasse. De stabilisator van een glijspiegeling is voortgebracht door alle verschuivingen evenwijdig met de as van de glijspiegeling en alle (glij)spiegelingen met een dezelfde as als de glijspiegeling.

A.14 De groepsstructuur van $\mathrm{Isom}(\mathbb{E}_2)$.

Eerst en vooral bekijken we de normaaldelers.

Stelling A.15. *Elke echte normaaldeler van* $\mathrm{Isom}(\mathbb{E}_2)$ *is van de vorm* $N = \{\vec{x} \mapsto A\vec{x}+\vec{b} | b \in \mathbb{R}^2 \text{ en } A \in G\}$ *waarbij* G *een deelgroep is van* SO_2.

Bewijs. Een echte normaaldeler kan geen spiegeling bevatten want dan bevat hij alle spiegelingen en is dus de volledige groep. Als een normaaldeler een draaiing bevat dan bevat hij alle draaiingen over dezelfde hoek rond alle mogelijke centra. Als je twee draaiingen met verschillende centra en dezelfde hoek maar verschillende zin samenstelt krijg je een verschuiving. Als een normaaldeler een verschuiving bevat dan bevat hij alle verschuivingen want je kan elke vector schrijven als een som van vectoren met allemaal dezelfde vooraf gekozen lengte. Als een normaaldeler een glijspiegeling ψ bevat, bevat hij ook een verschuiving ψ^2 en bijgevolg ook een spiegeling en dus is de normaaldeler de gehele groep.

Hieruit kunnen we dus besluiten dat elke echte normaaldeler $N \lhd \mathrm{Isom}(\mathbb{E}_2)$ de deelgroep van alle verschuivingen $\mathbb{R}^2$ bevat. Deze groep $\mathbb{R}^2$ is zelf een normaaldeler van $\mathrm{Isom}(\mathbb{E}_2)$ en het quotient is O_2. $N/\mathbb{R}^2$ is dus een normaaldeler van O_2 en aangezien deze geen spiegelingen mag bevatten is het een deelgroep van SO_2. Elke deelgroep van SO_2 is een normaaldeler van O_2 want de conjugatieklasse van een draaiing in O_2 is van de vorm $\{\varphi, \varphi^{-1}\}$. □

Stelling A.16. $\mathrm{Isom}(\mathbb{E}_2) \cong O_2 \ltimes \mathbb{R}^2 \cong (\mathbb{Z}/2\mathbb{Z} \ltimes SO_2) \ltimes \mathbb{R}^2$

Bewijs. De groepen O_2 en $\mathbb{R}^2$ brengen $\mathrm{Isom}(\mathbb{E}_2)$ voort, hebben een triviale doorsnede en zoals we reeds zagen is $\mathbb{R}^2$ een normaaldeler in $\mathrm{Isom}(\mathbb{E}_2)$. Neem nu de spiegeling rond de X-as. De groepen $\{1, \sigma_X\}$ en SO_2 brengen O_2 voort en hebben triviale doorsnede. Bovendien is $SO_2 \lhd O_2$. □

A.17 Eindige deelgroepen van $\mathrm{Isom}(\mathbb{E}_2)$.

Nu zullen we onze aandacht richten op deelgroepen die kunnen voorkomen als symmetriegroepen van objecten het vlak. Als een object eindig van vorm is en gemaakt is uit een eindige aantal lijnstukken dan moet de symmetriegroep eindig zijn. In dat geval zijn er slechts weinig mogelijkheden.

Stelling A.18. *Elke eindige deelgroep* $G \subset \mathrm{Isom}(\mathbb{E}_2)$ *is ofwel een cyclische groep of een diëdergroep.*

Bewijs. De elementen van G zijn ofwel spiegelingen ofwel draaiingen over een hoek $2\pi/n$ want dit zijn de enige elementen met eindige orde. Als ρ_1 en ρ_2 twee draaiingen zijn met verschillende centra dan is $\rho_1\rho_2\rho_1^{-1}\rho_2^{-1}$ een verschuiving, dus alle draaiingen moeten hetzelfde centrum hebben.

Stel nu dat G geen spiegelingen bevat. Laat ρ_θ de draaiing zijn met de kleinste niet-nul hoek. Dan is ρ_θ een voortbrenger van G. Inderdaad stel $\rho_{\theta'}$ een andere draaiing dan is θ' een veelvoud van θ want anders is $\theta' = k\theta + \gamma$ met $\gamma < \theta$ en $\rho_\gamma = \rho_{\theta'}\rho_\theta^{-k} \in G$. Dit is strijdig met het feit dat θ de kleinste hoek is. $G = \langle\rho_\theta\rangle \cong \mathbb{Z}/n\mathbb{Z}$ met $\theta = 2\pi/n$.

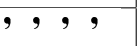
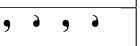
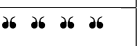
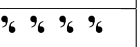
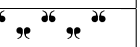
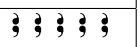
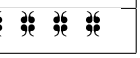
Als G een spiegeling σ bevat zijn er twee mogelijkheden ofwel is $G = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ ofwel bevat G een draaiing want als G twee spiegelingen bevat is hun samenstelling een draaiing. De deelgroep van alle draaiingen $G^+ = \langle\rho_\theta\rangle$ voor een zekere $\theta = 2\pi/n$. We tonen aan $G = \langle\sigma, \rho_\theta\rangle \cong D_n$. Inderdaad als $x \in G \setminus G^+$ dan is x een spiegeling en σx een draaiing dus $x = \sigma(\sigma x) = \sigma\rho_\theta^k \in \langle\sigma, \rho_\theta\rangle$.

Nu is $\sigma\rho_\theta\sigma \in G$ een draaiing met hetzelfde centrum als ρ_θ en dus moet $\sigma\rho_\theta\sigma = \rho_\theta^{-1}$. Dit impliceert dat $\langle\sigma, \rho_\theta\rangle \cong D_n$ □

A.19 Friesgroepen. Een fries is een patroon in het vlak dat zich in 1 richting herhaalt. Dit wil zeggen dat de verschuivingen in de symmetriegroep voortgebracht zijn door 1 element. Een friesgroep is dus een deelgroep $F \subset \mathrm{Isom}(\mathbb{E}_2)$ zodanig dat $F \cap \mathbb{R}^2 \cong \mathbb{Z}$.

Stelling A.20. *Stel τ een verschuiving en $\sigma_\perp$, $\sigma_{//}$ twee spiegelingen met as loodrecht op en evenwijdig aan de verschuivingsrichting. Verder definiëren we de draaiing $\rho_{180} = \sigma_\perp\sigma_{//}$ en de glijspiegeling $\gamma = \sigma_{//}\tau^{1/2}$, waarbij $\tau^{1/2}$ de verschuiving is in de richting van τ maar over de helft van de afstand van τ.*

Elke friesgroep F met $F \cap \mathbb{R}^2 = \langle\tau\rangle$ is geconjugeerd met 1 *van de volgende zeven groepen.*

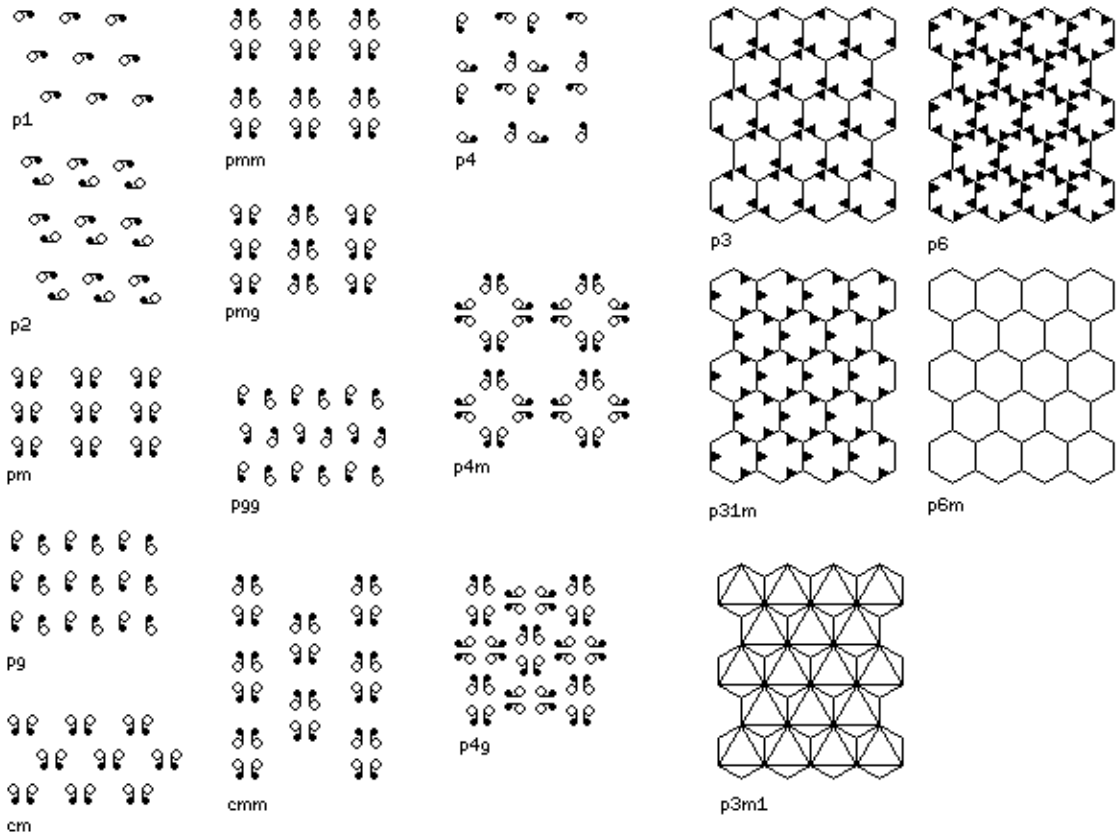
Naam	*Groep*	*Patroon*
p1	$\langle\tau\rangle$	
p1m1	$\langle\tau, \sigma_\perp\rangle$	
p11m	$\langle\tau, \sigma_{//}\rangle$	
p11g	$\langle\tau, \gamma\rangle$	
p2	$\langle\tau, \rho_{180}\rangle$	
p2mg	$\langle\tau, \gamma, \rho_{180}\rangle$	
p2mm	$\langle\tau, \sigma_\perp, \sigma_{//}\rangle$	

Bewijs. De enige isometriën die we aan τ kunnen toevoegen zijn isometriën die τ toevoegen tot $\pm\tau$. Dit zijn rotaties over 180°, spiegelingen evenwijdig en loodrecht op de vector τ en glijspiegelingen evenwijdig met τ. Bij de laatste moeten we we wel voor zorgen dat γ^2 een veelvoud is van τ want anders is $F \cap \mathbb{R}^2 \neq \langle\tau\rangle$. De rest van het bewijs bestaat er in alle mogelijke combinaties na te gaan en zien of ze niet dezelfde of geconjugeerde groepen opleveren (b.v. $\langle\tau, \sigma_\perp, \sigma_{//}\rangle = \langle\tau, \sigma_\perp, \rho_{180}\rangle$). □

A.21 Behangpatroongroepen. Behangpapier is een patroon in het vlak dat zich in 2 richtingen constant herhaalt. Dit wil zeggen dat de verschuivingen in de symmetriegroep voortgebracht zijn door 2 elementen die niet evenwijdig zijn. Een behangpatroongroep is dus een deelgroep $F \subset \mathrm{Isom}(\mathbb{E}_2)$ zodanig dat $F \cap \mathbb{R}^2 = \langle\tau_1, \tau_2\rangle$ waarbij τ_1, τ_2 lineair onafhankelijke vectoren zijn.

Stelling A.22. *Stel τ_1, τ_2 2 lineair onafhankelijke verschuivingen. Er zijn* 17 *verschillende soorten behangpatroongroepen met $F \cap \mathbb{R}^2 = \langle \tau_1, \tau_2 \rangle$.*

Bewijs. Analoog aan het voorgaande maar ingewikkelder. De uiteindelijke classificatie ziet er zo uit:



□

Eindige groepen, friesgroepen en behangpatroongroepen zijn voorbeelden van *discrete deelgroepen*. Een deelgroep G is discreet als de baan van een punt p onder deze deelgroep G een discrete verzameling is. D.w.z. dat de punten op een bepaalde minimumafstand van elkaar blijven

$$\exists \varepsilon > 0 : \forall x, y \in G : x \neq y \implies d(x, y) > \varepsilon.$$

A.2 Euclidische meetkunde in hogere dimensies

Analoog aan het Euclidische vlak definiëren we de n-dimensionale Euclidische ruimte als de verzameling $\mathbb{E}_n = \mathbb{R}^n$ uitgerust met de afstand $d(p, q) = |p - q| = \sqrt{(p_1 - q_1)^2 + \cdots + (p_n - q_n)^2}$. Net als in 2 dimensies definiëren we $\mathrm{Isom}(\mathbb{E}_n)$ als de groep van afstandsbewarende afbeeldingen.

$$\mathrm{Isom}(\mathbb{E}_n) = \{\varphi : \mathbb{R}^n \to \mathbb{R}^n | \forall p, q \in \mathbb{R}^n : d(p, q) = d(\varphi(p), \varphi(q))\}$$

De *orthogonale groep* is de groep van isometriën die de oorsprong fixeren en de *speciale orthogonale groep* is de deelgroep met determinant 1:

$$O_n = \{A \in \mathrm{Mat}_n(\mathbb{R}) | A^\top A = 1\} \text{ en } SO_n = \{A \in O_n | \det A = 1\}$$

De hoofdstellingen veralgemenen eenvoudig naar meer dimensies.

Stelling A.1.

$$\mathrm{Isom}(\mathbb{E}_n) = \{\vec{x} \mapsto A\vec{x} + \vec{b} | A \in \mathrm{Mat}_n(\mathbb{R}), b \in \mathbb{R}^n \text{ en } A^\top A = 1\}$$

Elke isometrie is de samenstelling van ten hoogste $n+1$ spiegelingen. (Een spiegeling is een isometrie die de punten van een $n-1$-dimensionale deelruimte fixeert.)

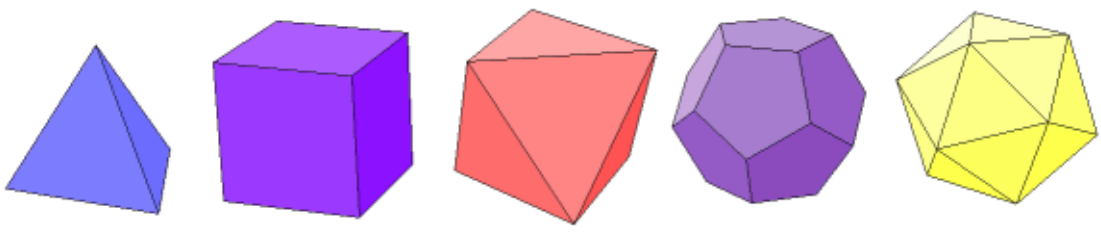
$$\mathrm{Isom}(\mathbb{E}_n) \cong O_n \ltimes \mathbb{R}^n \cong (\mathbb{Z}/2\mathbb{Z} \ltimes SO_n) \ltimes \mathbb{R}^n$$

Als n oneven is $O_n = \{1, -1\} \times SO_n$ en is het ene semidirect product een direct product.

Dit geeft ons weer een manier om isometriën op te splitsen in verschillend de soorten. In drie dimensies hebben we spiegeling, draaiingen (dit zijn samenstellingen van 2 spiegelingen met spiegelvlakken die snijden in de draaiingsas), verschuivingen (dit zijn samenstellingen van 2 spiegelingen met evenwijdige spiegelvlakken), glijspiegelingen (een spiegeling samengesteld met een verschuiving evenwijdig met het spiegelvlak), draaispiegelingen (een draaiing samengesteld met een spiegeling met spiegelvlak loodrecht op de draaias) en schroefbewegingen (een draaiing samengesteld met een verschuiving evenwijdig met de draaias). Elk van die types kunnen we dan weer opsplitsen in conjugatieklassen volgens de draaihoeken en de verschuivingsafstanden)

A.2 Eindige rotatiegroepen in drie dimensies. Net zoals in 2 dimensies kunnen we gaan kijken naar speciale deelgroepen. Aangezien $O_3 = \mathbb{Z}/2\mathbb{Z} \times SO_3$ beperken we ons tot eindige deelgroepen van SO_3. In dit geval kunnen we de symmetriegroepen characteriseren aan de hand van de *Platonische lichamen*. Een Platonisch lichaam is een driedimensionaal object waarvan de zijvlakken allemaal regelmatige veelhoeken zijn van hetzelfde type en in elk hoekpunt komen evenveel zijvlakken samen. Aangezien de totale som van de hoeken die samenkomen in een hoekpunt kleiner moet zijn dan 360° zijn er 5 mogelijke Platonische lichamen:

- 3 driehoeken geeft een een lichaam met 4 zijvlakken, 6 ribben en 4 hoekpunten: de tetraëder ,
- 3 vierhoeken geeft een een lichaam met 6 zijvlakken, 12 ribben en 8 hoekpunten: de kubus,
- 4 driehoeken geeft een een lichaam met 8 zijvlakken, 12 ribben en 6 hoekpunten: de octaëder,
- 3 vijfhoeken geeft een een lichaam met 12 zijvlakken, 30 ribben en 20 hoekpunten: de dodecaëder,
- 5 driehoeken geeft een een lichaam met 20 zijvlakken, 30 ribben en 12 hoekpunten: de icosaëder.



Stelling A.3. *Een eindige deelgroep van SO_3 is isomorf met* 1 *van de volgende groepen*

$\mathbb{Z}/n\mathbb{Z}$ *een cyclische groep, dit is de rotatiegroep van een regelmatige pyramide.*

D_n *een diëdergroep, dit is de rotatiegroep van een regelmatig prisma.*

A_4 *de alternerende groep in 4 elementen, dit is de rotatiegroep van de tetraëder.*

S_4 *de symmetrische groep in 4 elementen, dit is de rotatiegroep van de kubus of de octaëder.*

A_5 *de alternerende groep in 5 elementen, dit is de rotatiegroep van de dodecaëder of icosaëder.*

Bewijs. Merk op dat alle niet-triviale elementen van SO_3 draaiingen zijn. Inderdaad wegens de stelling is zo'n element de samenstelling van ofwel 2 of 4 spiegelingen met spiegelvlakken door de oorsprong. In het eerste geval heb je een draaiing rond de snijlijn van de twee vlakken. In het tweede geval hebben we de samenstelling van 2 draaiingen, rond de assen ℓ_1 en ℓ_2. Door beide draaiingen te herschrijven als een samenstelling de spiegeling om het vlak $\ell_1\ell_2$ en nog een andere spiegeling kunnen we de 4 spiegelingen reduceren tot twee omdat we de spiegeling om het vlak $\ell_1\ell_2$ dan twee keer na elkaar gebruiken en die dus wegvalt.

Met elk element niet-triviaal element van G kunnen we dus een as definiëren en deze as snijdt de eenheidssfeer in twee punten $p, -p$. Stel P de verzameling van al deze punten. Op P is een werking van G en we gaan kijken naar de banen van deze werking. Als p een punt is in P dan is de stabilisator in P de deelgroep van alle draaiingen met as door p en $-p$. Dit is een cyclische deelgroep en we stellen de orde van deze groep voor door $n_p > 1$. Het aantal elementen in de baan van p is dus $\#G/n_p$. Wegens de formule van Burnside en het feit dat $P_g = \{x \in P : gx = x\} = \{p, -p\}$ voor een niet-triviale draaiing met as door $p, -p$, is het aantal banen

$$\#P/G = \frac{1}{\#G}\sum_{g\in G}\#P^g = \frac{1}{\#G}(P + 2(\#G-1)) = \frac{1}{\#G}(\sum_{Gp\in P/G}\#G/n_p + 2(\#G-1))$$

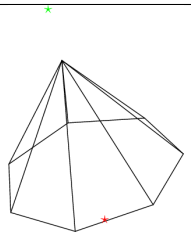
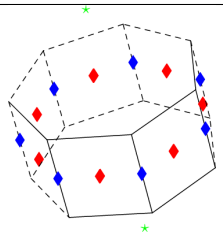
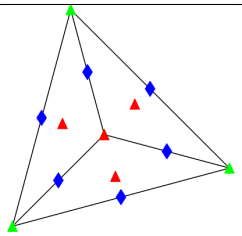
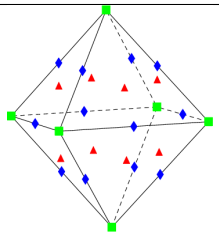
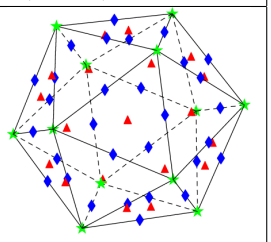
Als we de sommatie over P/G naar links brengen krijgen we

$$\#P/G - \sum_{Gp\in P/G} 1/n_p = 2(1 - \frac{1}{\#G})$$

$$\sum_{Gp\in P/G}(1 - 1/n_p) = 2 - \frac{2}{\#G}$$

$$\#G = \frac{2}{2 - \sum_{Gp\in P/G}(1-1/n_p)}$$

We moeten dus alle combinaties van $n_p's > 1$ zoeken waarvoor deze uitdrukking een positief geheel getal oplevert. De mogelijkheden zijn hieronder weergegeven, samen met een plaatje van de banen. Verschillende banen zijn in verschillende kleuren. De $n_p's$ kan je afleiden uit het symbool ($\Diamond = 2$, $\triangle = 3$, $\square = 4$, $\star$ =rest).

(n,n) $\#G=n$	$(2,2,n)$ $\#G=2n$	$(2,3,3)$ $\#G=12$	$(2,3,4)$ $\#G=24$	$(2,3,5)$ $\#G=60$
				

In het eerste geval hebben we te maken met een cyclische groep want de stabilisator van een punt p is een cyclische deelgroep van de orde n_p en $n_p = n = \#G$.

In het tweede geval hebben is er een rotatie van de orde n, de twee punten van die as zitten in 1 baan dus is er een rotatie over 180° die de as omkeert. Die twee rotaties genereren een diëdergroep $D_n \subset G$. Daar $\#G = 2n = \#D_n$ is G een diëdergroep.

In het derde geval heeft G een werking op de baan G_p met $n_p = 3$. Dit geeft een afbeelding $G \to S_4$. Deze afbeelding is een injectie want een isometrie ligt vast als je het beeld van vier punten kent die niet in 1 vlak liggen. Het beeld is een deelgroep van S_4 met 12 elementen en is dus gelijk aan A_4.

In het vierde geval beschouwen we de werking van G op de verzameling van de 4 rotatieassen die 2 overstaande punten van de baan met 8 elementen verbinden. Dit geeft opnieuw een afbeelding van G naar S_4. Deze afbeelding is injectief want het beeld van de 4 rechten niet in een vlak legt een isometrie vast. Aangezien G ook 24 elementen heeft is dit een bijectie.

In het laatste geval beschouw een punt p uit de baan $P_2 \subset P$ met $n_p = 2$. Dit komt overeen met een rotatie ρ over 180°. De centralisator van ρ (de deelgroep van alle elementen uit G die met ρ commuteren) bestaat uit de afbeeldingen die p afbeelden op p of $-p$. Er zijn 4 zulke afbeeldingen want er zijn precies twee afbeeldingen die p vasthouden ($n_p = 2$) en er is een afbeelding ψ die p op $-p$ afbeeldt want die zitten in dezelfde baan. Elke afbeelding kan dus geschreven worden als $\varphi^{0,1}\rho^{0,1}$. Deze groep is de viergroep van Klein want er zijn geen elementen van de orde 4 in G (anders was er een baan in P met $4|n_p$). De assen van de niet-triviale rotaties in de viergroep staan loodrecht op elkaar want ze commuteren allemaal met elkaar.

Beschouw de verzameling

$$\mathcal{V} = \{V \subset G | V \text{ is een viergroep van Klein }\}.$$

Er zijn 15 elementen van de orde 2 want er zijn 30 punten in de baan P_2 en de andere banen hebben een oneven $n_{p'}$ en kunnen dus geen draaiingen van de orde twee genereren. Als $\rho \in V$ dan is V de centralisator van ρ, dus als twee viergroepen van Klein een gemeenschappelijke niet-triviale draaiing bevatten, dan zijn ze allebei de centralizator van hetzelfde element en dus gelijk aan elkaar. Aangezien een viergroep 3 elementen van de orde twee bevat heeft $\mathcal{V}$ dus $15/3 = 5$ elementen.

Beschouw nu de conjugatiewerking van G op $\mathcal{V}$. Dit geeft een afbeelding van G naar S_5. We tonen aan dat het beeld alle permutaties van de vorm $(ab)(cd)$ bevat.

Stel φ een rotatie over 180° en $\varphi(V) = V$. Daar de orde van φ twee is en V drie nietriviale elementen heeft moet φ minstens 1 van die elementen vasthouden. Dus φ zit in de centralizator van dat element en die centralizator is V zelf. Dit wil zeggen dat als ρ een rotatie is over 180° dan fixeert

deze enkel zijn eigen viergroep en wisselt de andere 4 twee aan twee om. M.a.w. de permutatie ziet er uit als $(ab)(cd)$

Twee zulke rotaties kunnen niet dezelfde permutatie geven want dan zitten ze in dezelfde viergroep en geeft hun product, dat ook in die viergroep zit een triviale permutatie wat in tegenspraak is met de vorige paragraaf. Er zijn 15 elementen van de orde 2 en 15 permutaties van het type $(ab)(cd)$. Aangezien deze permutaties A_5 genereren zit A_5 in het beeld van $G \to S_5$. Daar G en A_5 beiden 60 elementen hebben is $G \cong A_5$.

Beschouw nu een Platonisch lichaam, de isometriën die dit lichaam op zichzelf afbeelden vormen een eindige deelgroep van SO_3.

De symmetriegroep van de tetraëder bestaat uit 4 draaiingen over 120° rond een as door een hoekpunt, 4 draaiingen over 240° rond een as door een hoekpunt en $6/2 = 3$ draaiingen over 180° rond een as door het middelpunt van een ribbe. Samen met de identiteit geeft dit $1 + 4 + 4 + 3 = 12$ symmetriën en dit geeft dus A_4 (D_6 en $\mathbb{Z}/12\mathbb{Z}$ zijn uitgesloten want er zijn geen draaiiingen over 60°).

De symmetriegroep van de kubus bestaat uit 8 draaiingen over 120° rond een as door een hoekpunt, 6 draaiingen over 90° rond een as door het middelpunt van een vierkant, $6/2$ draaiingen over 180° rond een as door het middelpunt van een vierkant en $12/2 = 2$ draaiingen over 180° rond een as door het middelpunt van een ribbe. Samen met de identiteit geeft dit $1 + 8 + 6 + 3 + 6 = 24$ symmetriën en dit geeft dus S_4. Idem voor de octaëder.

De symmetriegroep van de dodecaëder bestaat uit 20 draaiingen over 120° rond een as door een hoekpunt, 12 draaiingen over 72° rond een as door het middelpunt van een vijfhoek, 12 draaiingen over 144° rond een as door het middelpunt van een vijfhoek en $30/2 = 15$ draaiingen over 180° rond een as door het middelpunt van een ribbe. Samen met de identiteit geeft dit $1 + 20 + 12 + 12 + 15 = 24$ symmetriën en dit geeft dus A_5. □

A.4 Eindige reflectiegroepen. In hogere dimensies wordt de classificatie ingewikkelder want we kunnen S_n inbedden in O_n als de groep van permutatiematrices. Aangezien elke eindige groep kan ingebed worden is een symmetrische groep, wil dit zeggen dat elke eindige groep voorkomt als een deelgroep van O_n. We kunnen echter wel een classificatie maken van alle eindige deelgroepen die voortgebracht worden door spiegelingen.

Definitie A.5. Een *Coxeterdiagram* is een graaf die bestaat uit een verzameling knopen met daartussen zijden die gemarkeerd zijn met een getal ≥ 2. Zijden gemarkeerd met 2 worden niet getekend en zijden gemarkeerd met 3 worden getekend zonder de 3 erbij. Soms worden zijden gemarkeerd met een n ook getekend als $n-2$-voudige zijden.

Elke knoop stelt een spiegeling voor en als er tussen twee knopen een zijde is die gemarkeerd is met n dan maken de twee spiegelingen een hoek van π/n. Dit wil zeggen dat hun samenstelling een draaiing is met orde n.

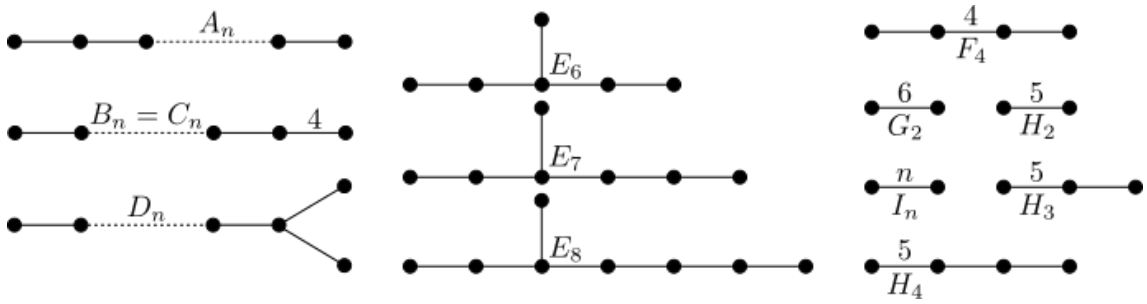
De Coxetergroep van het diagram G is dan de groep voortgebracht door deze spiegelingen. We kunnen deze als volgt schrijven met voortbrengers en relaties

$$\mathrm{Cox}(G) = \frac{\langle g_i \ i \text{ is een knoop} \rangle}{\langle g_i^2, (g_i g_j)^{m_{ij}} \rangle}$$

waarbij m_{ij} de markering is van de zijde tussen de knopen i en j.

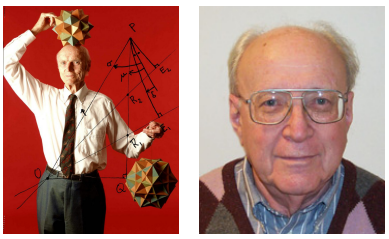
De diëdergroep D_n is de Coxetergroep van het diagram $\circ\overset{n}{—}\circ$, de symmetrische groep S_n is Coxetergroep van het diagram $\circ—\circ\cdots\circ—\circ$ met $n-1$ knopen. De spiegelingen zijn in dit geval de transposities $(ii+1)$.

Stelling A.6 (Coxeter)**.** *Als* $\mathrm{Cox}(G)$ *een eindige groep is dan is* G *een disjuncte unie van de volgende diagrammen.*



In deze notatie verwijst de subscript n *naar het aantal knopen, behalve bij* I_n*.*

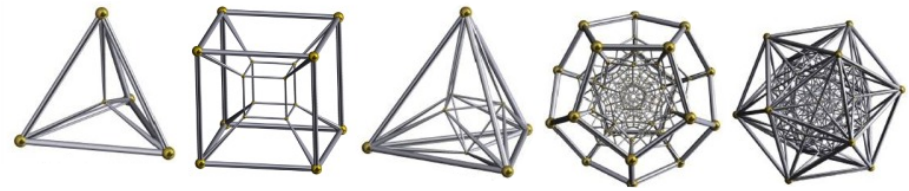
Deze diagrammen worden de (eindige) *Dynkindiagrammen* genoemd en zijn heel belangrijk in de moderne wiskunde. In bijna elk onderzoeksgebied komen deze diagrammen voor.



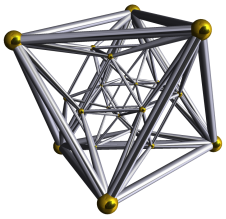
Donald Coxeter (1907–2003) en Eugene Dynkin, (1924–2014)

De diëdergroep D_n valt in deze classicatie onder I_n (of B_2, H_2, G_2 voor $n = 4, 5, 6$). Ook herkennen we de Platonische lichamen. Elk Platonisch lichaam heeft een symmetriegroep gegenereerd door spiegelingen. Deze is 2 keer zo groot als de symmetriegroep gegenereerd door draaiingen. De symmetriegroep van een Platonisch lichaam wordt gegenereerd door 3 spiegelvlakken: deze drie vlakken gaan door het middelpunt van het Platonisch lichaam en door het hoekpunt, het middelpunt van een zijvlak en het middepunt van een ribbe. De draaiingen hebben ordes $(2,3,3), (2,3,4)$ en $(2,3,5)$ en daarom zijn de Dynkin diagrammen A_3, B_3, B_3, H_3 en H_3.

In meer dimensies hebben we analogen van Platonische lichamen. n-dimensionale Platonische polytopen hebben $n-1$-dimensionale Platonische polytopen als zijvlakken en zijvlakken en alle hoekpunten zien er hetzelfde uit. In 4 dimensies zijn er 6. De 5-cel bestaat uit 5 tetraëders, de hyperkubus bestaat uit 8 kubussen, de 16-cel uit 16 tetraëders, de 120-cel bestaat uit 120 dodecaëders en de 600-cel uit 600 tetraëders. Dit zijn veralgemeningen van de 5 Platonische lichamen. De overeenkomstige diagrammen zijn A_4, B_4, B_4, H_4, en H_4.



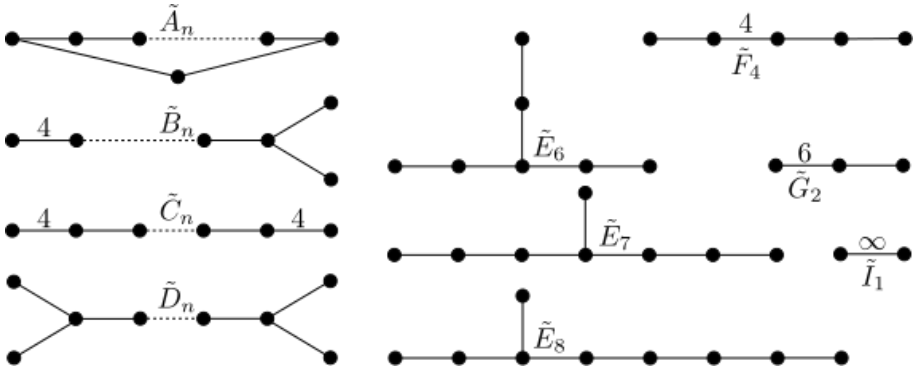
In 4 dimensies is er nog een speciale polytoop die geen analogon heeft in 3 dimensies: de 24-cell, die bestaat uit 24 octaëders. Zijn diagram is F_4.



In dimensie 5 of hoger zijn er enkel veralgemeningen van de tetraëder, de kubus en de octaëder. Deze hebben respectievelijk $n+1$, $2n$ en 2^n cellen en hun diagrammen zijn A_n en B_n. De andere Dynkin diagrammen leveren ook heel symmetrische objecten op maar deze zijn geen Platonische lichamen.

A.7 Affiene reflectiegroepen. Naast eindige deelgroepen zijn ook discrete deelgroepen van belang. De discrete deelgroepen van $\mathrm{Isom}(\mathbb{E}_n)$ waarvoor $G \cap \mathbb{R}^n = \mathbb{Z}^n = \langle \tau_1, \dots \tau_n \rangle$ met $\tau_1, \dots, \tau_n$ lineair onafhankelijke vectoren worden in het algemeen *Bieberbachgroepen* genoemd. In 2 dimensies zijn de Bieberbachgroepen de behangpatroongroepen en in 3 dimensies worden ze ruimtegroepen, kristalgroepen of Fedorovgroepen genoemd. Er zijn 230 ruimtegroepen en deze zijn van groot belang in de mineralogie omdat ze de verschillende mogelijkheden weergeven hoe kristallen kunnen opgebouwd zijn.

Stelling A.8 (Coxeter)**.** *Als* $\mathrm{Cox}(G)$ *een discrete groep is in* $\mathrm{Isom}(E_n)$ *dan is* G *een disjuncte unie van Dynkindiagrammen en affiene Dynkindiagrammen, die hieronder zijn weergegeven.*



Merk op dat je uit elk van deze affiene diagrammen (behalve bij $\tilde{I}_\infty$*) één knoop kan verwijderen en dan bekom je het overeenkomstige Dynkindiagram zonder tilde. Daarom worden affiene Dynkindiagrammen in het engels ook wel Extended Dynkin diagrams genoemd. In deze notatie verwijst de subscript* n *dus naar het aantal knopen* -1*.*

Deze classificatie overlapt met de classificatie van behangpatronen: we kunnen de behangpatroongroepen voortgebracht door spiegelingen terugvinden in de vorm van de volgende diagrammen: pmm= $\tilde{I}_\infty \cup \tilde{I}_\infty$, p4m= $\tilde{C}_2$, p6m= $\tilde{G}_2$, p3m1= $\tilde{A}_2$.

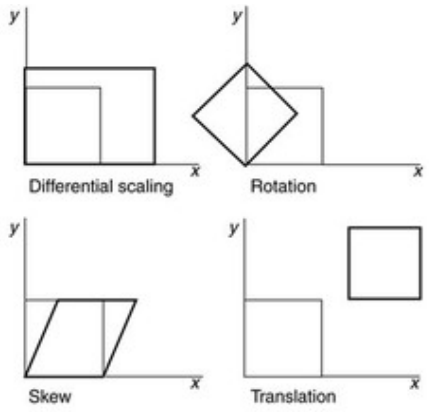
A.3 Andere soorten meetkunde

Zoals we gezien hebben is Euclidische meetkunde voornamelijk bepaald door de symmetriegroep die er op werkt. Door andere symmetriegroepen te beschouwen kunnen we dus nieuwe meetkundes maken.

A.1 Het affiene vlak $\mathbb{A}_2$. Deze meetkunde bevat dezelfde punten als het Euclidisce vlak, maar de symmetriegroep is nu

$$\mathrm{Aff}_2 = \{\vec{x} \mapsto A\vec{x} + \vec{b} | A \in \mathrm{Mat}_2(\mathbb{R}), \vec{b} \in \mathbb{R}^2 \text{ en } \det A \neq 0\}$$

Deze symmetriegroep beeldt nog steeds rechten op rechten af, dus een rechte is een welgedefiniëerd begrip in deze meetkunde. Afstanden en hoeken worden echter niet bewaard en dus worden cirkels niet noodzakelijk op cirkels afgebeeld. Het midden van een lijnstuk is welgedefiniëerd. Daarom is de stelling dat de drie zwaartelijnen van een driehoek elkaar in 1 punt snijden een stelling uit de de affiene meetkunde. De stelling dat de drie hoogtelijnen van een driehoek elkaar in 1 punt snijden is dan weer geen stelling uit de affiene meetkunde maar uit de Euclidische meetkunde.



In de affiene meetkunde zijn alle driehoeken gelijk want voor elk paar driehoeken is er een affiene transformatie die die driehoeken op elkaar afbeeldt. Daarnaast maakt de affiene meetkunde geen onderscheid tussen rechthoeken, parallellogrammen en ruiten want afstanden en hoeken zijn niet gedefiniëerd. Er is wel nog een onderscheid tussen trapezia en parallellogrammen want een affiene transformatie beeldt evenwijdige rechten af op evenwijdige rechten.

De classificatie van kegelsneden is ook heel eenvoudig: er zijn 3 banen: de ellipsen, de parabolen en de hyperbolen.

A.2 Het projectieve vlak $\mathbb{P}_2$. Dit heeft als punten de equivalentieklassen van tripels $(x : y : z)$ op herschaling na

$$\mathbb{P}_2 = \{(x : y : z) = \mathbb{R}(x, y, z) | (x, y, z) \in \mathbb{R}^3 \setminus \{(0, 0, 0)\}\}$$

De groep van transformaties zijn alle inverteerbare 3×3-matrices op herschaling na.

$$PGL_3(\mathbb{R}) = \{(x : y : z) \mapsto A(x : y : z) | A \in \mathrm{Mat}_3(\mathbb{R}), \det A \neq 0\} \cong GL_n(\mathbb{R})/\mathbb{R}^*$$

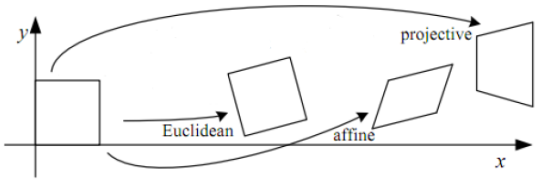
We kunnen het affiene vlak inbedden in het projectieve vlak:

$$\mathbb{A}_2 \to \mathbb{P}_2 : (x, y) \mapsto (x : y : 1)$$

De punten die niet in het beeld van deze afbeelding zitten worden de punten op oneindig genoemd. Zij hebben z-coordinaat gelijk aan 0.

Een rechte in het projectieve vlak zijn alle punten die voldoen aan een vergelijking $ax+by+cz = 0$. Elke rechte $ax+by+c = 0$ in het affiene vlak levert een rechte in het projectieve vlak $ax+by+cz = 0$, maar het projectieve vlak heeft nog 1 rechte meer namelijk $z = 0$. Dit noemen we de *rechte op oneindig* want ze bevat alle punten op oneindig. Een rechte $ax + by + cz = 0$ in het affiene vlak snijdt de rechte op oneindig in $(-b : a : 0)$. Twee evenwijdige rechten in het projectieve vlak snijden elkaar steeds, wanneer ze elkaar snijden in een punt op oneindig zijn ze evenwijdig in de affiene meetkunde.

In de projectieve meetkunde is de rechte op oneindig een rechte als een ander, er bestaan b.v. transformaties die de rechte op eindig afbeelden op de X-as zoals $(x : y : z) \mapsto (z : x : y)$. Deze transformatie beeldt dus evenwijdige rechten af op snijdende rechten en kan dus geen affiene transformatie zijn. De affiene transformaties zijn de projectieve transformaties die de rechte op oneindig op zichzelf afbeelden.

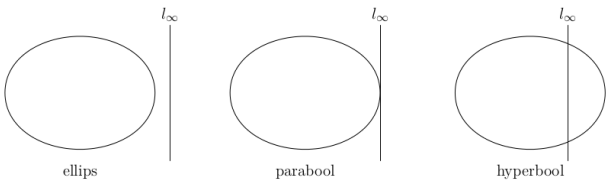


In projectieve meetkunde zijn niet alleen alle driehoeken gelijk maar ook alle vierhoeken gelijk. Als je de vierhoek $(1 : 0 : 0) - (0 : 1 : 0) - (0 : 0 : 1) - (1 : 1 : 1)$ wil afbeelden op $(a_1 : b_1 : c_1) - \cdots - (a_4 : b_4 : c_4)$, kan je eerst (a_4, b_4, c_4) schrijven als een lineaire combinatie $\lambda_1(a_1, b_1, c_1) + \cdots + \lambda_3(a_3, b_3, c_3)$. De matrix

$$\begin{pmatrix} \lambda_1 a_1 & \lambda_2 a_2 & \lambda_3 a_3 \\ \lambda_1 b_1 & \lambda_2 b_2 & \lambda_3 b_3 \\ \lambda_1 c_1 & \lambda_2 c_2 & \lambda_3 c_3 \end{pmatrix}$$

levert dan de gevraagde afbeelding.

Ook alle niet-ontaarde kegelsneden zijn gelijk. Het verschil tussen een ellips, parabool en hyperbool zit namelijk in hoe zij zich verhouden tot de rechte op oneindig: een hyperbool snijdt de rechte op oneindig in twee punten, een parabool raakt aan de rechte op oneindig en de ellips is disjunct met de rechte op oneindig.



Een praktische toepassing van projectieve meetkunde is perspectief. Twee fotos getrokken vanuit hetzelfde punt zijn projectieve transformaties van elkaar.

A.3 Het elliptisch vlak $\mathbb{S}_2$. Dit verhoudt zich tot het projectieve vlak zoals het Euclidische vlak zich verhoudt tot het affiene vlak: de punten van het elliptische vlak zijn dezelfde als die van het projectieve vlak maar de symmetriegroep is kleiner

$$PO_3(\mathbb{R}) = \{(x:y:z) \mapsto A(x:y:z) | A \in \mathrm{Mat}_3(\mathbb{R}), AA^\top = 1\} \cong O_3(\mathbb{R})/\{1,-1\} \cong SO_3.$$

Deze groep is dus de symmetriegroep van de eenheidssfeer en we kunnen de punten in $\mathbb{S}_2$ zien als paren tegenoverstaande punten op de eenheidssfeer.

Net zoals in de Euclidische meetkunde kunnen we een afstand tussen twee punten definiëren

$$d((x_1:y_1:z_1),(x_2:y_2:z_2)) = \cos^{-1}\left(\frac{|x_1x_2+y_1y_2+z_1z_2|}{\sqrt{x_1^2+y_1^2+z_1^2}\sqrt{x_2^2+y_2^2+z_2^2}}\right).$$

Dit is de kleinste afstand tussen de puntenparen $\pm(x_1:y_1:z_1)$ en $\pm(x_2:y_2:z_2)$ gemeten op de eenheidsfeer. Twee punten kunnen zich dus op maximaal $\pi/2$ van elkaar liggen. Men kan nagaan dat de afbeeldingen in PGL_3 die deze afstand bewaren de afbeeldingen in PO_3 zijn.

Een rechte $ax+by+cz=0$ komt overeen met de doorsnede van de eenheidsfeer en het vlak in de ruimte gedefiniëerd door $ax+by+cz=0$. De hoek tussen twee rechten kunnen we definiëren als de hoek tussen de twee vlakken. In deze meetkunde is de som van de hoeken van een driehoek steeds groter dan π en twee driehoeken zijn congruent als ze dezelfde hoeken hebben.

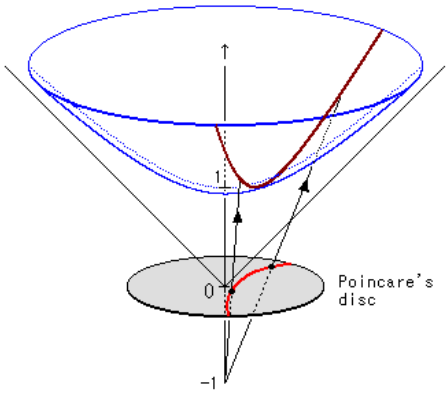
Elliptische meetkunde is van belang in de astronomie omdat we de sterrenhemel kunnen zien als een sfeer of een elliptisch vlak.

A.4 Het hyperbolisch vlak $\mathbb{H}_2$. Dit kan op dezelfde manier gedefiniëerd worden als elliptische meetkunde. De punten zijn tegenoverstaande puntenparen op de hyperboloide $x^2+y^2-z^2=-1$. De groep van isometriën is de groep van transformaties die de hyperboloide op zichzelf afbeelden

$$PO_{2,1}(\mathbb{R}) = \{(x:y:z) \mapsto A(x:y:z) | A \in \mathrm{Mat}_3(\mathbb{R}), A \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} A^\top = 1\}.$$

De rechten in deze meetkunde zijn doorsneden van vlakken $ax+by+cz=0$ met de hyperboloide. Door een punt kan je meerdere rechten tekenen die een gegeven rechte niet snijden want je kan ervoor zorgen dat het de snijlijn van de twee vlakken die deze rechtes definiëren, de hyperboloide niet snijdt. Deze meetkunde voldoet dus niet aan het parallellenpostulaat.

De hoek tussen twee rechten is de hoek tussen de twee vlakken die ze definiëren en de afstand tussen twee puntenparen wordt gemeten op de hyperboloide. In deze meetkunde is de som van de hoeken van een driehoek steeds kleiner dan π en twee driehoeken zijn congruent als ze dezelfde hoeken hebben.

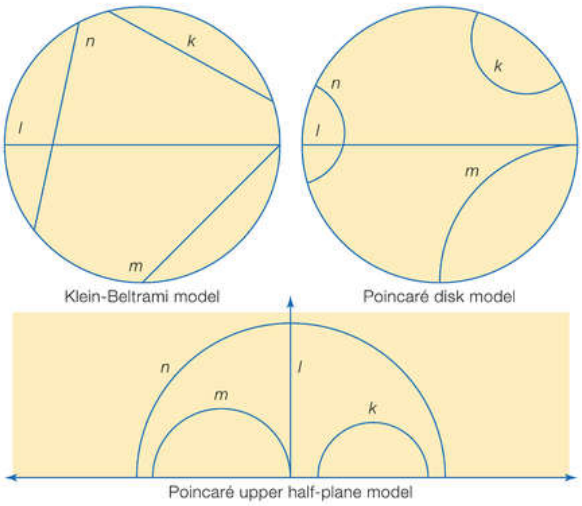


Om een beeld te vormen van het hyperbolisch vlak kan je het projecteren door het punt $(0, 0, -1)$ op het vlak $z = 1$. Het beeld van de hyperboloide onder deze projectie is het binnenste van de eenheidscirkel. En rechten in het hyperbolisch vlak worden afgebeeld op cirkels of rechten die loodrecht staan op de eenheidscirkel. Dit model van hyperbolisch vlak wordt het Poincaré disk model genoemd. De groep $PO_{2,1}(\mathbb{R})$ wordt in dit model voort gebracht door cirkelspiegelingen om de cirkels die rechten voorstellen in het hyperbolisch vlak. Een cirkelspiegeling rond een cirkel met middelpunt p en straal r beeldt een punt x af op een punt y zodat p, x, y op 1 rechte liggen en $|px||py| = r$.

Een ander model is het Poincaré halfvlak model. Dit heeft als punten de bovenste helft van het complexe vlak $\mathbb{H}_2 = \{u + vi | v > 0\}$ Op deze verzameling laten we de volgende groep werken

$$PSL_2(\mathbb{R}) = \{z \mapsto \frac{az+b}{cz+d} | a, b, c, d \in \mathbb{R} \text{ en } ad - bc = 1\} = \{A \in \mathrm{Mat}_2(\mathbb{R}) | \det A = 1\}/\{1, -1\}.$$

De 'rechtes' in deze meetkunde zijn de halve verticale rechtes $\mathrm{Re} z = u$ en de halve cirkels $|z - u| = r$ waarbij $u \in \mathbb{R}$ en $r \in \mathbb{R}_{>0}$. Men kan aantonen dat $PSL_2(\mathbb{R})$ transitief werkt op de verzameling van rechtes. $PSL_2(\mathbb{R})$ speelt hier de rol van directe isometriën om alle isometriën te krijgen moeten we nog een spiegeling om de imaginaire as toevoegen: $PO_{2,1}(\mathbb{R}) \cong \langle PSL_2(\mathbb{R}), \sigma : u + iv \mapsto -u + iv \rangle$. Het verband tussen het disk en het halfvlak model wordt gegeven door de afbeelding $z \mapsto \frac{1}{z+1}$.



Hyperbolische meetkunde was de eerste niet-Euclidische meetkunde die 'ontdekt' werd. Dit gebeurde onafhankelijk door de Rus Nicolai Lobatsjevski en de Hongaar János Bolyai in de eerste helft van de 19de eeuw.


Nicolai Lobatsjevski (1793–1856) en János Bolyai (1802–1860)

A.5 Euclidisch/Elliptisch/Hyperbolisch. Er zijn dus drie belangrijke 2-dimensionale meetkundes waarin afstanden gedefiniëerd zijn: de Euclidische, de elliptische en de hyperbolische. In elk van deze meetkundes kunnen we kijken naar discrete deelgroepen. Deze groepen komen overeen met bepaalde patronen die de meetkunde overdekken. In de elliptische meetkunde kan een discrete groep enkel een eindige groep zijn want alle punten liggen ten hoogste $\pi/2$ van elkaar. Zo een eindige deelgroep van SO_3 komt overeen met een patroon op een bol. In de Euclidische meetkunde zijn de belangrijkste discrete groepen de behangpatroongroepen. Deze komen overeen met betegelingen van het vlak. In de hyperbolische meetkunde staan de belangrijkste discrete groepen bekend als Fuchsiaanse groepen en zij geven aanleiding tot betegelingen van het hyperbolische vlak.

Lazarus Fuchs, Duits wiskundige, 1833-1902

.

De onderstaande stelling verbindt de discrete deelgroepen van de drie soorten meetkundes met elkaar.

Stelling A.6 (Driehoekgroepen)**.** *Beschouw het onderstaande diagram.*

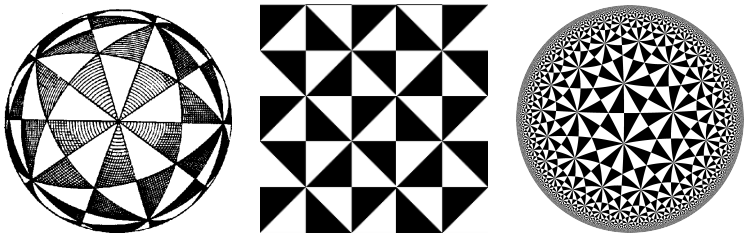
$$G = \quad n_1 \quad n_2 \quad n_3$$

1. *Als* $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} > 1$ *dan is* $\mathrm{Cox}(G)$ *een discrete deelgroep van het elliptische vlak.*
2. *Als* $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1$ *dan is* $\mathrm{Cox}(G)$ *een discrete deelgroep van het Euclidische vlak.*
3. *Als* $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} < 1$ *dan is* $\mathrm{Cox}(G)$ *een discrete deelgroep van het hyperbolische vlak.*

Merk op dat (1) en (2) reeds vervat zijn in de classificatie van Dynkin en Extended Dynkin diagrammen.

Bewijs. Idee: Beschouw een driehoek met als hoeken $\frac{\pi}{n_1}, \frac{\pi}{n_2}, \frac{\pi}{n_3}$. Als de som van de hoeken groter is dan π kunnen we de driehoek tekenen in het elliptische vlak, is de som π dan kunnen we hem tekenen in het Euclidsiche vlak en als de som kleiner is dan π kunnen we hem tekenen in het hyperbolische vlak. Beschouw nu de groep voortgebracht door spiegelingen om de zijden van de driehoek. De baan van de driehoek onder deze groep is een betegeling van het respectievelijke vlak en daarom discreet.

Hier geven we 3 voorbeelden met bijbehorende betegelingen: $(2, 3, 5)$, $(2, 4, 4)$ en $(2, 3, 7)$.



□

A.7 En nog veel meer... Om af te ronden geven we nog een kleine opsomming van enkele andere belangrijke meetkundes en de bijhorende groepen. Differentiaalmeetkunde: de groep van de gladde transformaties, topologie: de groep van de continue transformaties, algebraische meetkunde de groep van polynomiale transformaties, birationale meetkunde: de groep van alle rationale transformaties, complexe meetkunde: de groep van holomorfe transformaties.

Niet enkel in de wiskunde spelen groepen een belangrijke rol. Hier zijn nog enkele voorbeelden uit de fysica. Elke van onderstaande fysische theoriën bestudeert een soort ruimte en een bijbehorende groep. Speciale relativiteitstheorie: de Minkowski-ruimte en de groep van Lorentztransformaties, algemene relativiteitstheorie: de gekromde ruimtetijd en de groep van gladde transformaties, klassieke mechanica: de faseruimte en de groep van symplectische transformaties, quantummechanica: Hilbertruimten en unitaire groepen, quantumveldentheorie: hoofdvezelbundels, Liegroepen en ijkgroepen. M.a.w.

The universe is an enormous direct product of representations of symmetry groups.

Hermann Weyl, Duits wiskundige, (1885-1955)

.

Bijlage B

Fact Sheet

B.1 Nuttige stellingen voor het tentamen

0.9 ggd(a, b) is lineaire combinatie van a en b.

0.18 Priemfactor-ontbinding.

1.15 Definitie en formule voor Euler-functie $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^* = n\prod_{p|n}(1 - \frac{1}{p})$.

1.18 Schrijfwijze permutatie in cykels.

2.27 Characterizatie van het direct product.

2.29 De Chinese reststelling.

3.2 S_n is voortgebracht door 2-cykels,

3.7 Orde van het beeld van een element deelt orde van het element.

3.9 Orde van een element deelt orde van de groep.

3.11 Stelling van Euler: $a^{\varphi}(m) = 1 \mod m$

3.12 Kleine stelling van fermat: $a^p = a \mod p$

3.17 Nevenklassen zijn gelijk of disjunct.

3.23 Stelling van Lagrange: $\#G = [G : H] * \#H$

3.32 Stelling van Cauchy: als $p|\#G$ dan is er een element met orde p

2.19 formule voor teken van permutatie

4.4 $[G : H] = 2 \implies H$ normaaldeler

4.11 De Quotientconstructie (i.e. Kernen zijn normaaldelers en omgekeerd)

4.15 $[S_n, S_n] = A_n$, $[A_n, A_n] = A_n$ als $n > 4$ en $[A_4, A_4] = V_4$.

5.1 Homomorfiestelling

5.2 Eerste isomorfiestelling Beeld = G/Kern

5.6 Tweede isomorfiestelling $H/(N \cap H) = HN/N$

5.8 Derde isomorfiestelling $(G/N)/(N/N') = G/N'$

6.6 Stelling van Cayley: G kan ingebed worden in $S(G)$.

6.9 $[G : H]$=kleinste priemgetal dat $\#G$ deelt $\implies$ H normaaldeler.

6.14 Orde baan is index stabilizator.

6.18 Klasseformule.

6.19 p-groepen hebben een niet-triviaal center.

6.20 Formule van Burnside: aantal banen is gemiddeld aantal fixpunten per groepselement.

6.7 (opgave) De conjugatieclassen in S_n zijn de cykeltypes.

7.5 $\mathrm{Aut}(\mathbb{Z}/nZ) = (\mathbb{Z}/n\mathbb{Z})^*$.

7.7 Er zijn 2 groepen van de orde p^2 nl $\mathbb{Z}/p^2\mathbb{Z}$ en $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

7.9 Definitie van het semidirect product.

7.10 G is het semidirect product van H en N als N een normaaldeler is, $HN = G$ en $H \cap N = \{e\}$.

8.1 Elke eindige abelse groep is het product van cyclische groepen waarvan de opeenvolgende ordes elkaar delen.

8.10 Elke eindige abelse groep is het product van cyclische groepen met orde een priemmacht.

Ook goed om te weten:

Een partitie van n is een manier om n te schrijven als een som van natuurlijke getallen. b.v. de partities van 4 zijn

$$4, 3+1, 2+2, 2+1+1, 1+1+1+1.$$

Dingen die gelijk zijn aan het aantal partities van n: het aantal conjugatieklassen in S_n, het aantal abelse groepen van orde p^n,

B.2 Enkele belangrijke groepen en hun eigenschappen

- **De cyclische groep** $\mathbb{Z}/n\mathbb{Z} = C_n$
  Orde: n
  $\mathrm{Aut}(G) = (\mathbb{Z}/n\mathbb{Z})^*$
  $Z(G) = \mathbb{Z}/n\mathbb{Z}$
  $[G, G] = \{e\}$
  Alle conjugatieklassen hebben 1 element.

- **De viergroep van Klein** $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
  Orde: 4
  $\mathrm{Aut}(G) = S_3$
  $Z(G) = V$
  $[G, G] = \{e\}$
  Alle conjugatieklassen hebben 1 element.

- **De diëdergroep** D_n **met** n **oneven:** $\langle r, s | r^n = s^2 = (rs)^2 = 1 \rangle$ **(merk op** $S_3 \cong D_3$**)**
  Orde: $2n$
  $Z(G) = \{e\}$
  $[G, G] = \langle r \rangle$
  De conjugatieklassen zijn:
  $\{e\}$
  $\frac{n-1}{2}$ klassen van de vorm $\{r^i, r^{-i}\}$
  $\{s, r^1 s, ..., r^{n-1} s\}$.

- **De diëdergroep** D_n **met** n **even:** $\langle r, s | r^n = s^2 = (rs)^2 = 1 \rangle$
  Orde: $2n$
  $Z(G) = \{e, r^{n/2}\}$
  $[G, G] = \langle r^2 \rangle$
  De conjugatieklassen zijn
  $\{e\}$
  $\{r^{n/2}\}$
  $n/2 - 1$ klassen van de vorm $\{r^i, r^{-i}\}$
  $\{r^1 s, r^3 s, ..., r^{n-1} s\}$
  $\{r^0 s, r^2 s, ..., r^{n-2} s\}$

- **De symmetrische groep** $S_n, n > 5$
  Orde: $n!$
  $Z(G) = \{e\}$
  $[G, G] = A_n$
  De conjugatieklassen zijn de cykeltypes.

- **De alternerende groep** $A_n, n > 5$

Orde: n!/2
$Z(G) = \{e\}$
$[G, G] = A_n$
De conjugatieklassen zijn de cykeltypes behalve de cykeltypes met allemaal oneven cykels met verschillende lengtes (die bestaan uit 2 conjugatieklassen).

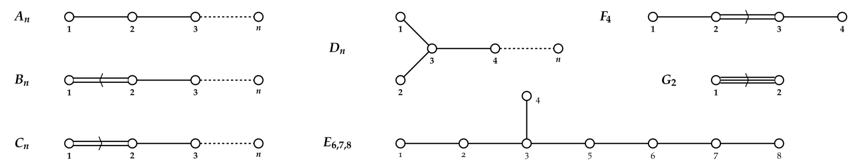
- **De draaiingssymmetriegroepen van de tetraeder:** A_4
  Orde: 12
  $Z(G) = \{e\}$
  $[G, G] = \{e, (12)(34), (13)(24), (14)(23)\} = V$
  Er zijn 4 conjugatieklassen:
  1 eenheids element: ()
  4 draaingen over 120 graden in wijzerzin om een hoekpunt: $\{(123), (214), (341), (432)\}$
  4 draaingen over 120 graden in tegenwijzerzin om een as door een hoekpunt $\{(132), (241), (314), (423)\}$
  3 draaiingen over 180 graden om een as door het centrum van een ribbe $\{(12)(34), (13)(24), (14)(23)\}$.

- **De draaiingssymmetriegroepen van de kubus (en de octaeder):** S_4
  Orde: 24
  $Z(G) = \{e\}$
  $[G, G] = A_4$
  Er zijn 5 conjugatieklassen:
  1 eenheids element: ()
  8 draaingen over 120 graden in wijzerzin om een hoekpunt: $\{(123), ...\}$
  6 draaingen over 90 graden in tegenwijzerzin om een as door een zijvlak: $\{(1234), ...\}$
  6 draaiingen over 180 graden om een as door het centrum van een ribbe: $\{(12), ...\}$
  3 draaingen over 180 graden in tegenwijzerzin om een as door een zijvlak: $\{(12)(34), (13)(24), (14)(23)\}$.

- **De draaiingssymmetriegroepen van de dodecaeder (en de icosaeder):** A_5
  orde: 60
  $Z(G) = \{e\}$
  $[G, G] = A_5$
  Er zijn 5 conjugatieklassen:
  1 eenheids element: ()
  20 draaingen over 120 graden in wijzerzin om een hoekpunt: $\{(123), ...\}$
  12 draaingen over 72 graden in tegenwijzerzin om een as door een zijvlak $\{(12345), ...\}$
  12 draaingen over 144 graden in tegenwijzerzin om een as door een zijvlak $\{(12354), ...\}$
  15 draaiingen over 180 graden om een as door het centrum van een ribbe $\{(12)(34), ...\}$

The Periodic Table Of Finite Simple Groups

Dynkin Diagrams of Simple Lie Algebras



$0, C_1, \mathbb{Z}_1$ **1** 1																	
C_2 2	$A_1(4), A_1(5)$ A_5 60											$A_2(2)$ $A_1(7)$ 168	${}^2A_3(4)$ $B_2(3)$ 25 920	$C_3(3)$ 4 585 351 680	$D_4(2)$ 174 182 400	$G_2(2)'$ ${}^2A_2(9)$ 6 048	${}^2D_4(2^2)$ 197 406 720
C_3 3	$A_1(9), B_2(2)'$ A_6 360											${}^2G_2(3)'$ $A_1(8)$ 504	$B_2(4)$ 979 200	$C_3(5)$ 228 501 000 000 000	$D_4(3)$ 4 952 179 814 400	${}^2A_2(16)$ 62 400	${}^2D_4(3^2)$ 10 151 968 619 520
C_5 5	A_7 2 520	$E_6(2)$ 214 841 575 522 005 575 270 400	$E_7(2)$ 7 997 476 042 075 799 759 100 487 262 680 802 918 400	$E_8(2)$ 337 804 753 143 634 806 261 388 190 614 085 595 079 991 692 242 467 651 576 160 959 909 068 800 000	$F_4(2)$ 3 311 126 603 366 400	$G_2(3)$ 4 245 696	${}^3D_4(2^3)$ 211 341 312	${}^2E_6(2^2)$ 76 532 479 683 774 853 939 200	${}^2B_2(2^3)$ 29 120	Tits* ${}^2F_4(2)'$ 17 971 200	${}^2G_2(3^3)$ 10 073 444 472	$A_1(11)$ 660	$B_3(2)$ 1 451 520	$C_4(3)$ 65 784 756 654 489 600	$D_5(2)$ 23 499 295 948 800	${}^2A_2(25)$ 126 000	${}^2D_5(2^2)$ 25 015 379 558 400
C_7 7	$A_3(2)$ A_8 20 160	$E_6(3)$ 7 257 703 347 541 463 210 028 258 395 214 643 200	$E_7(3)$ 1 271 375 236 818 136 742 240 479 751 139 021 644 554 379 203 770 766 254 617 395 200	$E_8(3)$ 18 830 052 912 953 932 311 099 032 439 972 660 332 140 886 784 940 152 038 522 449 391 826 616 580 150 109 878 711 243 949 982 163 694 448 626 420 940 800 000	$F_4(3)$ 5 734 420 792 816 671 844 761 600	$G_2(4)$ 251 596 800	${}^3D_4(3^3)$ 20 560 831 566 912	${}^2E_6(3^2)$ 14 636 855 916 969 695 633 965 120 680 532 377 600	${}^2B_2(2^5)$ 32 537 600	${}^2F_4(2^3)$ 264 905 352 699 586 176 614 400	${}^2G_2(3^5)$ 49 825 657 439 340 552	$A_1(13)$ 1 092	$B_2(5)$ 4 680 000	$C_3(7)$ 273 457 218 604 953 600	$D_4(5)$ 8 911 539 000 000 000 000	${}^2A_3(9)$ 3 265 920	${}^2D_4(4^2)$ 67 536 471 195 648 000
C_{11} 11	A_9 181 440	$E_6(4)$ 85 528 710 781 342 640 103 833 619 055 142 765 466 746 880 000	$E_7(4)$ 111 131 458 114 940 385 379 597 233 477 884 941 280 664 199 527 155 056 307 251 745 263 504 588 800 000 000	$E_8(4)$ 191 797 292 142 671 717 754 639 757 897 512 906 421 357 507 604 216 557 533 558 287 598 236 977 154 127 870 984 484 770 345 340 348 298 409 697 395 609 822 849 492 217 656 441 474 908 160 000 000 000	$F_4(4)$ 19 009 825 523 840 945 451 297 669 120 000	$G_2(5)$ 5 859 000 000	${}^3D_4(4^3)$ 67 802 350 642 790 400	${}^2E_6(4^2)$ 85 696 576 147 617 709 485 896 772 387 584 983 695 360 000 000	${}^2B_2(2^7)$ 34 093 383 680	${}^2F_4(2^5)$ 1 318 633 155 799 591 447 702 161 609 782 722 560 000	${}^2G_2(3^7)$ 239 189 910 264 352 349 332 632	$A_1(17)$ 2 448	$B_2(7)$ 138 297 600	$C_3(9)$ 54 025 731 402 499 584 000	$D_5(3)$ 1 289 512 799 941 305 139 200	${}^2A_2(64)$ 5 515 776	${}^2D_4(5^2)$ 17 880 203 250 000 000 000
$\mathbb{Z}_p$ C_p p	A_n $\frac{n!}{2}$	$E_6(q)$ $\frac{q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)}{(3,q-1)}$	$E_7(q)$ $\frac{q^{63}}{(2,q-1)}\prod_{i=1, i\neq 2,8}^{9}(q^{2i}-1)$	$E_8(q)$ $q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$	$F_4(q)$ $q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$	$G_2(q)$ $q^6(q^6-1)(q^2-1)$	${}^3D_4(q^3)$ $q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	${}^2E_6(q^2)$ $\frac{q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)}{(3,q+1)}$	${}^2B_2(2^{2n+1})$ $q^2(q^2+1)(q-1)$	${}^2F_4(2^{2n+1})$ $q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	${}^2G_2(3^{2n+1})$ $q^3(q^3+1)(q-1)$	$PSL_{n+1}(q), L_{n+1}(q)$ $A_n(q)$ $\frac{q^{n(n+1)/2}}{(n+1,q-1)}\prod_{i=1}^{n}(q^{i+1}-1)$	$O_{2n+1}(q), \Omega_{2n+1}(q)$ $B_n(q)$ $\frac{q^{n^2}}{(2,q-1)}\prod_{i=1}^{n}(q^{2i}-1)$	$PSp_{2n}(q)$ $C_n(q)$ $\frac{q^{n^2}}{(2,q-1)}\prod_{i=1}^{n}(q^{2i}-1)$	$O_{2n}^{+}(q)$ $D_n(q)$ $\frac{q^{n(n-1)}(q^n-1)}{(4,q^n-1)}\prod_{i=1}^{n-1}(q^{2i}-1)$	$PSU_{n+1}(q)$ ${}^2A_n(q^2)$ $\frac{q^{n(n+1)/2}}{(n+1,q+1)}\prod_{i=2}^{n+1}(q^i-(-1)^i)$	$O_{2n}^{-}(q)$ ${}^2D_n(q^2)$ $\frac{q^{n(n-1)}(q^n+1)}{(4,q^n+1)}\prod_{i=1}^{n-1}(q^{2i}-1)$

Mathieu Group M_{11} 7 920	*Mathieu Group* M_{12} 95 040	*Mathieu Group* M_{22} 443 520	*Mathieu Group* M_{23} 10 200 960	*Mathieu Group* M_{24} 244 823 040	*Janko Group* J_1 175 560	*Janko Group* J_2 604 800	*Janko Group* J_3 50 232 960	*Janko Group* J_4 86 775 571 046 077 562 880	*Higman-Sims Group* HS 44 352 000	*Mclaughlin Group* McL 898 128 000	*Held Group* He 4 030 387 200	*Rudvalis Group* Ru 145 926 144 000
Suzuki Group Suz 448 345 497 600	*O'Nan Group* $O'N$ 460 815 505 920	*Conway Group* Co_3 495 766 656 000	*Conway Group* Co_2 42 305 421 312 000	*Conway Group* Co_1 4 157 776 806 543 360 000	*Harada-Norton* HN 273 030 912 000 000	*Lyons Group* Ly 51 765 179 004 000 000	*Thompson Group* Th 90 745 943 887 872 000	*Fischer Group* Fi_{22} 64 561 751 654 400	*Fischer Group* Fi_{23} 4 089 470 473 293 004 800	*Fischer Group* Fi'_{24} 1 255 205 709 190 661 721 292 800	*Baby Monster* B 4 154 781 481 226 426 191 177 580 544 000 000	*Monster* M 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

- Cyclic Groups
- Alternating Groups
- Classical Chevalley Groups
- Chevalley Groups
- Classical Steinberg Groups
- Steinberg Groups
- Suzuki Groups
- Ree Groups and Tits Group*
- Sporadic Groups

Alternates† Symbol Order‡

*The Tits group ${}^2F_4(2)'$ is not a group of Lie type, but is the (index 2) commutator subgroup of ${}^2F_4(2)$. It is usually given honorary Lie type status.

The groups starting on the second row are the classical groups. The sporadic suzuki group is unrelated to the families of Suzuki groups.

†For sporadic groups and families, alternate names in the upper left are other names by which they may be known. For specific non-sporadic groups these are used to indicate isomorphims. All such isomorphisms appear on the table except the family $B_n(2^m) \cong C_n(2^m)$.

‡Finite simple groups are determined by their order with the following exceptions:
$B_n(q)$ and $C_n(q)$ for q odd, $n > 2$;
$A_8 \cong A_3(2)$ and $A_2(4)$ of order **20160**.